# 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

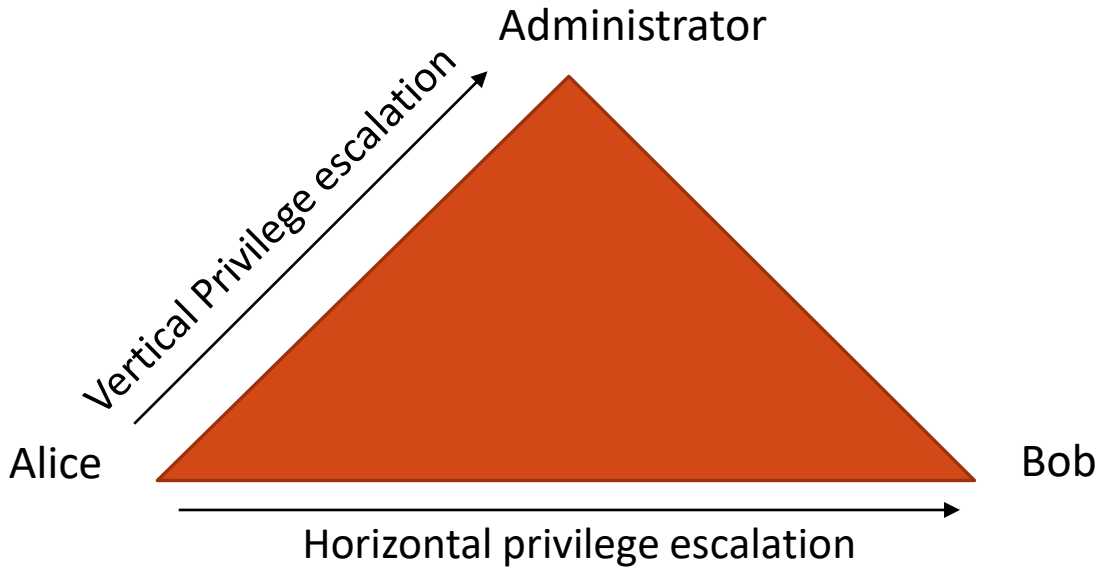
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

# Lab 3: Escalating Privileges and Installing a Backdoor

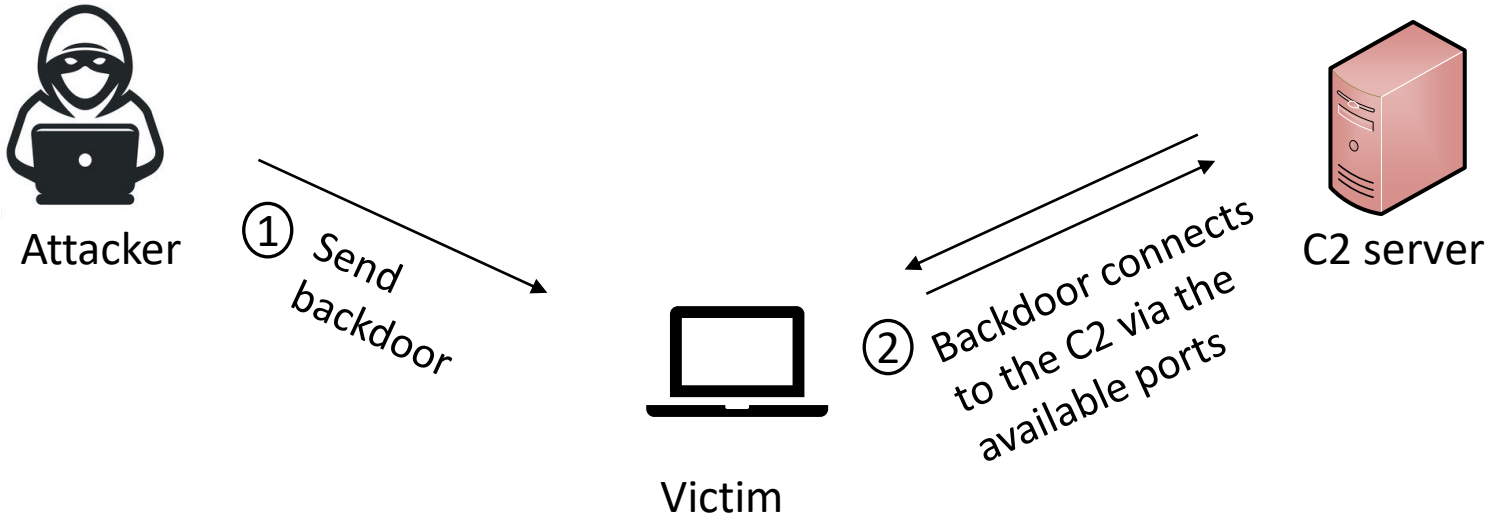
# Privilege Escalation

- 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

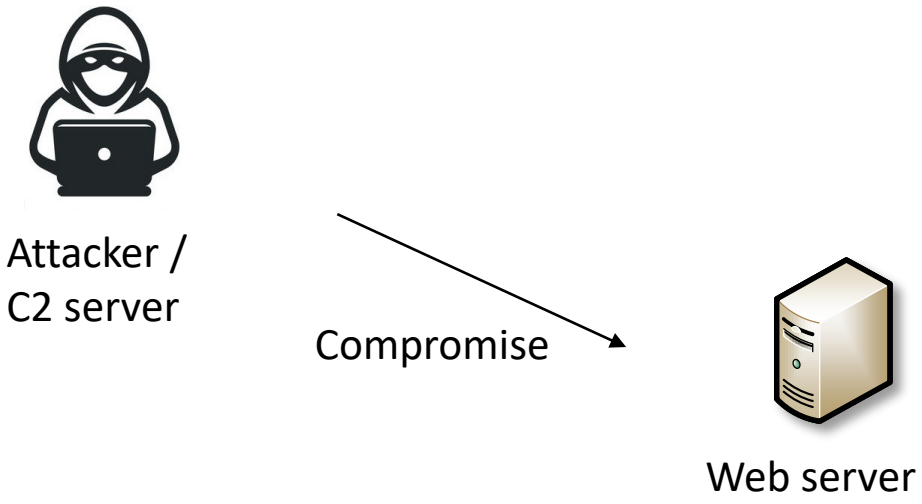
- A backdoor enables the attacker to have persistent access to the victim's machine[1]
- Backdoors allow the attacker to return later to the victim's machine and bypass any security settings
- Installing a backdoor requires modifying system files, and thus, requires elevated privileges




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

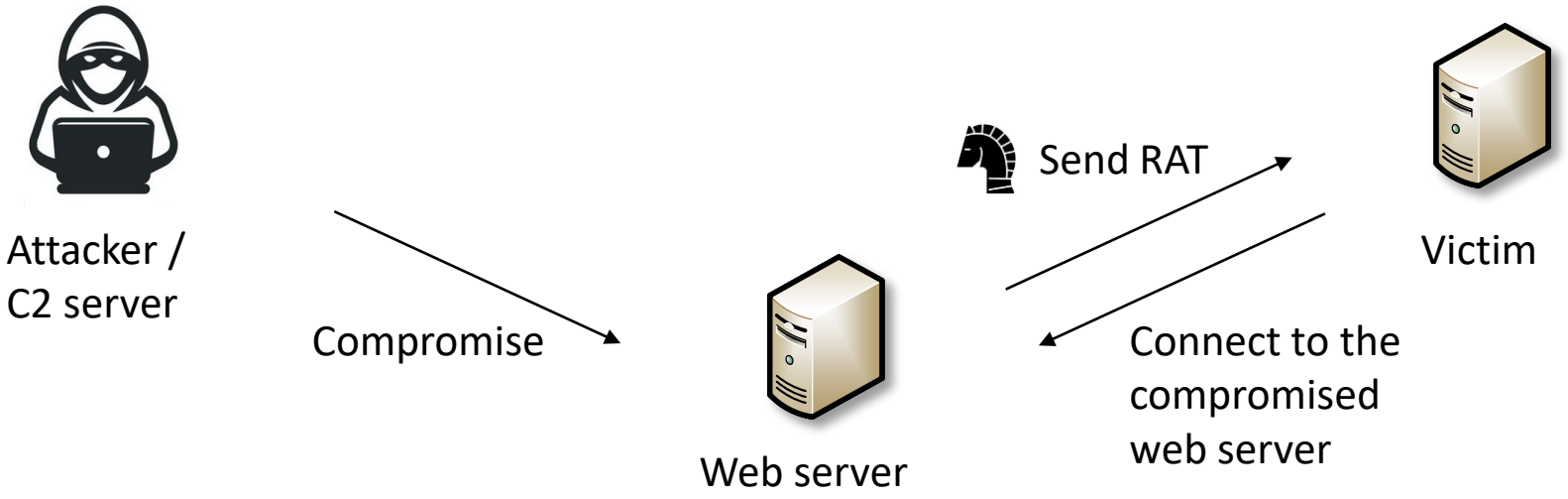
# Attack Scenario

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



# Attack Scenario

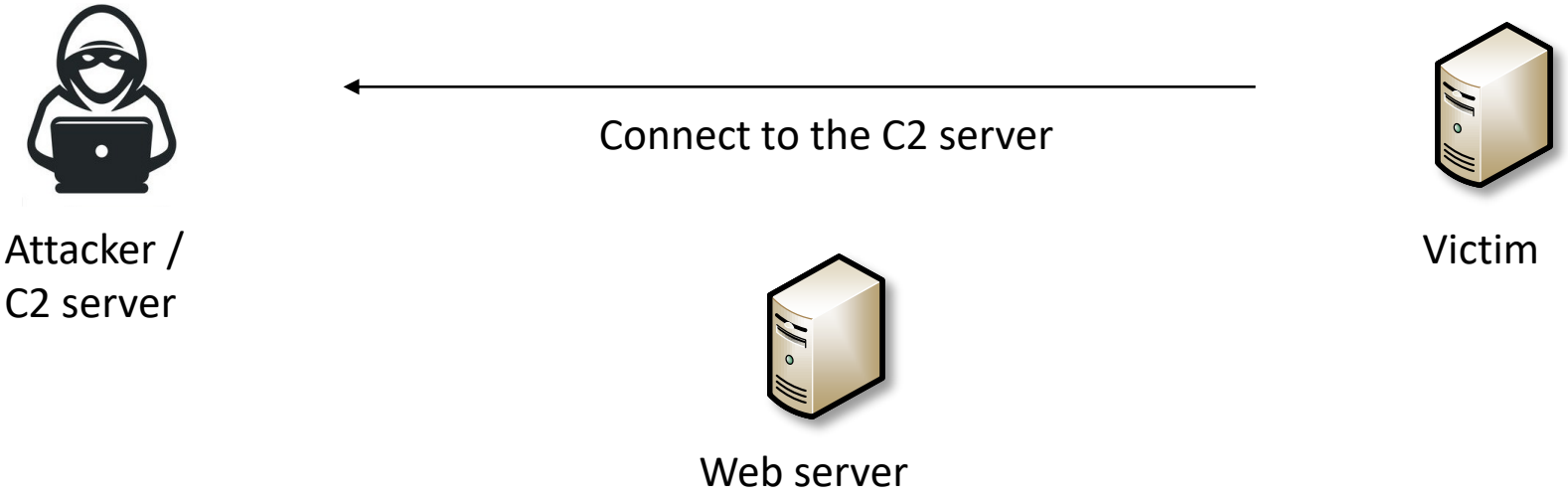
- The victim visits the compromised website and downloads the malicious file
- The downloaded file is a Remote Access Trojan (RAT) that is crafted by the attacker using *msfvenom*[1] tool
- The crafted payload is a “reverse TCP meterpreter” that allows the attacker to establish a reverse shell to the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

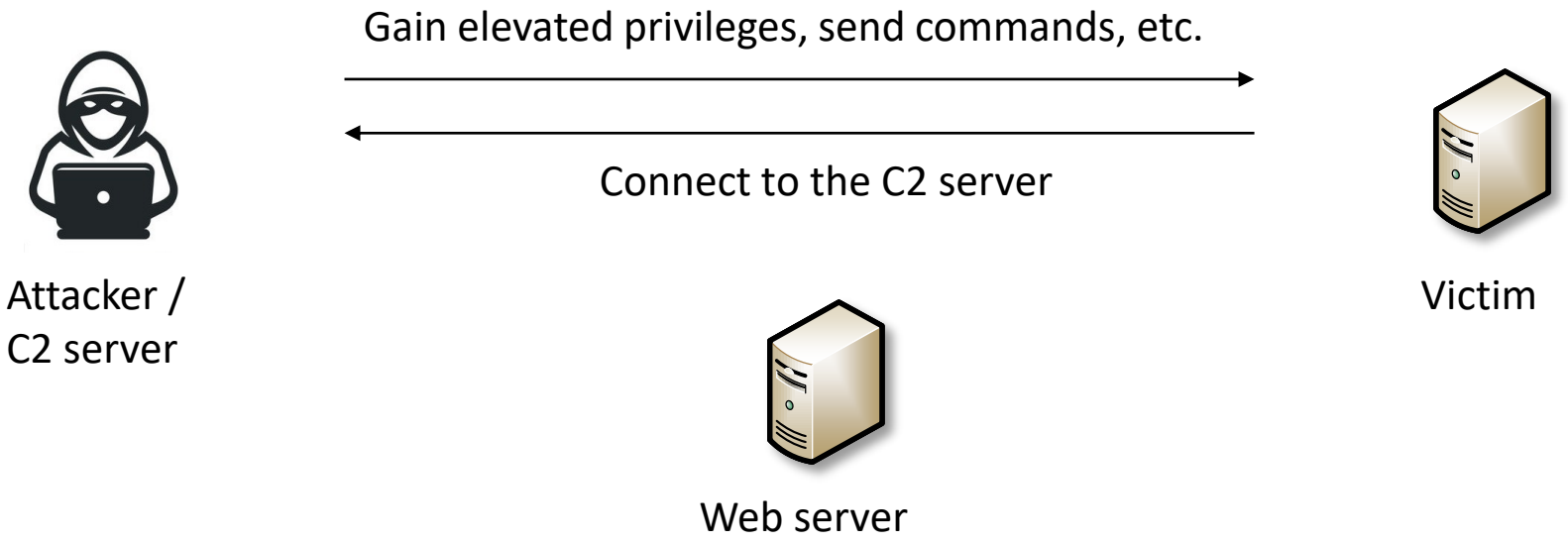
# Attack Scenario

- 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

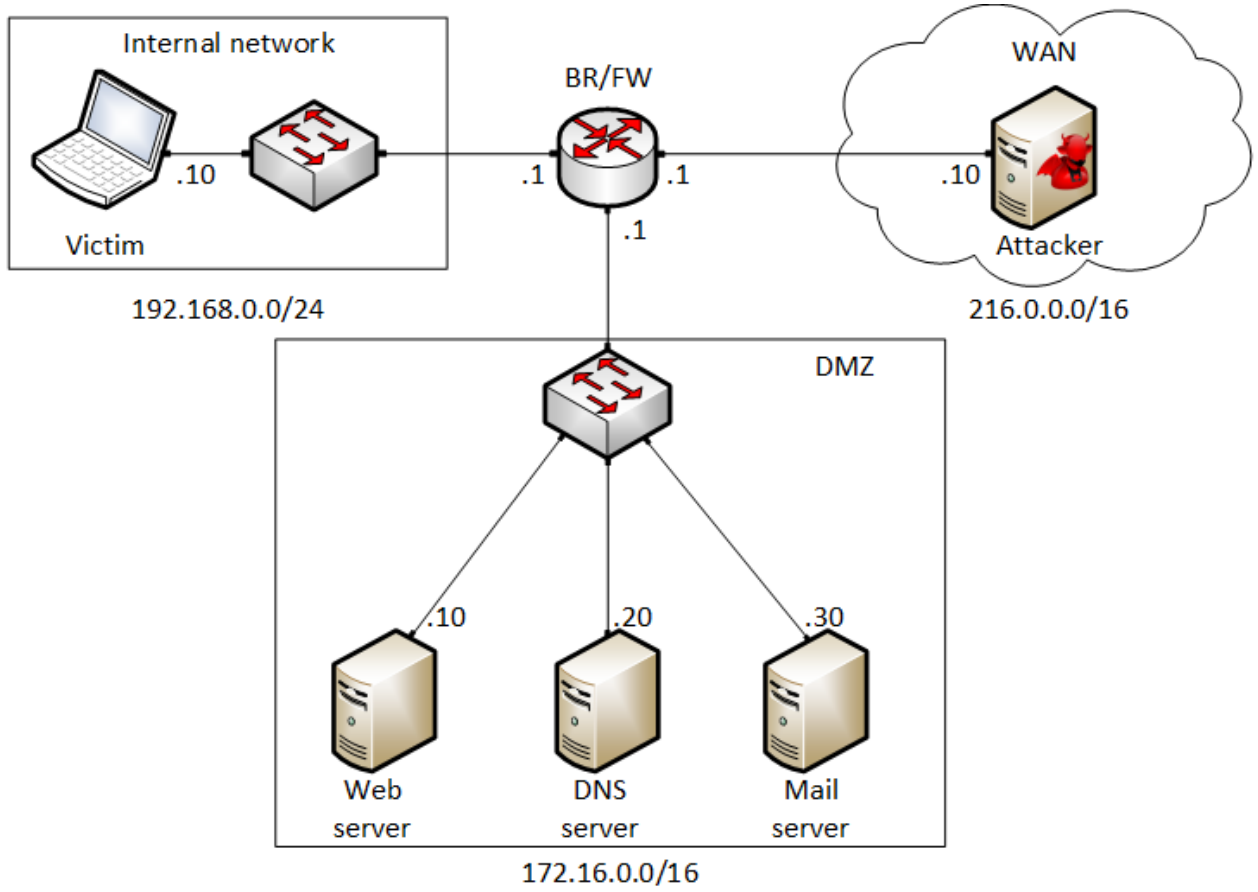
- The attacker gains elevated privileges by tricking the victim into confirming a pop-up dialog (using the *Metasploit* module *windows/local/ask*)
- The attacker installs a backdoor that provides permanent access to the victim's machine (using the *Metasploit* module *windows/local/persistence_service*



# Lab Topology

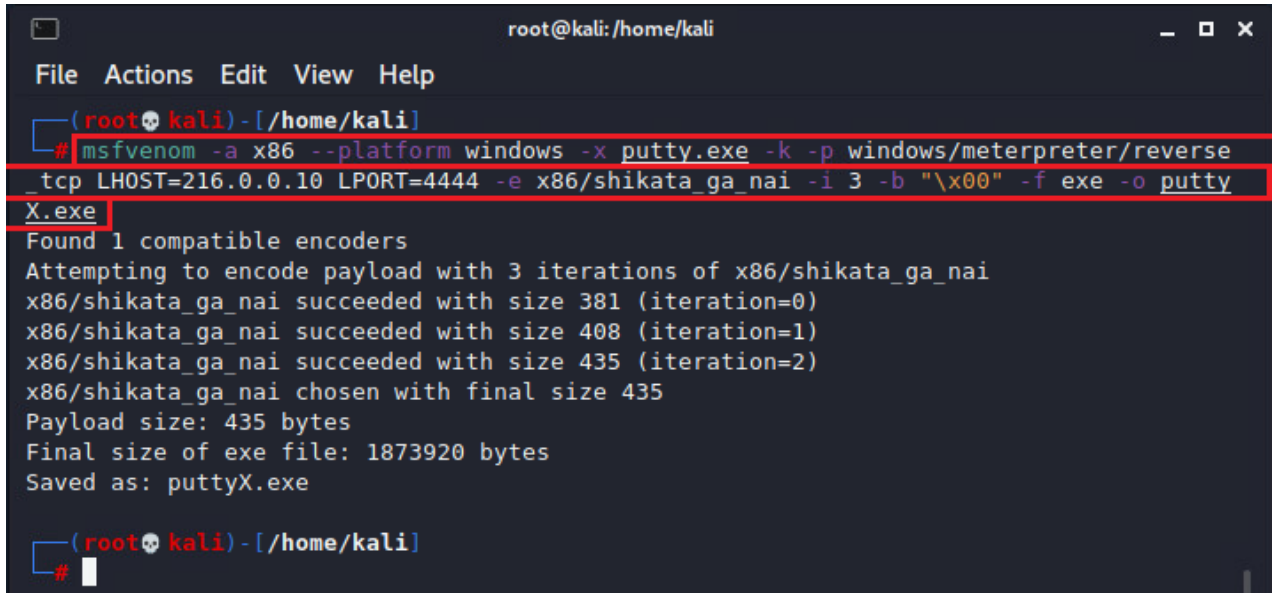
The topology consists of:

- 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

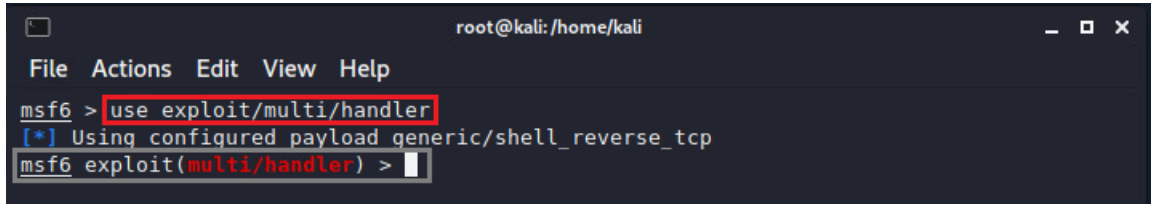


# Weaponization using *msfvenom*

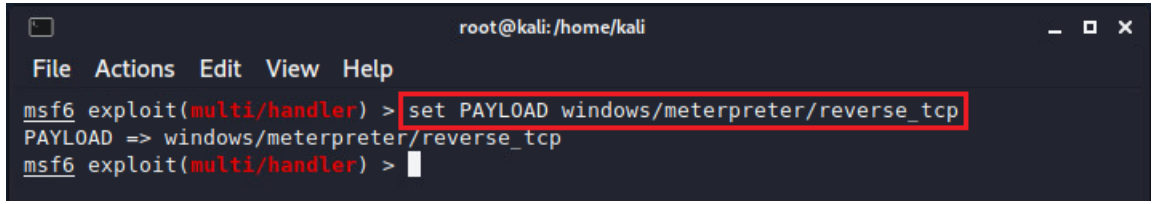
Attacker creates the malicious payload

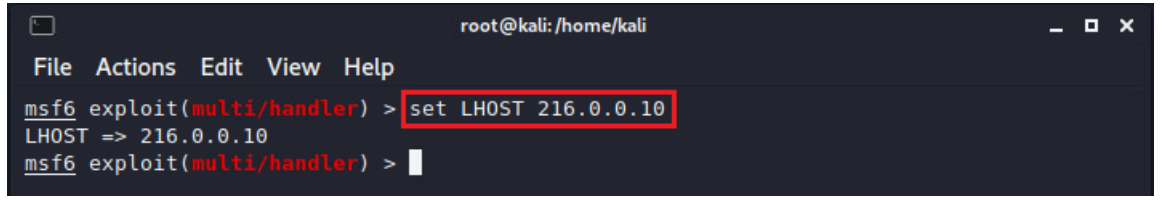



Attacker creates the C2 server to listen for multiple victims



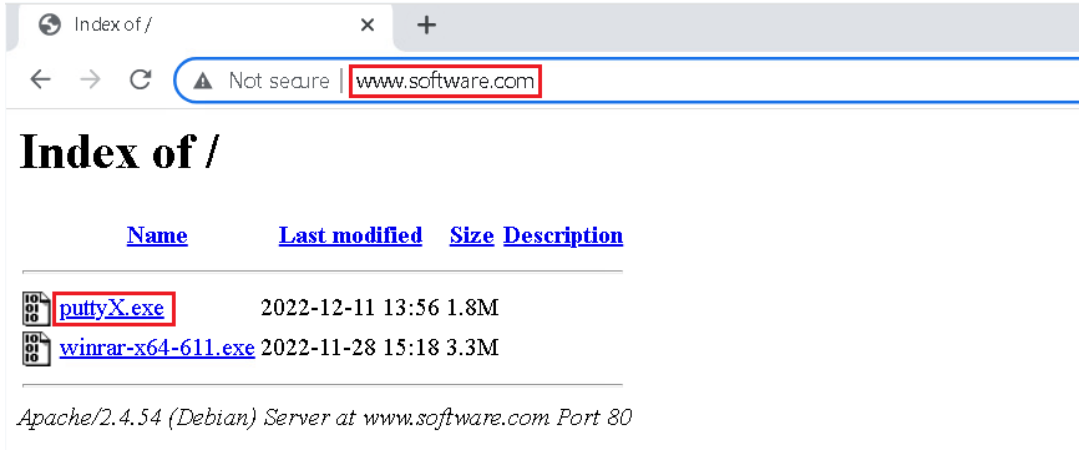

Attacker sets the C2 session configuration



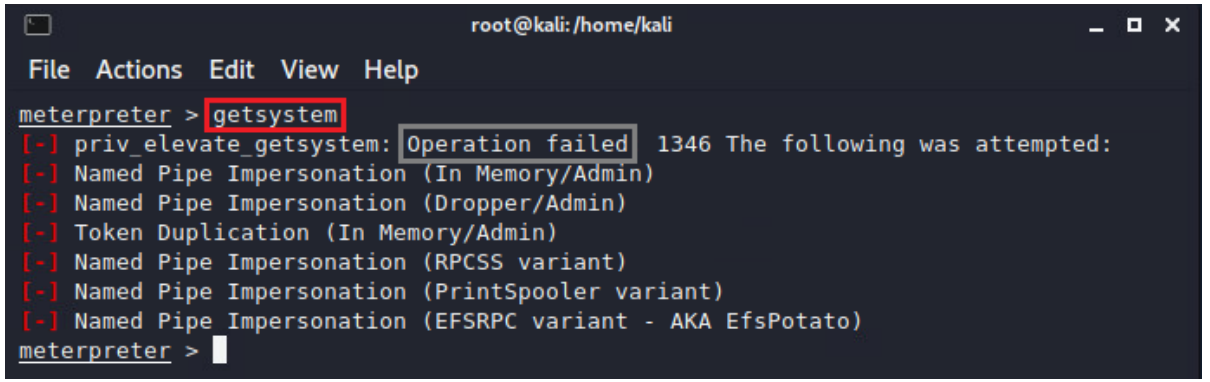



# Weaponization using *msfvenom*

Victim downloads and runs the file from the compromised website

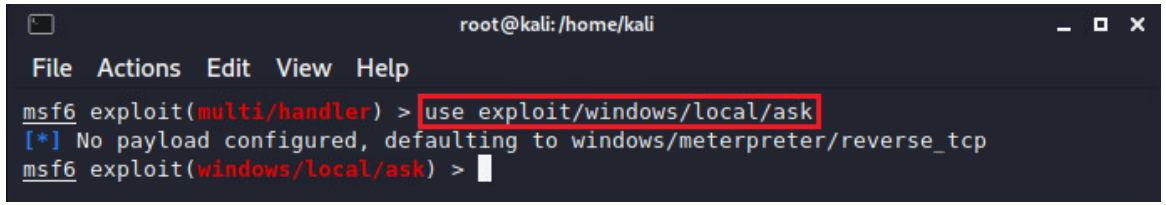



A session is established between the C2 server and the victim. No administrator privileges are given yet

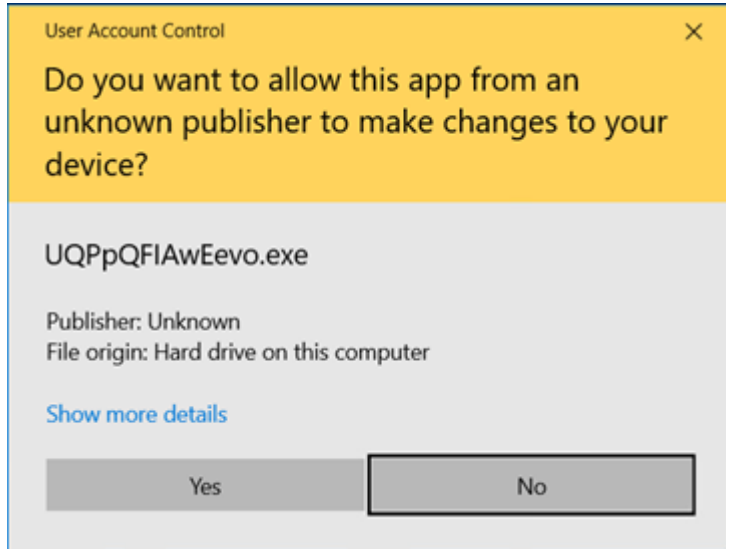


# Privilege Escalation

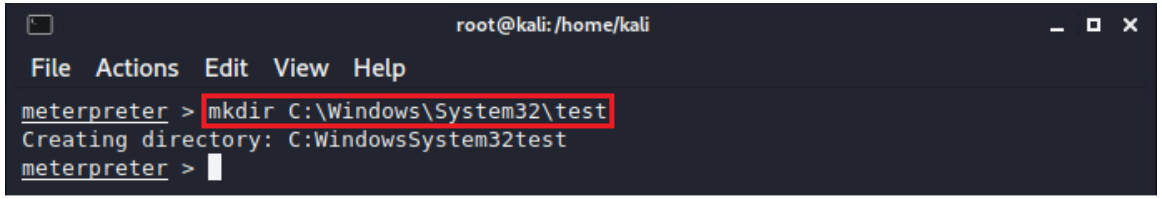
Attacker uses a Metasploit module to ask the user for privilege escalation




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

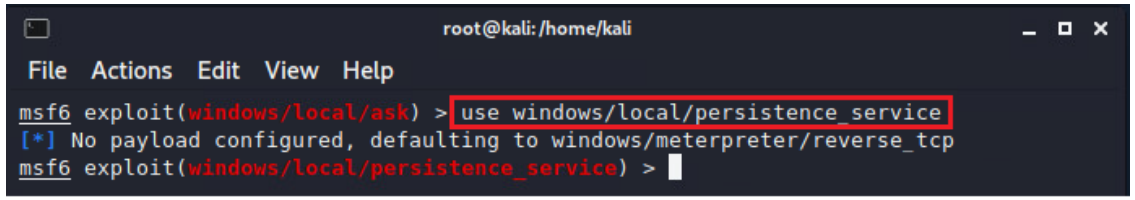



Attacker gains root privileges to the victim's machine

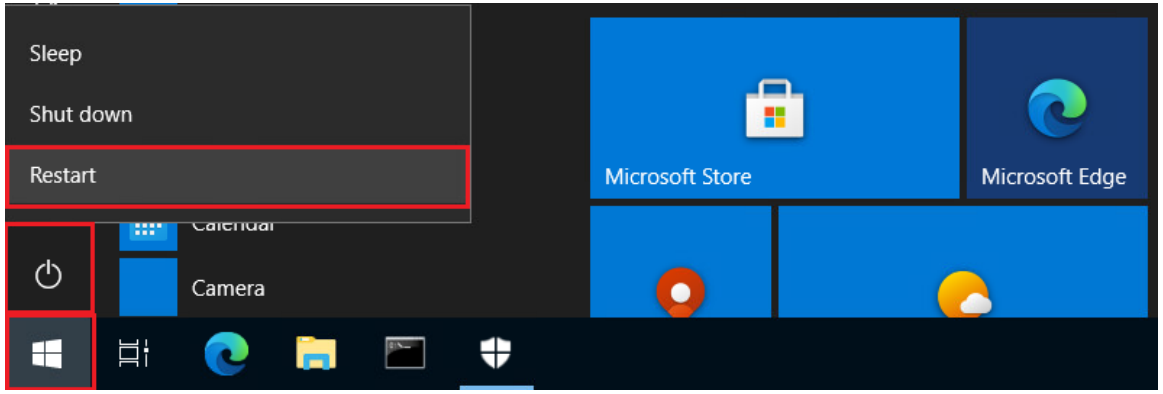


# Privilege Escalation

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




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