Document Reference:	RARTU-1	Effective Date:	29 April 2024
Document Name:	Root Access Red Team Usecase	Expiry Date:	29 April 2025

Root Access Red Team Usecase

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Liya Thomas
Next Review Date:	17 June 2024	Last Modified on:	24 April 2024

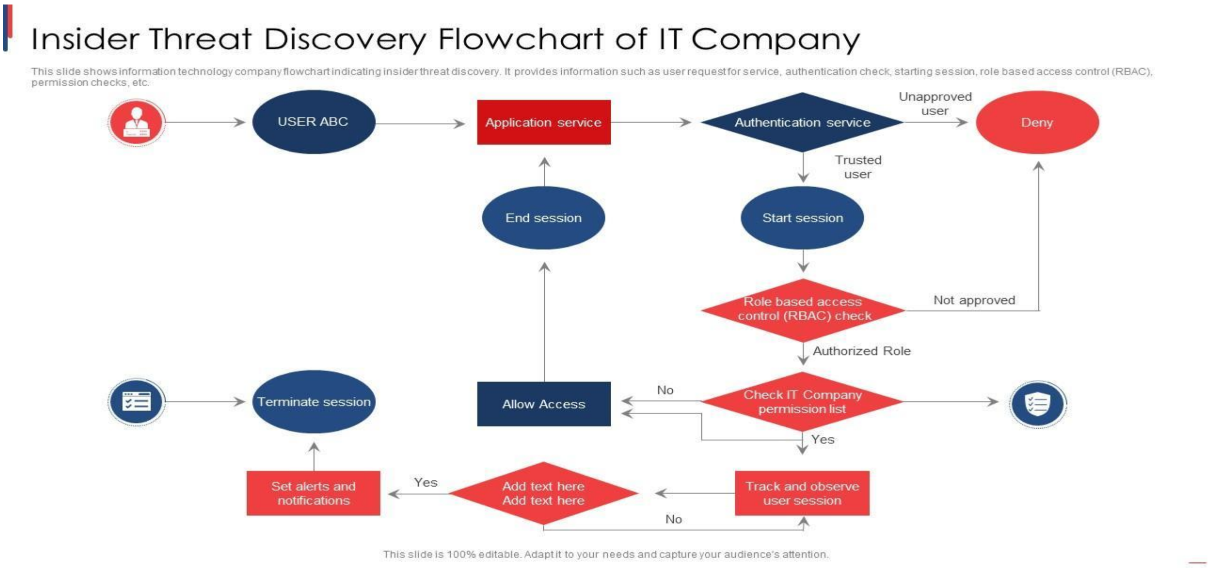
Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas	NA	24 April 2024	Initial Draft
0.2	Joel Daniel		29 April 2024	Cosmetic Changes
1.0	Liya Thomas	Joel Daniel	29 April 2024	Approved for Publishing

Table of Contents

1 Introduction

As part of our red team operations, our goal is to run thorough simulations that gauge the organization's security readiness across different threat scenarios. We'll mimic real-world attack methods to pinpoint weaknesses, defensive shortcomings, and areas needing enhancement. Our simulations cover insider threats, external attacks, data breaches, phishing attempts, ransomware incidents, and credential theft scenarios, all with the aim of gaining root access—the highest level of privilege within the organization's systems. Our findings will offer practical insights to bolster security measures and response strategies.

2 Insider Threat Simulation



Insider Threat Discovery Flowchart of IT Company

This slide shows information technology company flowchart indicating insider threat discovery. It provides information such as user request for service, authentication check, starting session, role based access control (RBAC), permission checks, etc.

USER ABC
Application service
Authentication service
Unapproved user
Deny
Trusted user
End session
Start session
Role based access control (RBAC) check
Not approved
Authorized Role
Terminate session
Allow Access
No
Check IT Company permission list
Yes
Set alerts and notifications
Yes
Add text here Add text here
Track and observe user session
No

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

2.1 Objective:

Our mission in this simulation is to assess how well the organization can fend off attempts by insiders to gain unauthorized access to higher levels of privilege within the system.

2.2 Steps:

1. Research the organization's internal structure, roles, and access levels to identify potential targets: We'll delve deep into the organization's hierarchy, understanding who has access to what, and which positions hold the keys to sensitive information or critical systems. By meticulously analyzing roles and permissions, we aim to pinpoint the most lucrative targets for exploitation.
2. Gain initial access through legitimate means, such as an employee account: We'll start by slipping into the system using methods that insiders might employ, like tricking an employee into revealing their credentials or exploiting weak security protocols. Once inside, we'll blend into the environment, mirroring the behavior of legitimate users to avoid suspicion.
3. Enumerate available privileges and attempt to escalate to root access using techniques like privilege escalation exploits or misconfigurations: Once inside, we'll scrutinize the permissions of the compromised account. We'll then employ tricks such as exploiting loopholes in configurations or using known methods to escalate privileges, inching closer to obtaining root access. By meticulously navigating the system's architecture, we'll seek out vulnerabilities that could lead to elevated privileges.
4. Maintain persistence while avoiding detection by security controls: We'll work to stay hidden within the system, ensuring our actions don't set off any alarm bells. This means erasing our digital footprints, evading security tools like intrusion detection systems, and staying under the radar of security personnel. Through careful evasion and stealthy maneuvers, we'll aim to remain undetected for as long as possible, simulating the persistence of a determined attacker.

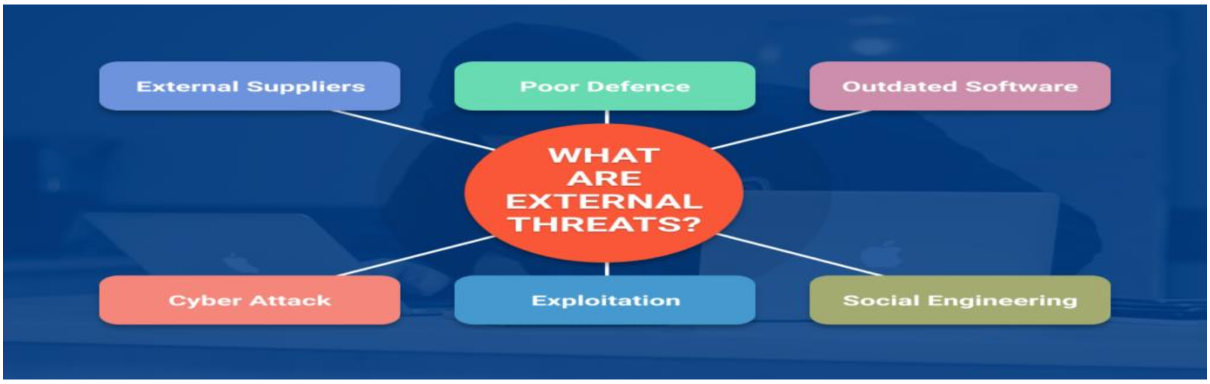
2.3 Tools & Techniques:

- Metasploit: Think of this as our Swiss Army knife. Metasploit offers a range of exploits and tools to help us breach defenses, escalate privileges, and maintain control over compromised systems. With its extensive database of vulnerabilities and automated exploitation capabilities, Metasploit streamlines the process of identifying and exploiting weaknesses in the organization's defenses.
- Mimikatz: This tool is like a master key for stealing credentials. Mimikatz helps us extract login details and perform pass-the-hash attacks, crucial for moving up the privilege ladder. By harvesting credentials from compromised systems, Mimikatz enables us to impersonate legitimate users and gain access to sensitive resources undetected.
- BloodHound: It's our map through the organization's Active Directory. BloodHound lets us visualize trust relationships and find the best paths to escalate privileges,

making our job easier and more efficient. By graphically representing the network's topology and identifying attack paths, BloodHound helps us identify critical assets and prioritize our exploitation efforts.

- PowerShell Empire: This toolkit is our silent partner. With PowerShell Empire, we can execute commands discreetly, maintain control over systems, and slip past traditional security measures with ease. By leveraging PowerShell's scripting capabilities, PowerShell Empire enables us to evade detection by antivirus software and execute sophisticated attacks with minimal traceability.

3 External Attack Simulation:



3 .1 Objective

Our goal in this simulation is to evaluate how well the organization can withstand external threats attempting to gain root access to its systems.

3.2 Steps:

1. Conduct reconnaissance to gather information about the organization's external-facing assets, such as websites, servers, and applications: We'll start by scouting out the organization's digital footprint, identifying all publicly accessible assets. This involves scouring the internet for information on websites, servers, and applications that could serve as potential entry points for attackers.
2. Identify vulnerabilities using automated scanners or manual testing: Once we have a clear picture of the organization's external assets, we'll use tools like Nmap and Nessus to scan for vulnerabilities. These tools will help us identify weaknesses in the

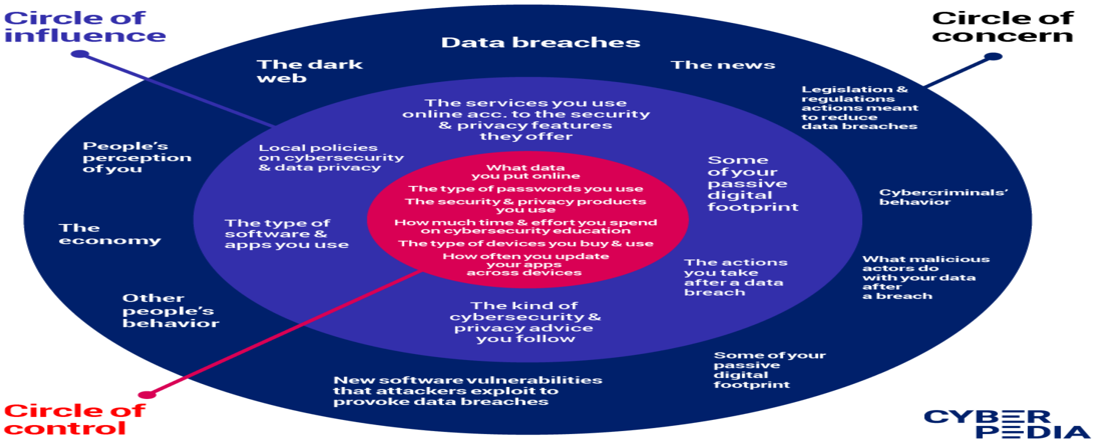
organization's defenses, such as outdated software versions or misconfigurations that could be exploited by attackers.

3. Exploit vulnerabilities to gain initial access to the network or systems: With a list of vulnerabilities in hand, we'll leverage tools like Metasploit and Burp Suite to exploit them and gain a foothold into the organization's network or systems. This could involve launching targeted attacks against specific vulnerabilities, such as exploiting unpatched software or misconfigured services.
4. Escalate privileges to root level by exploiting weaknesses in authentication mechanisms or misconfigurations: Once inside the network, our next step is to escalate our privileges to gain root access. We'll use techniques like brute force attacks with Hydra or exploiting weaknesses in authentication mechanisms to elevate our privileges and gain full control over the organization's systems.

3.3 Tools & Techniques:

- Nmap: This powerful network scanning tool helps us map out the organization's external infrastructure, identifying open ports, services, and potential vulnerabilities. By providing detailed insights into the organization's network topology, Nmap enables us to prioritize our attack vectors effectively.
- Nessus: Nessus is a comprehensive vulnerability scanner that automates the process of identifying security weaknesses in the organization's external assets. By conducting thorough vulnerability assessments, Nessus helps us identify potential entry points for exploitation and assess the organization's overall security posture.
- Burp Suite: Burp Suite is a versatile web application security testing tool that enables us to identify and exploit vulnerabilities in web applications. With features like proxying, scanning, and exploitation, Burp Suite allows us to uncover security flaws such as SQL injection and cross-site scripting (XSS) that could be leveraged by attackers.
- Metasploit: Metasploit is a penetration testing framework that provides a wide range of exploits and payloads for gaining unauthorized access to systems. By leveraging its extensive database of exploits, Metasploit enables us to launch targeted attacks against vulnerable systems and escalate our privileges to gain root access.
- Hydra: Hydra is a popular password-cracking tool that helps us perform brute force attacks against authentication mechanisms, such as login screens and web forms. By systematically guessing passwords, Hydra enables us to exploit weak or default credentials and gain unauthorized access to systems.

4 Data Breach Simulation:


Circle of influence
Circle of concern
Data breaches
The dark web
The news
Legislation & regulations actions meant to reduce data breaches
People's perception of you
The services you use online acc. to the security & privacy features they offer
Local policies on cybersecurity & data privacy
Some of your passive digital footprint
What data you put online
The type of passwords you use
The security & privacy products you use
How much time & effort you spend on cybersecurity education
The type of devices you buy & use
How often you update your apps across devices
Cybercriminals' behavior
The economy
The type of software & apps you use
The actions you take after a data breach
What malicious actors do with your data after a breach
Other people's behavior
The kind of cybersecurity & privacy advice you follow
Some of your passive digital footprint
New software vulnerabilities that attackers exploit to provoke data breaches
Circle of control
CYBERPEDIA

4.1 Objective

Our objective in this simulation is to evaluate the organization's ability to detect and respond to unauthorized access leading to data exfiltration.

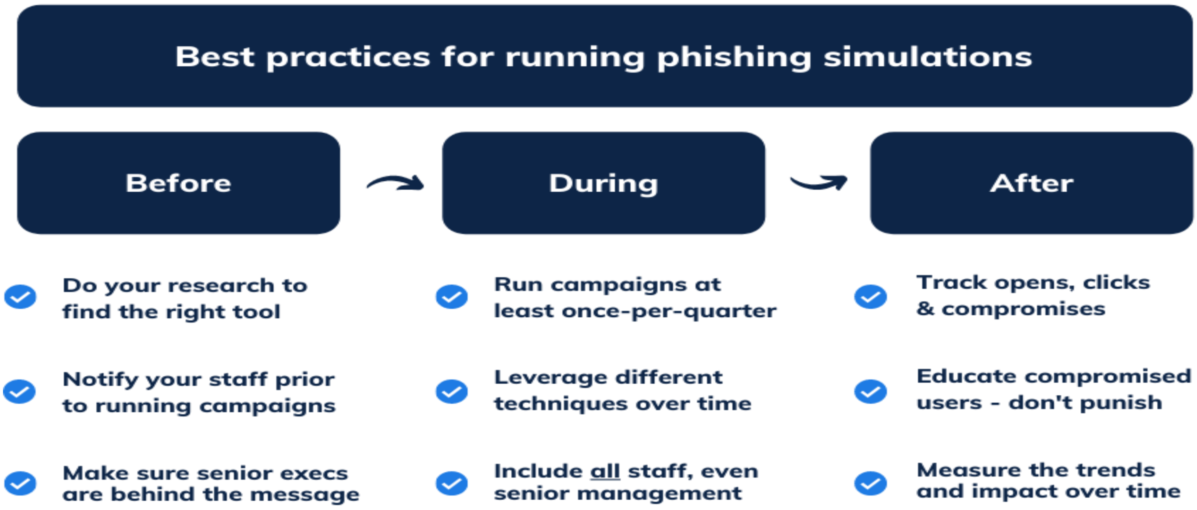
4.2 Steps:

1. Gain initial access to sensitive systems or databases: We'll begin by infiltrating the organization's network or systems through various means, such as exploiting vulnerabilities or compromising user credentials. Our aim is to gain a foothold in sensitive areas where valuable data is stored.
2. Identify and exfiltrate valuable data without triggering detection mechanisms: Once inside, we'll carefully identify and extract valuable data without raising suspicion. This could involve searching for databases containing sensitive information or accessing file servers where confidential documents are stored.
3. Cover tracks to avoid detection, such as deleting logs or modifying timestamps: To evade detection, we'll take steps to cover our tracks and erase any evidence of our activities. This might include deleting log files, altering timestamps, or using anti-forensic techniques to make it difficult for investigators to trace our actions.

4.3 Tools & Techniques:

- Cobalt Strike: Cobalt Strike is a powerful penetration testing tool that provides advanced capabilities for post-exploitation activities, including data exfiltration. With its built-in command and control (C2) framework, Cobalt Strike allows us to maintain control over compromised systems and exfiltrate data stealthily.
- Wireshark: Wireshark is a network protocol analyzer that enables us to capture and inspect network traffic in real-time. By monitoring network communications, Wireshark helps us identify and extract sensitive data being transmitted over the network, such as login credentials or confidential documents.
- rsync: rsync is a file synchronization tool that can be abused for data exfiltration purposes. By leveraging its ability to transfer files between systems, we can exfiltrate large volumes of data from compromised servers to external locations without attracting attention.
- Data exfiltration frameworks: These frameworks provide a set of tools and techniques for exfiltrating data from compromised systems using various covert channels. By encrypting data and disguising it within legitimate network traffic or file transfers, these frameworks enable us to bypass security controls and evade detection.
- Data exfiltration over encrypted channels: Encrypting data before exfiltration helps conceal sensitive information from detection mechanisms, making it harder for defenders to identify and block unauthorized data transfers.
- File transfer protocols: Leveraging protocols like FTP, SCP, or HTTP, we can securely transfer stolen data from compromised systems to external servers without raising suspicion. By encrypting data during transit, we can further enhance the security of the exfiltration process.

5 Phishing Incident Simulation:



Best practices for running phishing simulations

Before → **During** → **After**

Before:
- ✓ Do your research to find the right tool
- ✓ Notify your staff prior to running campaigns
- ✓ Make sure senior execs are behind the message

During:
- ✓ Run campaigns at least once-per-quarter
- ✓ Leverage different techniques over time
- ✓ Include all staff, even senior management

After:
- ✓ Track opens, clicks & compromises
- ✓ Educate compromised users - don't punish
- ✓ Measure the trends and impact over time

5.1 Objective:

Our aim in this simulation is to assess how well the organization's email security measures and user awareness training can defend against phishing attacks, a common vector for cyber threats.

5.2 Steps:

1. Craft convincing phishing emails designed to trick employees into divulging credentials or executing malicious payloads: We'll meticulously design phishing emails tailored to appear legitimate and compelling, enticing employees to take action. These emails may mimic official communication from trusted sources or present urgent scenarios to prompt immediate response.
2. Distribute phishing emails to targeted employees or departments: Using tools like GoPhish and the Social-Engineer Toolkit (SET), we'll execute the distribution phase. We'll target specific individuals or departments within the organization, tailoring the phishing emails to match their roles or interests. This targeted approach enhances the likelihood of successful deception.
3. Capture credentials entered by users who fall for the phishing emails: As recipients interact with the phishing emails and provide their credentials, we'll capture this sensitive information using techniques like Evilginx. This tool intercepts and logs

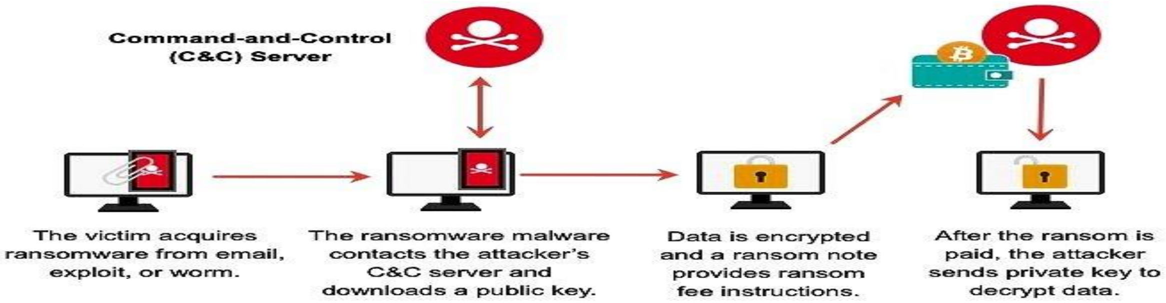
login credentials entered by unsuspecting users, allowing us to harvest valuable data for further exploitation.

4. Use obtained credentials to gain access to sensitive systems or escalate privileges to root level: With the harvested credentials in hand, we'll attempt to infiltrate sensitive systems or escalate privileges within the organization's network. Techniques such as spear phishing and credential harvesting enable us to bypass security measures and gain unauthorized access. This step demonstrates the potential consequences of successful phishing attacks, highlighting the importance of robust security measures and user vigilance.

5.3 Tools & Techniques:

- GoPhish: GoPhish is a phishing simulation and training platform that allows us to create and execute realistic phishing campaigns. It provides templates for crafting convincing phishing emails and features for tracking recipient interactions. GoPhish enables us to assess the organization's susceptibility to phishing attacks and measure the effectiveness of user awareness training.
- Social-Engineer Toolkit (SET): SET is a comprehensive toolkit for social engineering attacks, including phishing. It provides a range of tools and modules for crafting and delivering phishing emails, as well as conducting credential harvesting and other malicious activities. SET facilitates the automation of phishing campaigns and enhances their success rate.
- Evilginx: Evilginx is a tool specifically designed for intercepting and logging user credentials obtained through phishing attacks. It operates as a man-in-the-middle proxy, capturing login credentials entered by users and storing them for later retrieval. Evilginx enables us to demonstrate the ease with which attackers can harvest credentials from unsuspecting users, emphasizing the need for robust authentication mechanisms and user education.

6 Ransomware Attack Simulation:



Command-and-Control (C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware malware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends private key to decrypt data.

6.1 Objective

Our objective in this simulation is to evaluate the organization's readiness to prevent, detect, and respond to ransomware attacks that target root access, thereby safeguarding critical systems and data.

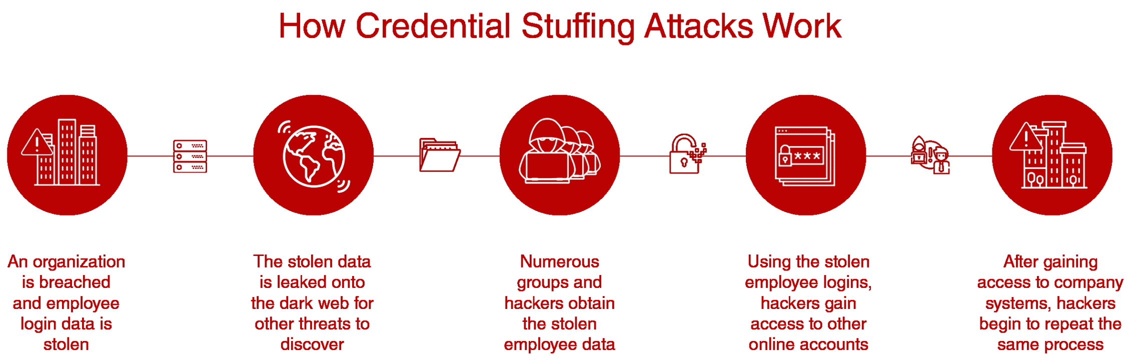
6.2 Steps:

1. Gain initial access to the network or systems through phishing or exploiting vulnerabilities: To initiate the attack, we'll first establish a foothold within the organization's network or systems. This could involve exploiting vulnerabilities discovered during reconnaissance or leveraging phishing techniques to trick employees into executing malicious payloads.
2. Deploy ransomware payloads across the organization's infrastructure: Once inside the network, we'll deploy ransomware payloads across various endpoints and servers. These payloads are carefully crafted to encrypt files and systems rapidly, maximizing the impact of the attack and rendering critical data inaccessible to legitimate users.
3. Encrypt critical files and systems, including those with root access: Our primary objective is to encrypt critical files and systems, including those with root access privileges. By targeting these assets, we aim to disrupt the organization's operations significantly and exert pressure on decision-makers to comply with ransom demands.
4. Demand ransom payment and monitor the organization's response: Following the encryption phase, we'll deliver ransom notes to the organization's administrators, demanding payment in exchange for decryption keys. Throughout this process, we'll monitor the organization's response and assess its effectiveness in containing the attack, negotiating with threat actors, and restoring operations.

6.3 Tools & Techniques:

- Cobalt Strike: Cobalt Strike serves as our primary command and control (C2) framework, enabling us to execute malicious activities stealthily and maintain persistence within the organization's network. It provides a range of capabilities for post-exploitation, including fileless malware deployment and lateral movement techniques.
- Locky, WannaCry, CryptoLocker: These are examples of ransomware families commonly used in simulated attacks. Each variant is designed to encrypt files using strong encryption algorithms, making decryption without the proper key practically impossible. By deploying these ransomware payloads strategically, we can maximize the impact on the organization's systems and data.
- Malicious payload delivery: We'll leverage various delivery methods, such as phishing emails or exploit kits, to distribute ransomware payloads across the organization's infrastructure. By disguising malicious payloads as legitimate files or documents, we increase the likelihood of successful execution and infection.
- Lateral movement: To maximize the scope of the attack, we'll employ lateral movement techniques to propagate the ransomware across the organization's network. This could involve exploiting vulnerabilities in unpatched systems or abusing legitimate tools and protocols to move laterally between endpoints and servers.
- Encryption of files and directories: Ransomware payloads are programmed to encrypt files and directories using strong encryption algorithms, rendering them inaccessible to legitimate users. By encrypting critical data, including those with root access privileges, we aim to disrupt the organization's operations and increase the urgency of ransom payment.

7 Credential Theft Simulation:


How Credential Stuffing Attacks Work
An organization is breached and employee login data is stolen
The stolen data is leaked onto the dark web for other threats to discover
Numerous groups and hackers obtain the stolen employee data
Using the stolen employee logins, hackers gain access to other online accounts
After gaining access to company systems, hackers begin to repeat the same process

7.1 Objective:

Our objective in this simulation is to evaluate the organization's ability to withstand credential theft attacks, which can lead to unauthorized access to sensitive systems and escalation of privileges to root level.

7.2 Steps:

1. Use various methods such as phishing, keylogging, or password spraying to steal employee credentials: We'll employ a variety of tactics to steal employee credentials, including phishing emails designed to trick users into revealing their login credentials, keyloggers installed on compromised systems to capture keystrokes, and password spraying attacks that attempt to guess weak passwords.
2. Test stolen credentials to identify accounts with elevated privileges, including root access: Once we have obtained credentials through our chosen methods, we'll test them to identify accounts with elevated privileges, such as those with root access. This involves querying the organization's authentication systems to determine the level of access associated with the stolen credentials.
3. Attempt to gain access to sensitive systems or escalate privileges using stolen credentials: With the stolen credentials verified and accounts with elevated privileges identified, we'll attempt to gain access to sensitive systems or escalate privileges within the organization's network. This may involve exploiting weaknesses in authentication mechanisms or misconfigurations to achieve root access.

7.3 Tools & Techniques:

- Mimikatz: Mimikatz is a powerful tool used for extracting plaintext passwords, hashes, and other credentials from compromised systems. It enables us to perform credential dumping, allowing us to harvest credentials stored in memory or on disk, including those associated with accounts with elevated privileges.
- LaZagne: LaZagne is another credential recovery tool that specializes in retrieving passwords stored on local systems. It supports various applications and platforms, making it useful for extracting credentials from a wide range of sources.
- CrackMapExec: CrackMapExec is a versatile post-exploitation tool that enables us to perform credential-based attacks across Windows networks. It supports functionalities such as brute force attacks, credential dumping, and lateral movement, making it valuable for testing the organization's resilience against credential theft.
- Hydra: Hydra is a popular password-cracking tool that supports multiple protocols and services, allowing us to conduct brute force attacks against authentication mechanisms. By systematically guessing passwords, Hydra helps us test the strength of user credentials and assess the organization's susceptibility to password-based attacks.
- Credential dumping: Credential dumping refers to the extraction of authentication credentials from compromised systems. Techniques like Mimikatz and LaZagne facilitate credential dumping by retrieving plaintext passwords, hashes, and other credential data stored on target systems.
- Brute force attacks: Brute force attacks involve systematically guessing passwords until the correct one is found. Tools like Hydra enable us to automate this process and test the strength of user passwords across various services and protocols.

8 Conclusion

The red team simulations have given us important insights into how well the organization can handle and respond to threats aiming for root access. We've pinpointed areas where our access controls, privilege management, incident response procedures, and employee awareness need improvement. These findings will help us bolster our defenses, proactively implement security measures, and better defend against ever-changing cyber threats. As the threat landscape evolves, ongoing red team exercises will be crucial to keeping the organization ready and alert to new risks.

9 References

Insider Threat- https://www.slideteam.net/media/catalog/product/cache/1280x720/i/n/insider_threat_discovery_flowchart_of_it_company_slide01.jpg

External Threat - https://securetriad.io/wp-content/uploads/2021/06/What-are-External-Threats-1024x640.png

Data Breaches- https://blogapp.bitdefender.com/cyberpedia/content/images/2021/11/Data-Breaches.png

Ransomware Attack Simulation - https://images.squarespace-cdn.com/content/v1/5a05e672fe54ef1b4ad127a0/341d2dd4-3c37-4a11-9c5d-d719d3edd55f/how-ransomware-works.jpg

Phising Simulation - https://blog.usecure.io/hs-fs/hubfs/Phishing%20simulation%20best%20practices.png?width=1500&name=Phishing%20simulation%20best%20practices.png

Credential Stuffing Attack - https://foresite.com/wp-content/uploads/2021/02/credential-stuffing-vector-v8-1.png