Offense

September 4, 2023

Windows Offense

Contents

1 Introduction

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu

To be a good blue team, we should practice red teaming.

2 Covenant Malware

Covenant is a .NET command and control framework. It works by installing Grunts on the target machine. Grunts work like reverse shells, they connect to a listener on the C2 server.

You should install covenant on whatever computer you plan to use as the C2 server. This will let you control the windows machines. Covenant requires GIT and .NET to work. You will also need to install .NET on the victim machine.

- Instructions on their GitHub
- Blog Tutorial
- More information on listeners

To install GIT on windows, go here: https://git-scm.com/download/win

To install .NET, you can download it from the website or you can install it in server manager (in the "Features" menu).

To install .NET on linux, follow these directions

After installing the dependencies, we can install and run covenant with:

```
git clone --recurse-submodules https://github.com/cobbr/Covenant
cd Covenant/Covenant
dotnet build
dotnet run
```

"After running these commands, the Covenant service should be up and running. You can then browse to the Covenant application interface on its default web port of 7443 to set up a user account and begin using the framework." -Bing

If you would like to have listeners on ports 1-1023, you should run Covenant as root.

The web console can be accessed at https://127.0.0.1:7443 and not localhost:7443, as the https is important

For the Grunt to work, .NET has to be installed on the victim.

Anti Grunt countermeasures: "If you uninstall the .NET Framework 3.5 from the victim machine, it is likely that the Grunt will stop working." -Bing. I think it is very funny that malware has dependencies.

2.1 Troubleshooting the VPN

I tried a lot of ways to get the Grunt to recognize my machine. The only solutions that worked are a Kali VM or Cloudflare Tunnels.

To get your IP address from the RDP connection:

1. Open the Command Prompt by pressing the Windows key + R and typing cmd.
2. Type netstat -n — find ":3389" and press Enter. This will display a list of active connections to the RDP port (3389).
3. Look for the connection that corresponds to your RDP session. The IP address of the RDP client will be listed next to the ESTABLISHED entry.

Advanced Usage of Covenant

3 Cloudflare Tunnels

Justin mentioned how he was going to connect to the machines using cloudflare tunnels. So I will practice that and document it.

1. You can use your own domain, or you can have cloudflare provide one for you.
2. You need to install cloudflared on the machines you are connecting to
3. To install on proxmox:

```
wget -q
https://github.com/cloudflare/cloudflared/releases/latest/download/cloudflared-linux-amd64.deb
&& sudo dpkg -i cloudflared-linux-amd64.deb
```

4. To do it without a domain: cloudflared tunnel –url http://localhost:80
5. Take note of the random url generated.
6. cloudflared access tcp –hostname randomsubdomain.trycloudflare.com –url tcp://localhost:5900

4 BloodHound

BloodHound is a tool that maps out Active Directory (AD) relationships and permissions, turning them into clear visual graphs. It helps both defenders and attackers see potential security risks within AD environments, making it easier to spot vulnerabilities or misconfigurations.

5 WinPeas

Windows Privilege Escalation Scripts.

This script dumps a bunch of information about potentially interesting things to look for on the windows machine. It can be found here.

6 SMBGhost / EternalDarkness / CVE-2020-0796

SMBGhost (CVE-2020-0796), also referenced as EternalDarkness, is a severe vulnerability in Microsoft's Server Message Block (SMB) 3.1.1 protocol. This flaw permits unauthenticated remote attackers to execute arbitrary code on vulnerable systems.

This could be important to understand as it is a significant vulnerability in old Windows Server systems. TODO: add more potential vulnerabilities, explain this one more.

- ZecOps Blog on SMBGhost - Writeup and PoC on exploiting SMBGhost (CVE-2020-0796) for local privilege escalation.
- Carbon Black's EternalDarkness Remediation - Detecting and remediating the EternalDarkness vulnerability.
- VMware's Threat Analysis on EternalDarkness - VMware's analysis of EternalDarkness/GhostSMB.
- CISA Alert on CVE-2020-0796 - CISA giving resources on EternalDarkness/GhostSMB.

7 Stupid Active Directory Things

These are the low hanging fruit. However, they are not obvious as windows is very convoluted.

In AD, to view accounts marked as "IsCriticalSystemObject", the user has to click the "view -¿ advanced features" option. This is stupid and not obvious. So you can just make an account and mark it as "isCriticalSystemObject" and it will be much more difficult to see.

You can set IsCriticalSystemObject from adsi edit or you can do it from powershell like

Setting IsCriticalSystemObject can interfere with the replication of the account (?)

To run the script, you must have the permissions of a domain admin (can log in explicilty as a domain admin like administrator@cyber).

8 Mimikatz

Mimikatz can be used to create Golden and Silver tickets. These can be used to access system resources even if an account is locked or disabled.

8.1 Working Principles of Mimikatz

Mimikatz is a well-known post-exploitation tool designed for Windows environments. It targets the Local Security Authority Subsystem Service (LSASS) to extract credentials and perform various forms of attacks. Here are its primary functionalities:

- **LSASS Targeting:** Mimikatz injects a Dynamic Link Library (DLL) into the LSASS process to extract sensitive credential information stored in memory.
- **Credential Dumping:** It is capable of obtaining plaintext passwords, NTLM hashes, and Kerberos tickets.
- **Overpass-The-Hash and Pass-The-Hash:** Mimikatz can use NTLM hashes to request Kerberos tickets or authenticate directly to other services.
- **Ticket Manipulation:** It can craft or manipulate Kerberos Golden and Silver Tickets.
- **DPAPI Interaction:** Mimikatz can decrypt credentials stored by the Data Protection API (DPAPI).

8.2 What is a Kerberos ticket

8.3 Golden and Silver Tickets

Silver Tickets: These are Kerberos tickets that are used for a particular service and are generated using the Service Account's secret key. They are essentially 'forged' tickets that can be used to access specific services as a legitimate user. An attacker could use a silver ticket to impersonate a user and gain unauthorized access to network resources.

Silver tickets require elevated privileges, but not necessarily on the DC.

Silver Tickets remain valid as long as the service account password hasn't changed.

Golden Tickets: These are more powerful than silver tickets. A golden ticket is a TGT that is forged with the Key Distribution Center's (KDC) secret key (KRBTGT). It can grant access to any resource within the domain, effectively making the holder a superuser. Golden tickets are generally the result of an attacker having compromised the domain controller.

Golden tickets require Domain-Admin level privileges.

Golden Tickets remain valid as long as the KRBTGT account's password (or rather, its hash) remains the same.

9 Malware to look into

Here is some random stuff so I don't forget to look into it:

- WinKit - A collection of useful Windows utilities and configurations.
- Spectre - Tool for generating payload delivery scripts.
- DarkCoderSc's repositories - Contains various hacking and penetration testing tools, notably ones focused on Windows exploitation.
- DarkComet (infected file, do not run on main OS: GitHub Link) - A Remote Access Trojan (RAT) that allows control over infected devices.
- Quasar - An open-source RAT for Microsoft Windows operating systems.
- TheFatRat - A tool for generating backdoor payloads and bypassing common anti-virus solutions.
- win-brute-logon - A tool for bruteforcing login credentials on Windows systems.
- evil-winrm -

10 Real Administration Software to try

- ISL Online - Remote desktop and support software solution.
- Remote Desktop Manager by Devolutions - Software for managing multiple remote connections efficiently.