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. I think in the past, the red team has even had access to the laptops you are given. Be paranoid!

Also assume that the red team has fully gone through your public material the machines from previous years. I know they have gloated in the past of busting teams who reuse passwords across multiple years. They have a wordlist of all of the passwords used in past competions and run through it. On the topic of passwords, one red teamer gloated that he could enumarate 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 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 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.

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.

7.1 Process Explorer

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

8 Securing DNS

8.1 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

8.2 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

9 Securing Active Directory