

Contents

1	Introduction	1
2	Active Directory Freebies	2
3	Local Account Freebies	2
4	Registry Keys and Autoruns	2
4.1	What is the Windows Registry?	2
5	Firewall / Network	3
5.1	Banning IPs	3
6	Red Team Gimmicks	3
6.1	Visitors	3
6.2	The Intern	3
6.3	Other devices in the room	3
7	Running an Anti Virus	3
8	Sysinternals	4
8.1	Process Explorer	4
8.2	Autoruns	5
8.3	Process Monitor	5
9	Securing DNS	6
9.1	Disabling Recursive Lookups	6
9.2	DNSSEC	6
10	Securing Active Directory	6
11	Event Logs	6

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!

Also assume that the red team has fully gone through your public material the machines from previous years, as I know they have gloated of busting teams who reuse passwords across multiple years. They have a wordlist of all of the passwords used in past competitions and run through it. On the topic of passwords, one red teamer gloated that he could enumerate all 12 character passwords in some short amount of time (6 hours?). The red team does have the entire night to crack hashes. So make long passwords!

This is probably especially relevant for windows, as kerberos uses hashes extensively. `update` with more details.

2 Active Directory Freebies

There are some very easy and quick 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 disabling the accounts with: `Disable-LocalUser -Name "Guest"`

4 Registry Keys and Autoruns

Write a program to scan the windows registry and report any anomalies in the keys. Often keys in things like Firefox or AmazonVM thingie will be creatively named by the red team so you don't notice them. Need a program to definitively scan all registry keys for malware.

4.1 What is the Windows Registry?

Idk

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

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 pictures, 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.

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.

Kaspersky seems to be a good antivirus choice.

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 Process Explorer

Great presentation, 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

Video mentions program modifying the shortcut to use command line arguments. Could be a funny way of running malware. Don't trust the shortcut icons!

8.1 Process Explorer

Be wary that just because a program is started by System32 does not mean it is safe. [covenant malware] The red team may give you some low hanging fruit with malware that rings up on VirusTotal. Suspicious processes include: conhost.exe / command prompts powershell prompts exe files

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

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 irreparable 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

This command checks all executables in the C drive on VirusTotal, and opens the browser to the ones that are detected.

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

Checks for dlls being signed

```
listdlls -u *
```

8.2 Autoruns

1. Show only images that are not signed by microsoft
2. WMI tab autoruns (What is WMI)
3. Timestamp column

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

8.3 Process Monitor

"When in doubt, run process monitor"

Mark Russinovich

Useful filter is: Category isRight only shows changes made to the system

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
<https://www.cisa.gov/sites/default/files/publications/DNS-recursion033006.pdf>

9.2 DNSSEC

Domain Name System Security Extensions

Protect against DNS spoofing and cache poisoning

<https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en>

https://www.akadia.com/services/dns_hardening.html

10 Securing Active Directory

One inject mentioned Sean Metcalf. He runs the site adsecurity.org/ and I have made a playlist of some useful videos: [playlist](#).

11 Event Logs