|  |  |  |  |
|---|---|---|---|
| Document Reference: | EPRTU-1 | Effective Date: | 10 May 2024 |
| Document Name: | Elevation of Privilege Red Team Usecase | Expiry Date: | 10 May 2025 |

# Elevation of Privilege Red Team Usecases

*Redback Operations*

|  |  |  |  |
|---|---|---|---|
| Document Owner: | Purple Team | Last Modified By: | Liya Thomas |
| Next Review Date: | 17 July 2024 | Last Modified on: | 8 May 2024 |

| Version | Modified By | Approver | Date | Changes made |
|---|---|---|---|---|
| 0.1 | Liya Thomas | | 8 May 2024 | First Draft |
| 0.2 | Joel Daniel | | 10 May 2024 | Cosmetic Changes |
| 1.0 | Liya Thomas | Joel Daniel | 10 May 2024 | Approved for Publishing |
| | | | | |
| | | | | |

# Table of Contents

# 1 Introduction:

In today's rapidly evolving digital landscape, cybersecurity threats continue to pose significant challenges to organizations worldwide. Among the myriad of attack vectors, elevation of privilege attacks stand out as particularly insidious, enabling malicious actors to gain elevated access within systems or networks. This clandestine access empowers attackers to bypass security measures, execute unauthorized actions, and potentially wreak havoc on targeted systems. Understanding the methodologies behind such attacks is paramount for organizations to fortify their defenses effectively.

In this exploration, we delve into five distinct types of elevation of privilege attacks: exploiting vulnerabilities, privilege escalation, social engineering, brute force attacks, and backdoors. For each attack vector, we outline the objectives, tools, and techniques employed by red teams—simulated adversaries—to mimic real-world threats. By comprehensively examining these attack vectors, organizations can enhance their preparedness, fortify their defenses, and mitigate the risk posed by elevation of privilege attacks.

# 2 Privilege Escalation:

## 2.1 Objective:

Elevate privileges by exploiting flaws in system configuration or design.

## 2.2 Steps:

1. Enumeration:

Utilize enumeration tools like enum4linux or PowerSploit to gather detailed information about the target system. This includes enumerating users, groups, shares, services, and other resources that may provide avenues for privilege escalation.

2. Identification of Vulnerabilities:

Leverage exploitation frameworks like PowerUp.ps1 or Windows-Exploit-Suggester to identify potential privilege escalation vulnerabilities within the target system. These tools automate the process of analyzing system configurations and identifying known vulnerabilities that could be exploited to escalate privileges.

3. Exploitation:

Exploit misconfigured permissions, insecure default settings, or known privilege escalation vulnerabilities to elevate privileges within the target system. This may involve exploiting vulnerabilities in system services, applications, or the underlying operating system to gain elevated access rights.

4. Persistence Mechanisms:

Establish persistence mechanisms to maintain elevated privileges even after the initial exploitation. This could involve creating new user accounts with higher privileges, modifying system configurations, or installing persistent backdoors to ensure continued access to the compromised system.

## 2.3 Tools & Techniques:

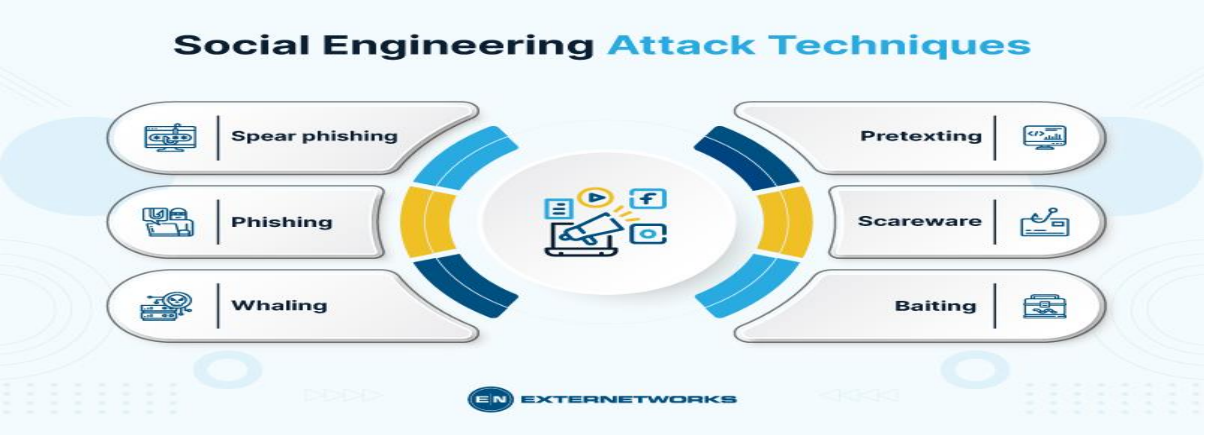
1. Enumeration tools such as enum4linux or PowerSploit are utilized to systematically gather detailed information about the target system, including user accounts, network shares, and system configuration, aiding in identifying potential vulnerabilities and attack vectors.

2. Exploitation frameworks like PowerUp.ps1 or Windows-Exploit-Suggester are employed to automate the discovery of potential privilege escalation vulnerabilities within Windows

environments, facilitating the identification and exploitation of weaknesses to elevate access privileges.

3. Exploiting misconfigured permissions, insecure default settings, or known privilege escalation vulnerabilities involves leveraging weaknesses in system configurations or design flaws to escalate privileges beyond intended levels, granting attackers elevated access to resources and functionalities within the system.

# 3 Social Engineering:



## 3.1 Objective:

Obtain access to privileged accounts or information through manipulation.

## 3.2 Steps:

1. Preparation:

Conduct reconnaissance to gather information about the target individuals or organizations. This includes identifying potential targets, their roles within the organization, and any relevant personal or professional information that could be used in the social engineering attack.

2. Crafting Social Engineering Tactics:

Develop spear-phishing emails with enticing subject lines and content designed to trick recipients into opening malicious attachments or clicking on malicious links. Additionally, prepare phone scripts or scenarios for impersonating trusted individuals or authority figures during phone calls.

3. Execution:

Launch social engineering attacks by sending spear-phishing emails to targeted individuals or making phone calls pretending to be trusted entities. Create fake websites or login pages to steal credentials through phishing attacks. Use pretexting techniques to create plausible scenarios that elicit sensitive information or access from unsuspecting victims.

4. Exploitation of Trust:

Exploit the trust of targeted individuals or organizations to obtain access to privileged accounts or sensitive information. This may involve convincing victims to disclose login credentials, share sensitive information, or download and execute malicious files or scripts.

## 3.3 Tools and techniques

1. Spear-phishing emails: Crafted with tailored content to deceive recipients into opening attachments or clicking on links, often leading to malware installation or credential theft, exploiting human trust and curiosity for malicious purposes.

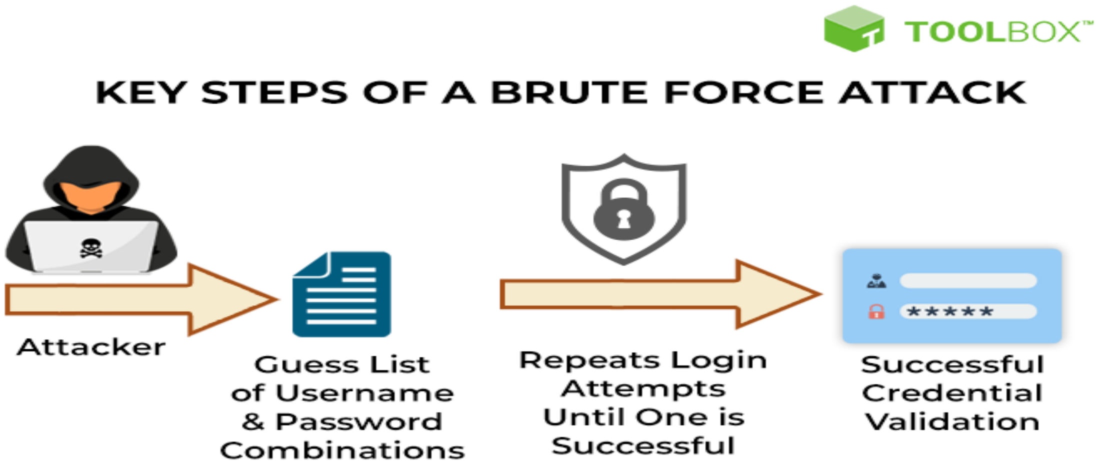
2. Phone calls impersonating trusted figures: Utilized to manipulate victims into divulging sensitive information or performing actions by posing as someone they trust, exploiting human tendency to comply with authority.

3.Fake websites for credential theft: Mimic legitimate sites to trick users into entering login credentials, which are then harvested by attackers for unauthorized access, exploiting users' trust in familiar interfaces and brands.

4. Impersonation via email/social media: Pretend to be trusted individuals or entities in digital communications to manipulate victims into sharing sensitive information or taking harmful actions, exploiting the inherent trust people place in online interactions.

5. Pretexting: Fabricating convincing scenarios or stories to manipulate victims into divulging information or performing actions they wouldn't otherwise, exploiting human desire to be helpful or cooperative in social interactions.

# 4 Brute Force Attacks:


TOOLBOX™
KEY STEPS OF A BRUTE FORCE ATTACK
Attacker
Guess List of Username & Password Combinations
Repeats Login Attempts Until One is Successful
Successful Credential Validation
*****

## 4.1 Objective:

Guess passwords or access tokens to gain elevated privileges.

## 4.2 Steps:

1 . Selection of Target:

Identify target accounts or systems that may grant elevated privileges if compromised. This could include administrative accounts, service accounts, or accounts with high-level access permissions.

2. Brute Force Tool Selection:

Choose appropriate brute force tools like Hydra, Medusa, or THC-Hydra to automate password guessing. Configure the tools to perform brute force attacks against the target accounts or systems using wordlists or dictionaries containing commonly used passwords.

3.Execution:

Launch brute force attacks against the target accounts or systems, systematically attempting different password combinations until a valid credential is found. Employ techniques like slow and low to avoid detection by account lockout mechanisms or intrusion detection systems.

4. Credential Stuffing:

Utilize breached credentials obtained from previous data breaches to perform credential stuffing attacks against the target accounts or systems. This involves systematically testing compromised credentials to gain unauthorized access to the target environment.

### 4.3 Tools & Techniques:

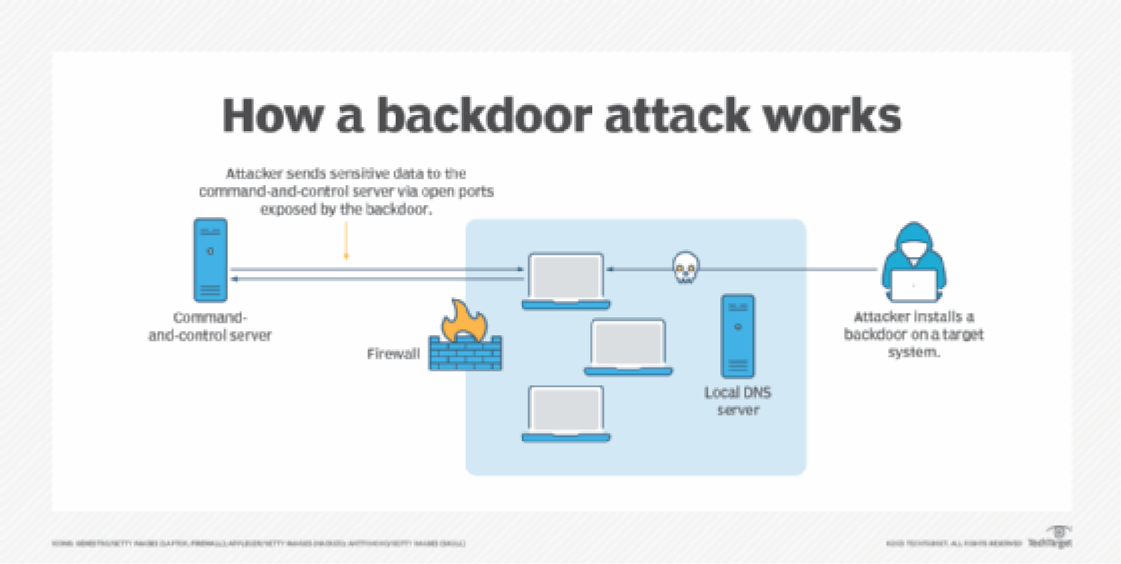
1. Brute force tools such as Hydra, Medusa, or THC-Hydra automate password guessing by systematically trying different combinations until a correct one is found, exploiting weak or default credentials to gain unauthorized access to systems or accounts.

2. Wordlists or dictionaries containing commonly used passwords serve as the foundation for brute force attacks. These lists include frequently used passwords, dictionary words, and common variations, enabling attackers to efficiently guess credentials during password cracking attempts.

3.Credential stuffing attacks leverage breached credentials obtained from previous data breaches. Attackers use these stolen username and password combinations to gain unauthorized access to other accounts or systems where users have reused their compromised credentials.

4. Slow and low technique involves conducting brute force attacks at a slower pace, with fewer attempts per unit of time, to avoid triggering account lockouts or raising suspicion. This stealthy approach helps evade detection by security measures while persistently attempting to guess passwords.

# 5 Backdoors:


How a backdoor attack works
Attacker sends sensitive data to the command-and-control server via open ports exposed by the backdoor.
Command-and-control server
Firewall
Local DNS server
Attacker installs a backdoor on a target system.
TechTarget

## 5.1 Objective:

Install persistent access mechanisms to maintain elevated privileges.

## 5.2 Steps:

1. Selection of Backdoor Tool:

Choose appropriate backdoor tools like Meterpreter or Poison Ivy to establish remote access to the compromised system. Select tools that provide stealthy and persistent access while evading detection by security measures.

2. Installation of Backdoor:

Install the selected backdoor tool on the compromised system using techniques like exploiting vulnerabilities, social engineering, or physical access. Ensure that the backdoor is configured to establish a covert communication channel with the attacker-controlled infrastructure.

3. Persistence Mechanisms:

Implement persistence mechanisms to ensure that the backdoor remains active and undetected even after system reboots or security updates. This may involve modifying system configurations, creating new user accounts, or installing rootkits to hide the presence of the backdoor.

4. Customization:

Customize the backdoor tool to suit the specific requirements of the attack, such as evading antivirus detection, bypassing firewall restrictions, or collecting sensitive information discreetly. Develop custom malware tailored to exploit zero-day vulnerabilities and install stealthy backdoors that are difficult to detect and remove.

## 5.3 Tools & Techniques:

1. Remote access trojans (RATs) like Meterpreter or Poison Ivy provide covert remote access to compromised systems, allowing attackers to execute commands, steal data, and maintain control over targeted environments surreptitiously.

2. Web shells are scripts or programs installed on web servers to enable remote access and control. Attackers use them to execute commands, upload/download files, and maintain persistence on compromised systems.

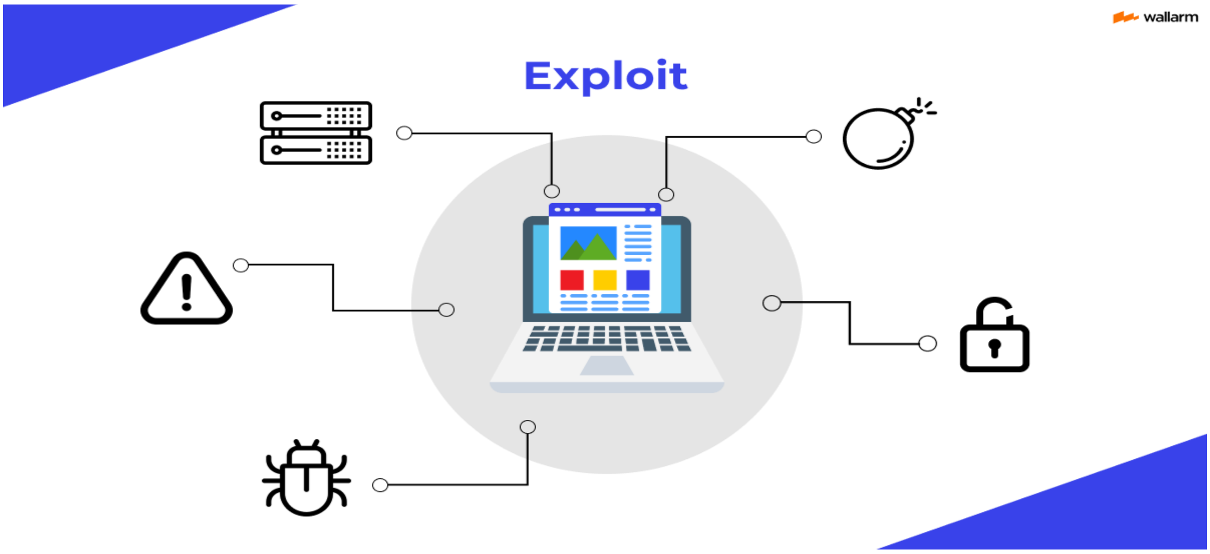
3. Rootkits hide malicious activity by modifying operating system functionality. They enable persistent access and control over compromised systems while evading detection by security tools and concealing their presence from system administrators.

4. Custom malware is specifically designed to evade detection by antivirus software. It employs advanced obfuscation techniques, polymorphism, and encryption to disguise its malicious payload and avoid detection by traditional security measures.

5. Exploiting zero-day vulnerabilities involves leveraging previously unknown security flaws in software to install backdoors or gain unauthorized access. These vulnerabilities provide attackers with a window of opportunity to infiltrate systems before security patches are released.

.

# 6 Exploiting Vulnerabilities



## 6.1 Objective:

The objective of this Red Team exercise is to simulate a real-world cyberattack scenario where the Red Team aims to gain elevated privileges within the target organization's network by exploiting known software vulnerabilities.

## 6.2 Steps:

1. Reconnaissance:

Conduct reconnaissance to gather information about the target organization's network infrastructure, including IP ranges, domain names, and network services. Utilize tools like Nmap, Shodan, and theHarvester to identify potential entry points and attack surfaces.

2. Vulnerability Assessment:

Use vulnerability scanners like Nessus or OpenVAS to perform a comprehensive assessment of the target organization's systems and applications. Identify potential vulnerabilities, misconfigurations, and missing patches that can be exploited by the Red Team.

3. Exploit Identification:

Analyze the results of the vulnerability assessment to identify specific vulnerabilities that can be exploited to gain elevated privileges. Utilize exploit frameworks like Metasploit or Exploit-DB to select appropriate exploits based on the identified vulnerabilities.

4. Exploit Customization:

Customize selected exploits or payloads to suit the target environment and maximize the chances of success. Modify exploit parameters, payload options, or shellcode to evade detection by security measures and achieve the desired objectives.

5. Exploitation:

Launch the selected exploits against the target systems to exploit identified vulnerabilities and gain unauthorized access. Utilize techniques such as buffer overflow, SQL injection, or code injection to compromise target systems and escalate privileges.

6. Privilege Escalation:

Once initial access is gained, escalate privileges to gain elevated access rights within the target organization's network. Exploit additional vulnerabilities or misconfigurations to escalate privileges to administrative or root level.

7. Persistence Establishment:

Establish persistence mechanisms to maintain access to the compromised systems even after the initial exploitation. Install persistent backdoors, create new user accounts, or modify system configurations to ensure continued access and control over the target environment.

8. Post-Exploitation Activities:

Conduct post-exploitation activities to achieve the Red Team's objectives. This may include exfiltrating sensitive data, installing additional malware or tools, or using the compromised systems as pivot points to launch further attacks within the network.

9. Covering Tracks:

Cover tracks to minimize the risk of detection and attribution. Delete logs, remove evidence of the attack, and restore system configurations to their original state to conceal the Red Team's presence and actions.

## 6.3 Tools & Techniques:

1. Reconnaissance: Tools like Nmap, Shodan, and theHarvester gather information about target systems, networks, and services. They identify potential entry points and vulnerabilities, aiding in understanding the target's infrastructure for effective planning.

2. Vulnerability Assessment: Nessus and OpenVAS conduct thorough scans to identify vulnerabilities, misconfigurations, and missing patches within target systems. They provide insights into security weaknesses, enabling proactive remediation to mitigate potential risks.

3. Exploit Identification: Metasploit and Exploit-DB offer a repository of pre-built exploits and vulnerabilities. They aid in identifying and selecting appropriate exploits to target specific vulnerabilities discovered during reconnaissance and vulnerability assessment phases.

4.Exploit Customization: Scripting languages like Python, Ruby, and PowerShell allow for the customization of exploits to suit target environments. This customization enhances exploit effectiveness by tailoring payloads, parameters, and techniques to evade detection and achieve objectives.

5. Exploitation: Metasploit Console and custom scripts execute selected exploits to compromise target systems. They automate the process of launching attacks, exploiting vulnerabilities, and gaining unauthorized access to exploit identified weaknesses within the target environment.

6. Privilege Escalation: Enumeration tools such as enum4linux, Windows-Exploit-Suggester, and PowerUp.ps1 identify additional vulnerabilities or misconfigurations to escalate privileges. They aid in gaining higher access levels, facilitating further compromise within the target infrastructure.

7. Persistence Establishment: Backdoor tools like Meterpreter, Poison Ivy, and Netcat install persistent access mechanisms. They ensure continued access to compromised systems, allowing attackers to maintain control even after initial exploitation.

8. Post-Exploitation Activities: Data exfiltration tools such as Cobalt Strike, Mimikatz, and PowerSploit facilitate the theft of sensitive information. They extract, manipulate, and exfiltrate data from compromised systems to achieve the Red Team's objectives.

9. Covering Tracks: Log cleaners, file deletion tools, and anti-forensic techniques remove evidence of the attack. They help conceal the Red Team's presence, activities, and the impact of the exploitation, minimizing the risk of detection and attribution.

## 7 Conclusion

Elevation of privilege attacks represent a formidable threat landscape that organizations must confront with vigilance and resilience. Through meticulous examination of attack vectors such as exploiting vulnerabilities, privilege escalation, social engineering, brute force attacks, and backdoors, organizations can glean valuable insights into the tactics employed by adversaries. By adopting proactive cybersecurity measures, including robust access controls, ongoing vulnerability assessments, and comprehensive user training, organizations can bolster their defenses against these insidious threats. Moreover, fostering a culture of cybersecurity awareness and collaboration is paramount in safeguarding against the ever-evolving landscape of cyber threats. With concerted efforts and a steadfast commitment to cybersecurity, organizations can navigate the complexities of elevation of privilege attacks and fortify their resilience in an increasingly digital world.

## 8 Reference

Privilege Escalation - https://i.ytimg.com/vi/7PpYavvu-6k/maxresdefault.jpg

Social Engineering - https://www.extnoc.com/learn/wp-content/uploads/2022/10/Social-Engineering.jpg

Brute Force Attacks - https://images.spiceworks.com/wp-content/uploads/2022/05/10131245/Critical-Steps-of-a-Brute-Force-Attack.png

Backdoor - https://cdn.ttgtmedia.com/rms/onlineimages/how_a_backdoor_attack_works-f_mobile.png

Exploiting Vulnerabilities - https://assets.website-files.com/5ff66329429d880392f6cba2/63fe1e3ecc9eae2ce6ab1fb0_185%20Preview.png