Hardening

September 3, 2023

Contents

1 Introduction

I remembered how Albert Camus talks about the concept of resistance. The idea is that if you see that you cannot win, do everything in your power to resist. And that memory gave me the determination I needed.

Ding Liren

Assume everything is compromised. Even the laptops you are using for the competition! Be paranoid!

Assume the Red Team has thoroughly reviewed all publicly available material, including systems from past years. They've highlighted instances of teams reusing passwords over multiple years, and the red team uses a wordlist of passwords from previous competitions. One read teamer even claimed the capability to enumerate all 12-character passwords in 6 hours (involving renting cloud GPUs).

Given that the Red Team has the entire night to crack hashes, it's important to use good passwords. I make passwords by thinking of random objects and then scattering some symbols & numbers around. The red team's hash-cracking ability is probably especially relevant for windows, as kerberos uses hashes extensively.

2 Active Directory Freebies

There are some very quick and easy ways to harden active directory.

1. Disable all of the accounts besides the black team and your own
2. Change your password to something random and good
3. At some point, you can make a new administrator account with an unusual username. You can keep the old account around as a honeypot if you want
4. After disabling accounts, you must kick them off of the machine! Merely disabling the account does not kick the user off of the machine
5. You must also view the ssh connections and kick them off. (both ssh and rdp)
6. Look at GPO and disable any malicious policies, such as policies that disable microsoft defender.

3 Local Account Freebies

In addition to active directory, your computer has a local directory of users. These include the Guest user. Make sure all of the local accounts are disabled.

You can get the local users with:

```
get-LocalUser
```

And disable the accounts with:

```
Disable-LocalUser -Name "Guest"
```

4 Registry Keys and Autoruns

Tryhackme on Windows Forensics Zimmerman registry explorer

Often keys in things like Firefox or AmazonVM thingie will be creatively named by the red team so you don't notice them.

4.1 What is the Windows Registry?

The Windows Registry is a database storing Windows OS and application settings. Watch this video

Keys and Subkeys These are like folders and subfolders. They can contain other keys (subkeys) and values.
For instance, HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla might be a key where settings specific to Mozilla software are stored.
Values: These are the actual data entries within a key or subkey. Each value has a **name, a type, and data.**

Value Types

- REG_SZ: A string value. It's a readable text value and one of the most common types you'll encounter.
- REG_DWORD: A 32-bit number. Often used for flags, settings, or Boolean values. For example, a setting might be 0 (off) or 1 (on).
- REG_QWORD: A 64-bit number.
- REG_BINARY: Raw binary data.
- REG_MULTI_SZ: Multiple string values, usually in an array. Useful when an application needs to store multiple entries in a single value.
- REG_EXPAND_SZ: A string that includes variables to be replaced when called by an application. For instance, %UserProfile% might expand to the directory path of the current user's profile.

There are other types, but these are the most common.

Image File Execution Options (IFEO) in the Windows Registry allow developers to specify debugging tools to launch when a particular executable starts, but they can be misused by malware to redirect or hijack the execution of legitimate programs

5 Firewall / Network

5.1 Banning IPs

Banning IPs makes me paranoid of accidentally "red teaming" myself, but it can be a good idea.

I will look into this program called IP Ban.

6 Red Team Gimmicks

I was surprised by it, but I wasn't surprised that I was surprised. I expected a surprise, I just wasn't sure which one.

Fabiano Caruana

The red team loves gimmicks. It adds some fun and lets them be creative. So expect to be surprised.

6.1 Visitors to the room

Assume all visitors are malicious. If people walk in the room, cover your password sheets. I kept mine in my pocket and only took it out when I needed it.

6.2 The Intern

There is an intern, and they will be polite and unassuming. But their goal is to mess with you! Never take your eyes off the intern! They can try to plug USBs into your computers, take pictures with your password sheets (don't allow them to take any pictures). Apparently the intern and her handler will follow any rules you tell them. So tell them to not take picures, install unwanted programs, plug in devices, etc.

6.3 Other devices in the room

One time the red team got passwords by having a hidden camera in the room and using it to view passwords on the whiteboard. Be careful of physical devices in the room. I think there was speculation that a doll had a camera in it, idk.

7 Running an Anti Virus

Windows Defender is good and easy as it comes preinstalled. Of course you should remove any exclusions.

Allowed Programs Rules about The CCDC rules say programs/information "are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee"
So we can use free antiviruses, or those with a no-card-required free trial.

Possible Antiviruses

- Kaspersky free
- Hitman Pro seems to be a good choice for scanning the file hashes against a large database.
- Norton Power Eraser can check for Potentially Unwanted Applications (PUA) and can scan for rootkits.
- Kaspersky's TDSSKiller to remove rootkits.

8 Sysinternals

The best antivirus is you. It's not empowering, it's mostly just sad. You need to be able to identify malicious processes using Sysinternals tools.

Mark Russinovitch He has a youtube channel with great presentations on sysinternals (and he made sysinternals!):

- Mark Russinovich on Malware Hunting with Sysinternals
- License to Kill: Malware Hunting with the Sysinternals Tools
- Russinovich also wrote a book (don't pirate it): Windows Sysinternals Administrator's Reference

8.1 Process Explorer

Process Explorer provides detailed information about processes, including a hierarchical view of parent and child processes, as well as in-depth details about resources, handles, and DLLs in use. It allows you to suspend and kill processes, and can scan the file hashes against VirusTotal.

The red team may give you some low hanging fruit with malware that rings up on VirusTotal. But if it is not that simple, always remember that suspicious processes include: conhost.exe / command prompts, powershell prompts, and exe files.

Replacing task manager In process explorer, click "run as task manager." Now Ctrl+Shift+Esc will open Process Explorer (instead of task manager).

Tips from a Professor K video Professor K on Process Explorer

"Put malware to sleep, and only then kill it. Then they don't know what's happening. A lot of malware out there has the buddy system. Instead of racing against the buddy system and deleting both malicious files before they respawn each other, suspend them and then terminate them."

"Also if it is necessary, you don't want to cause irreperable damage to your system."

Things to look for from the Professor K video:

1. No "Verified Signer"
2. VirusTotal scan
3. Strings of the executable
4. Process' properties & the TCP/IP tab
5. DLLs of the process
6. Handles of the process
7. Where the process is launching from
8. Can view the autostart location from the registry

From Mark Russinovich:

1. Purple means a process is packed / encrypted
2. Have process explorer verify image signatures
3. Change your refresh rate to 9 seconds so you can see short lived processes

From me

1. Be wary that just because a program is started by System32 does not mean it is safe. I experienced this personally when Eduardo used the Covenant malware against me. It used processes started by System32.

Sigcheck command The sigcheck command with these flags recursively scans the C: drive for unsigned executables, verifies their status against VirusTotal.com, and opens the browser to the viruses that are detected.

```
sigcheck -e -u -vr -s c:\
```

listdlls Lists all processes that have loaded unsigned DLLs

```
listdlls -u *
```

8.2 Autoruns

1. Show only images that are not signed by microsoft. This will reduce the noise and focus only on the potential malware.

2. WMI tab autoruns (What is WMI) WMI-based persistence is less well-known and therefore may be overlooked during manual investigations.

3. Timestamp column. The timestamp indicates when a file was created or last modified.

To remove the program that is started by the shell, he changes its registry startup from Shell to explorer.exe

8.3 Process Monitor

"When in doubt, run process monitor"

Mark Russinovich

8.4 TCPView

TCPView provides a real-time graphical representation of the active TCP and UDP endpoints on a system. It displays details about the processes that initiated the connections, the local and remote addresses, as well as the state of each connection. This tool is particularly useful for network diagnostics, security investigations, and understanding the network activity of a system.

You can view active TCP and UDP connections from TCPView, but you must go to Process Explorer to kill them.

9 Securing DNS

9.1 Disabling Recursive Lookups

"Disabling recursive lookups can help prevent DNS-based DDoS attacks. Recursive DNS queries are when a DNS server processes a domain name request on a domain name for which it is not authoritative (or has not already cached) by querying the root name servers for the IP address of the requested domain name1. A remote attacker could spoof a recursive DNS query with a source address of a network they wish to cause a denial of service for. The attacker spoofs a query with a small payload and causes the DNS server to reply with

much more data. This floods the target network with answers to questions it never asked for2. Disabling open recursion, which causes the server to accept DNS requests from any IP address, can reduce DNS attack loopholes" -Bing

CISA on DNS recursion

9.2 DNSSEC

Domain Name System Security Extensions

Protect against DNS spoofing and cache poisoning

DNSSEC Resources

- ICANN on DNSSEC
- Akadia DNS Hardening

10 Securing Active Directory

Sean Metcalf A mobster in the AD space. He runs the site adsecurity.org/ and I have made a playlist of some useful videos: playlist.

Black Hills Information Security Video This video is pretty good. Active Directory Best Practices That Frustrate Pentesters

11 Event Logs

I am going to do this room and then get back to you. But they are definitely very important!

Event Viewer can be launched by typing eventvwr.msc

Event Viewer has three panes.

1. The pane on the left provides a hierarchical tree listing of the event log providers.
2. The pane in the middle will display a general overview and summary of the events specific to a selected provider.
3. The pane on the right is the actions pane.

12 Caution with Shortcuts

Shortcuts can have extra properties and run other programs when you click them. For example, the Firefox shortcut could really run a script that opens firefox and also some other malicious program.
Viewing the properties of a shortcut in the desktop is very straightforward.

Properties of a shortcut in the taskbar To view the properties of a shortcut in the taskbar,

- Right-click on the shortcut in the taskbar.
- If the program is already running or pinned to the taskbar, you may see a "jumplist" (a list of recent items, tasks, or pinned items related to that application). If you see this jumplist:
- Right-click again on the application's name or icon in that jumplist (i.e., the entry at the top).
- A context menu will appear. Choose Properties from the context menu.

13 GPO Policies

Group Policy Objects (GPOs) are a way to centrally manage and enforce configuration settings for computers and users within an Active Directory domain.

- What are job objects? How can I use them to set limits on program execution /

1. Audit logs for login attempts, file access, system configurations
2. Account Lockout policy, to prevent brute force attacks. Can I hook it up to an auto-ban as well?
3. Restrict USB drives (can't hurt. You never know)
4. Restrict command prompt and powershell
5. SRP (software restriction policies). Only allows identified applications to run.
6. Enforce LDAPS. Domain Controller: LDAP server signing requirements
7. Enforce encryption for SMB, RPC, others?
8. Setup the firewall from GPO to not have to do it multiple times.
    - Block SSH (we only use RDP, can reduce attack surface/scripting ability)
    - Block WinRM
    - Allow RDP
    - Allow LDAP on port 389.
    - Allow LDAPS on port 636.
    - Allow DNS on port 53.
    - Allow Kerberos on port 88.

- Allow RDP on port 3389 for specified IP ranges or administrators.
- Allow SMB on port 445.
- Allow NetBIOS (if required) on ports 137, 138, 139.
- Allow NTP (network time protocol) on port 123
-

9. Task scheduler. Can run antivirus scans on all the computers
10. Software Installation. Can automatically install antivirus and sysinternals, for example.
11. Set the local admin passwords through a script given by GPO. Or can use LAPS (Local Administrator Password Solution).
12. Can send a script to kick off all users who had their accounts disabled

14 Volatility Framework

Metasploit and other viruses can run only in RAM. We can find them from their network connections, but also from RAM forensics.