Introduction to penetration testing

With the onboarding of devices no the cyberspace comes the increase in complexities and attack vectors which has led to a rise in the importance of security. Security such that we are protecting devices which hold a magnitude of personal identifiable information. This information includes names of people, security numbers, passwords etc.Johnson (2020) defines penetration testing as an objectifiable testing activity that tries to validate an item against a checklist to ensure that it meets the defined criterias. Wilhelm (2010) identifies the thought process of penetration tests as attacking systems with penetration testing tools and goes further to identify there is more to the concept. Saqib and Moon (2023) details the problems facing network security which lead to data breach as a function of authentication and privacy issues and also give a classification for penetration testing which can be divided into

1. White box testing: this is penetration testing in which the organization's information is given to the tester . Also known as Overt security testing by NIST.
2. Black box; in this testing methodology the tester is completely left in the dark, also known as covert by NIST. its purpose is to replicate the impact an adversary might have on an organization in the most rudimentary way.
3. Gray-Box testing: this is a methodology in which the Tester has partial knowledge of organizations information

In this work we will consider penetration testing as a step by step objectified approach to validate a system against a checklist. The checklist employed is the National Institute of Standards and Technology special publication 800 115(NIST SP 800 115) although there are others like Open Source Security Testing Methodology Manual (OSSTMM) etc. This simulation will be considered a white box testing and we will not be following the guidelines strictly due to the nature of the assessment.

THE ENVIRONMENT

The scope/environment of this simulated network pentest is going to encompass a network consisting of 4 physical endpoint devices, 5 if the logical topology is considered. Among this devices we have

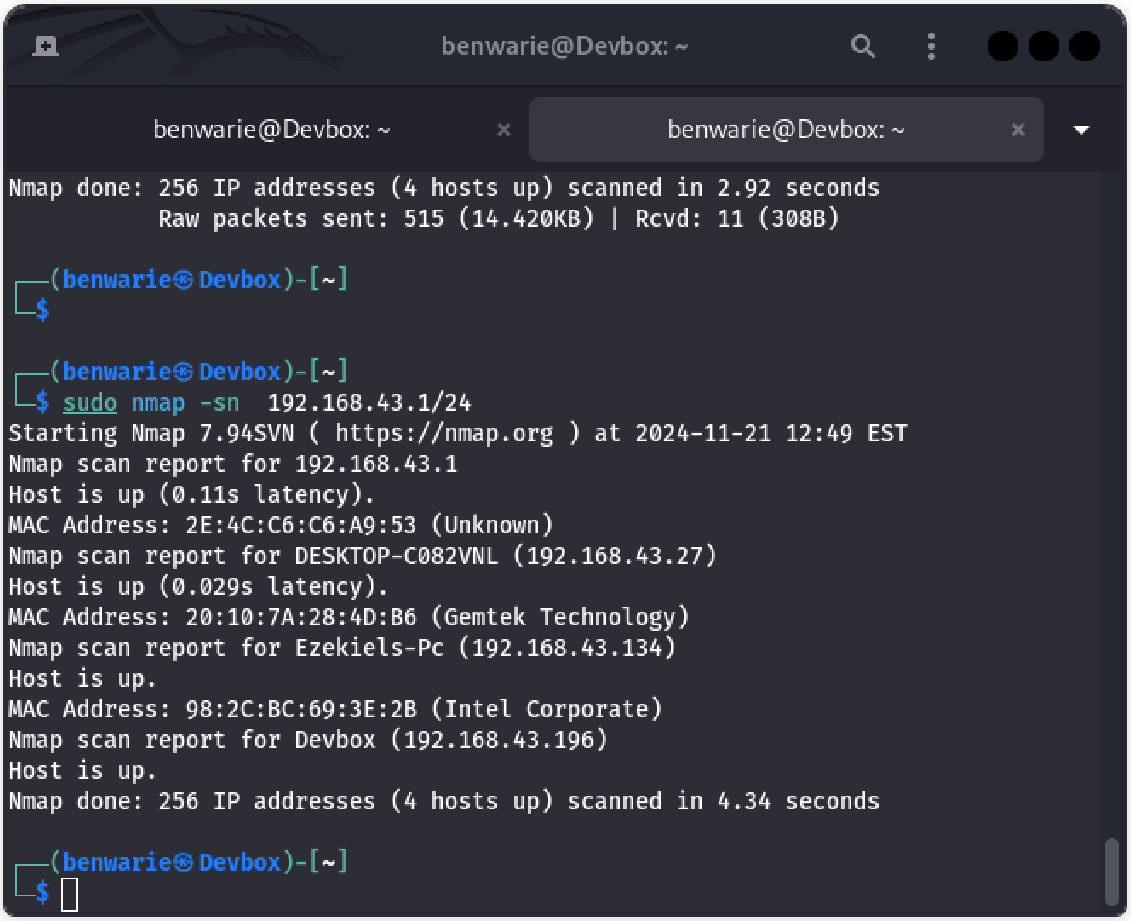
1. A mobile device doubling as the access point/router(galaxy s9)(192.168.43.1/24)
2. Desktop 1 (our server DESKTOP-C082VNL)(192.168.43.27/24)
3. Desktop 3 (hosting our Kali Linux our attacker, Devbox (192.168.43.196) and doubling as another server)

The topology below shows the physical and logical topology of our simulated network.

Using the Nist sp 800 115 we begin at network discovery. Our tool of choice to discover hosts on the network include nmap and netdiscover. Below is the output of our nmap scan. The available host in our network include:

1. 192.168.43.27/24 DESKTOP-C082VNL (192.168.43.27)MAC Address: 20:10:7A:28:4D:B6 (Gemtek Technology)
2. 192.168.43.1/24 MAC Address: 2E:4C:C6:C6:A9:53 (Unknown)
3. 192.168.43.196/24 Devbox (192.168.43.196)
4. 192.168.43.134/24 Ezekiels-Pc (192.168.43.134) MAC Address: 98:2C:BC:69:3E:2B (Intel Corporate)

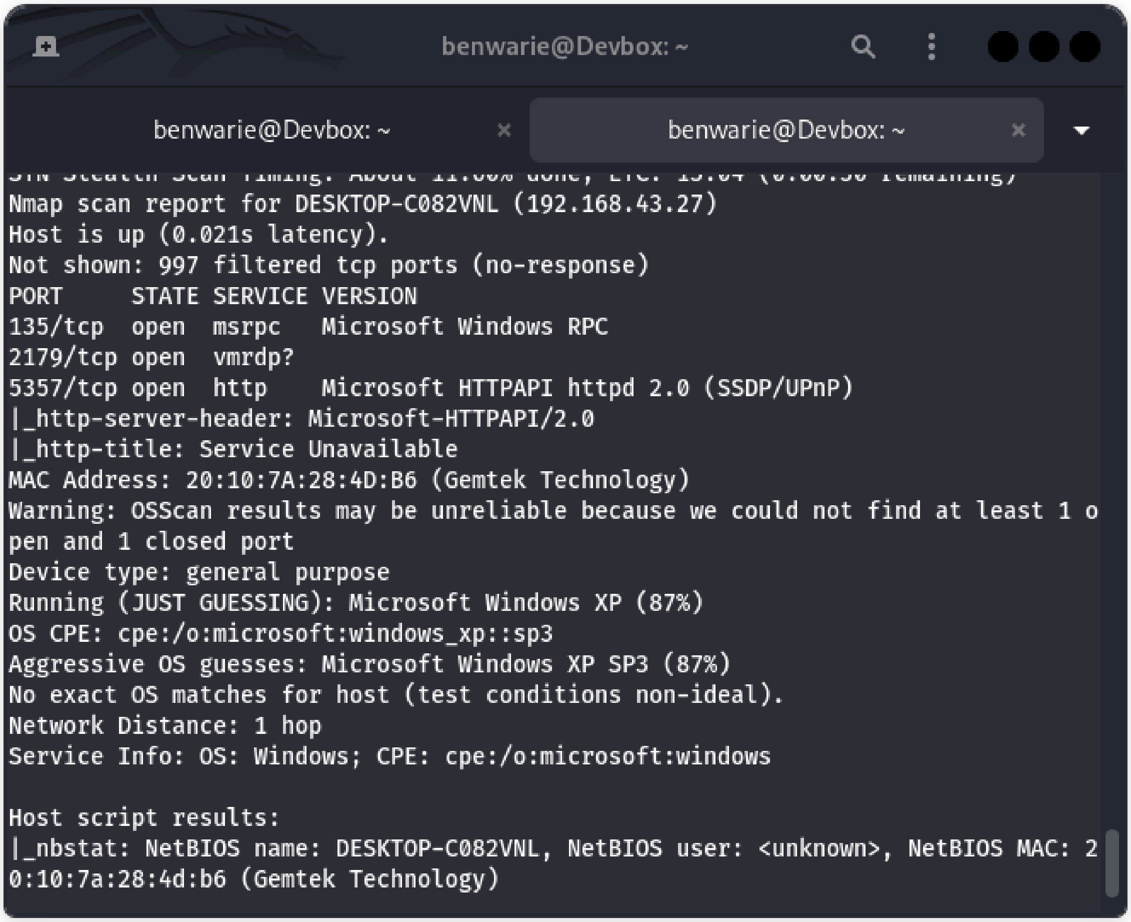
Below is a screen shot from nmap which shows our host.



```
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.92 seconds
           Raw packets sent: 515 (14.420KB) | Rcvd: 11 (308B)

┌──(benwarie㉿Devbox)-[~]
└─$

┌──(benwarie㉿Devbox)-[~]
└─$ sudo nmap -sn  192.168.43.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 12:49 EST
Nmap scan report for 192.168.43.1
Host is up (0.11s latency).
MAC Address: 2E:4C:C6:C6:A9:53 (Unknown)
Nmap scan report for DESKTOP-C082VNL (192.168.43.27)
Host is up (0.029s latency).
MAC Address: 20:10:7A:28:4D:B6 (Gemtek Technology)
Nmap scan report for Ezekiels-Pc (192.168.43.134)
Host is up.
MAC Address: 98:2C:BC:69:3E:2B (Intel Corporate)
Nmap scan report for Devbox (192.168.43.196)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.34 seconds

┌──(benwarie㉿Devbox)-[~]
└─$ 
```

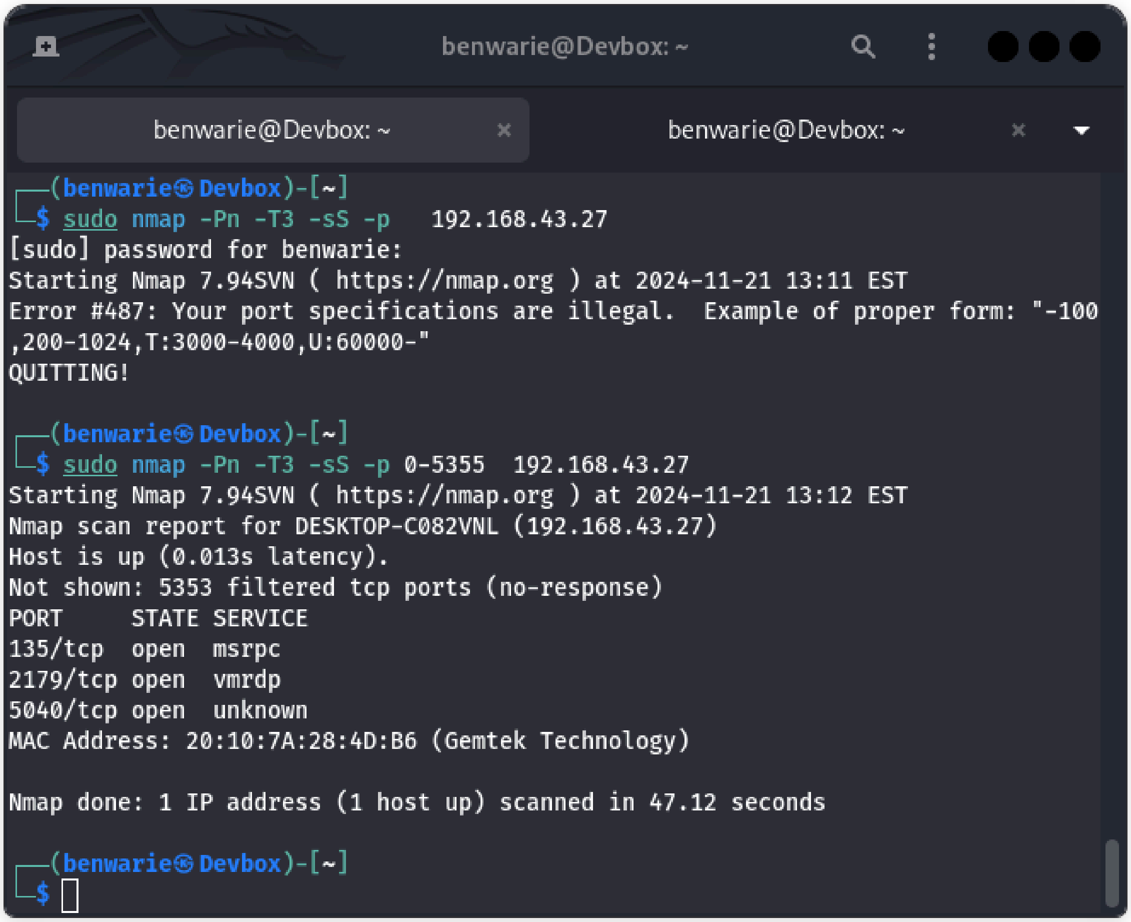
Network Port and Service Identification

Overview of the Vulnerability Identified and tools used to identify it.
The scope of our pentest has been limited to 192.168.43.27/24 DESKTOP-C082VNL (192.168.43.27)MAC Address: 20:10:7A:28:4D:B6 (Gemtek Technology). We proceed to identify the open ports and services running on this machine. The tool we will achieve this with is nmap which is a very robust tool in penetration testing. Below is the nmap output for open ports, os and banner information.



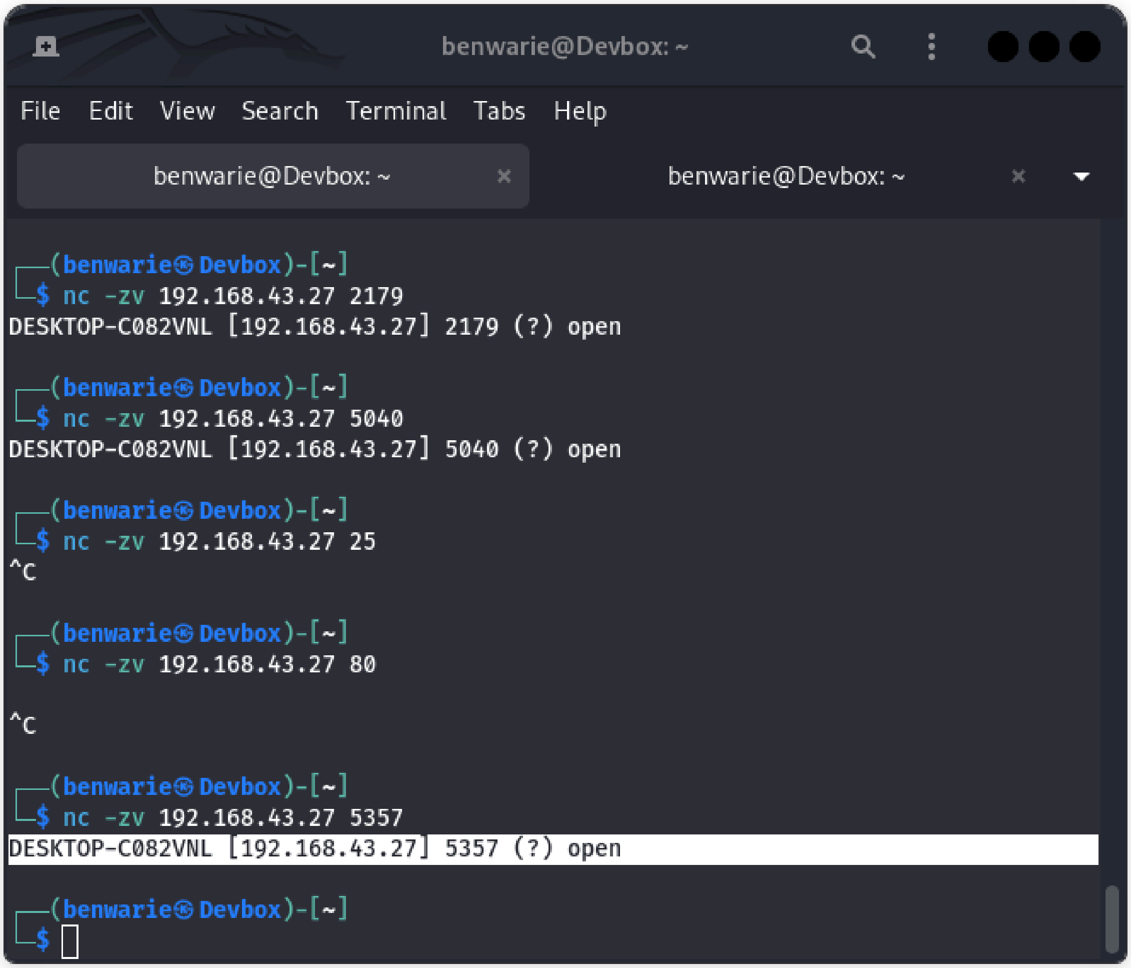
```
SYN Stealth Scan Timing: About 11.00% done; ETC: 13:04 (0:00:36 remaining)
Nmap scan report for DESKTOP-C082VNL (192.168.43.27)
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
135/tcp  open  msrpc   Microsoft Windows RPC
2179/tcp open  vmrdp?
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 20:10:7A:28:4D:B6 (Gemtek Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-C082VNL, NetBIOS user: <unknown>, NetBIOS MAC: 2
0:10:7a:28:4d:b6 (Gemtek Technology)
```

From this scan we discover our target has 3 ports open including port 135/tcp running msrpc, port 2179/tcp running vmrdp and port 5357/tcp running http and they are all open. We can also ascertain that the device is running the Windows operating system. Additionally port 5040? Tcp running an unknown service was discovered when a deeper search was conducted with nmap.

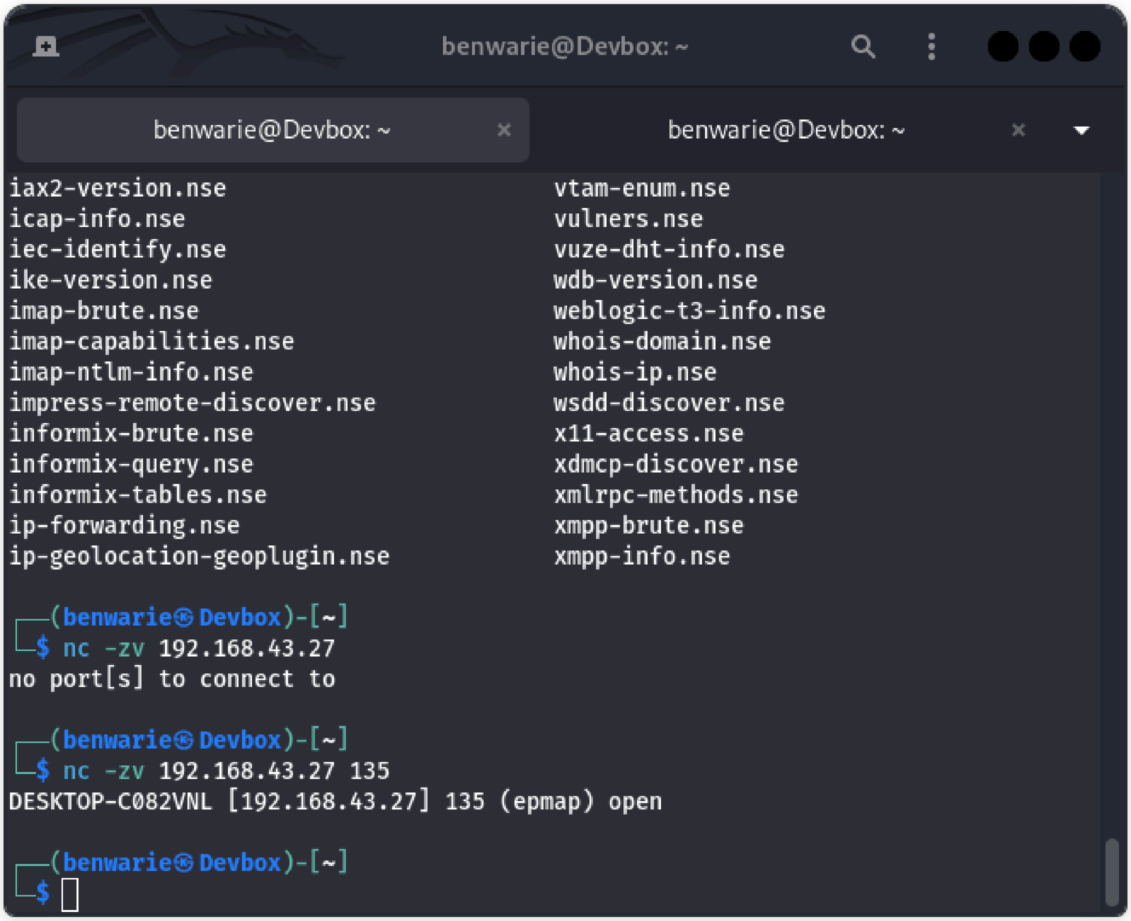


```
┌──(benwarie㉿Devbox)-[~]
└─$ sudo nmap -Pn -T3 -sS -p   192.168.43.27
[sudo] password for benwarie:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 13:11 EST
Error #487: Your port specifications are illegal.  Example of proper form: "-100
,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(benwarie㉿Devbox)-[~]
└─$ sudo nmap -Pn -T3 -sS -p 0-5355  192.168.43.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 13:12 EST
Nmap scan report for DESKTOP-C082VNL (192.168.43.27)
Host is up (0.013s latency).
Not shown: 5353 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
5040/tcp open  unknown
MAC Address: 20:10:7A:28:4D:B6 (Gemtek Technology)

Nmap done: 1 IP address (1 host up) scanned in 47.12 seconds

┌──(benwarie㉿Devbox)-[~]
└─$ 
```

Futhter enumeration of individual open ports with netcat revealed no new information.



```
┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 2179
DESKTOP-C082VNL [192.168.43.27] 2179 (?) open

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 5040
DESKTOP-C082VNL [192.168.43.27] 5040 (?) open

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 25
^C

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 80

^C

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 5357
DESKTOP-C082VNL [192.168.43.27] 5357 (?) open

┌──(benwarie㉿Devbox)-[~]
└─$ 
```

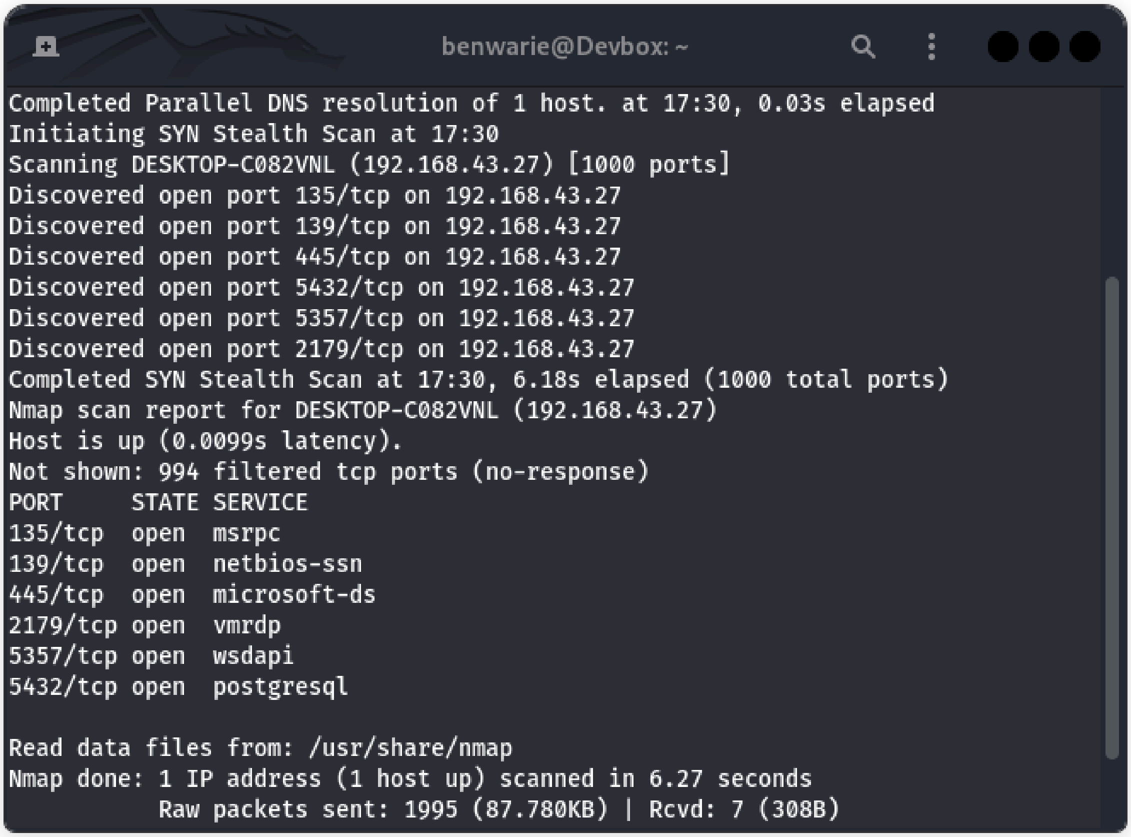


```
iax2-version.nse                        vtam-enum.nse
icap-info.nse                           vulners.nse
iec-identify.nse                        vuze-dht-info.nse
ike-version.nse                         wdb-version.nse
imap-brute.nse                          weblogic-t3-info.nse
imap-capabilities.nse                   whois-domain.nse
imap-ntlm-info.nse                      whois-ip.nse
impress-remote-discover.nse             wsdd-discover.nse
informix-brute.nse                      x11-access.nse
informix-query.nse                      xdmcp-discover.nse
informix-tables.nse                     xmlrpc-methods.nse
ip-forwarding.nse                       xmpp-brute.nse
ip-geolocation-geoplugin.nse            xmpp-info.nse

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27
no port[s] to connect to

┌──(benwarie㉿Devbox)-[~]
└─$ nc -zv 192.168.43.27 135
DESKTOP-C082VNL [192.168.43.27] 135 (epmap) open

┌──(benwarie㉿Devbox)-[~]
└─$ 
```

Below is reconnaissance output using netcat

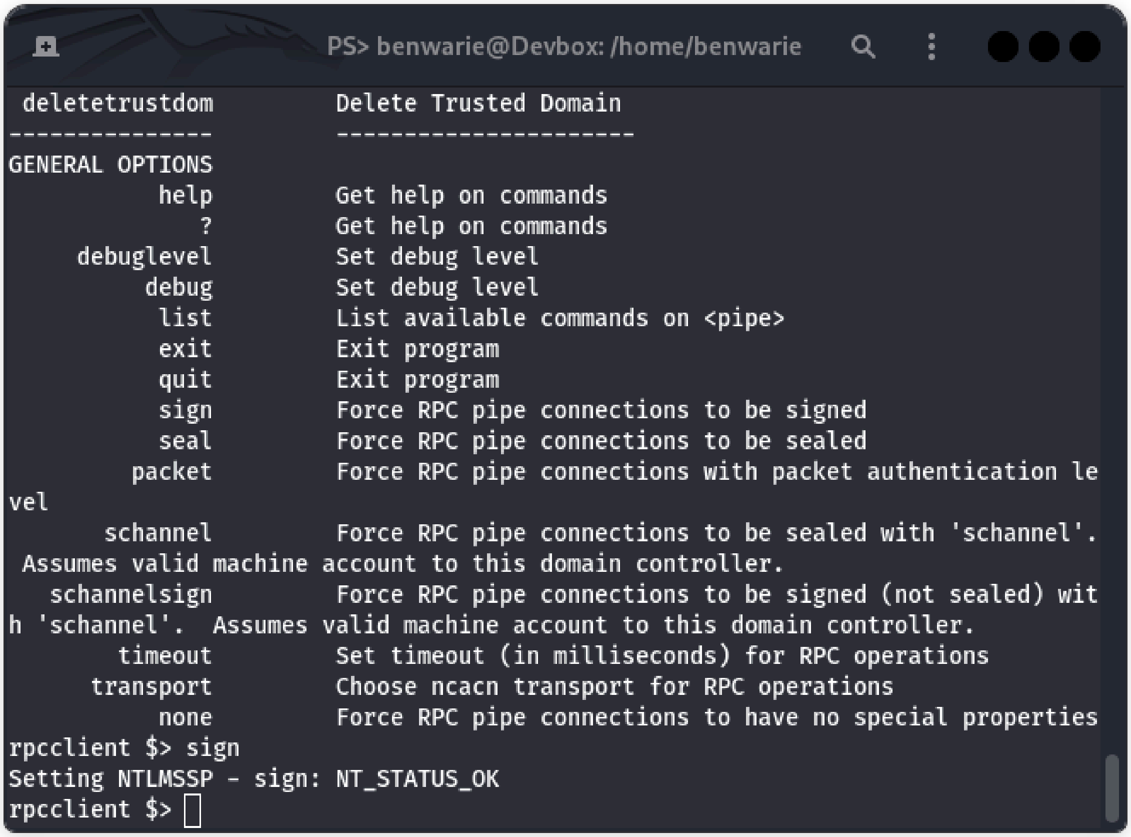
1. DESKTOP-C082VNL [192.168.43.27] 135 (epmap) open
2. DESKTOP-C082VNL [192.168.43.27] 5357 (?) open
3. DESKTOP-C082VNL [192.168.43.27] 5040 (?) open
4. DESKTOP-C082VNL [192.168.43.27] 2179 (?) open

A later assessment with Nmap revealed we have a postgresql server running on the target machine listening on port 5432

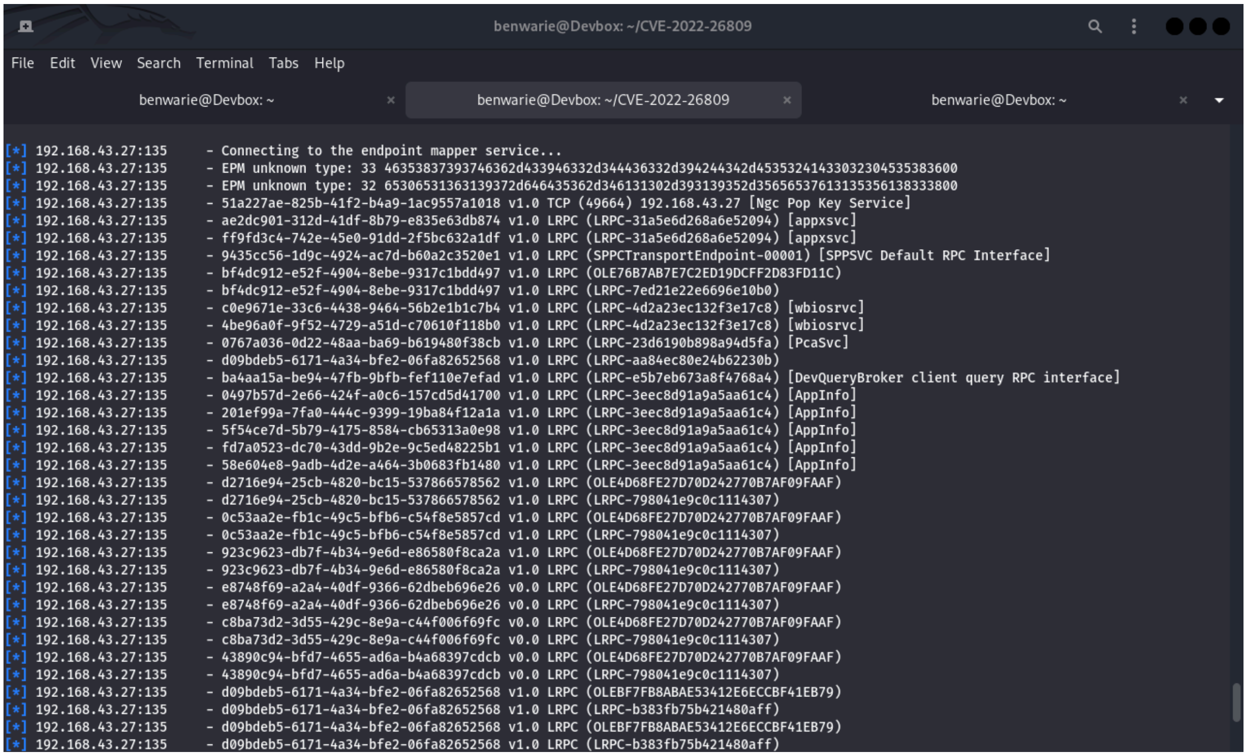


```
Completed Parallel DNS resolution of 1 host. at 17:30, 0.03s elapsed
Initiating SYN Stealth Scan at 17:30
Scanning DESKTOP-C082VNL (192.168.43.27) [1000 ports]
Discovered open port 135/tcp on 192.168.43.27
Discovered open port 139/tcp on 192.168.43.27
Discovered open port 445/tcp on 192.168.43.27
Discovered open port 5432/tcp on 192.168.43.27
Discovered open port 5357/tcp on 192.168.43.27
Discovered open port 2179/tcp on 192.168.43.27
Completed SYN Stealth Scan at 17:30, 6.18s elapsed (1000 total ports)
Nmap scan report for DESKTOP-C082VNL (192.168.43.27)
Host is up (0.0099s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi
5432/tcp open  postgresql

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
           Raw packets sent: 1995 (87.780KB) | Rcvd: 7 (308B)
```

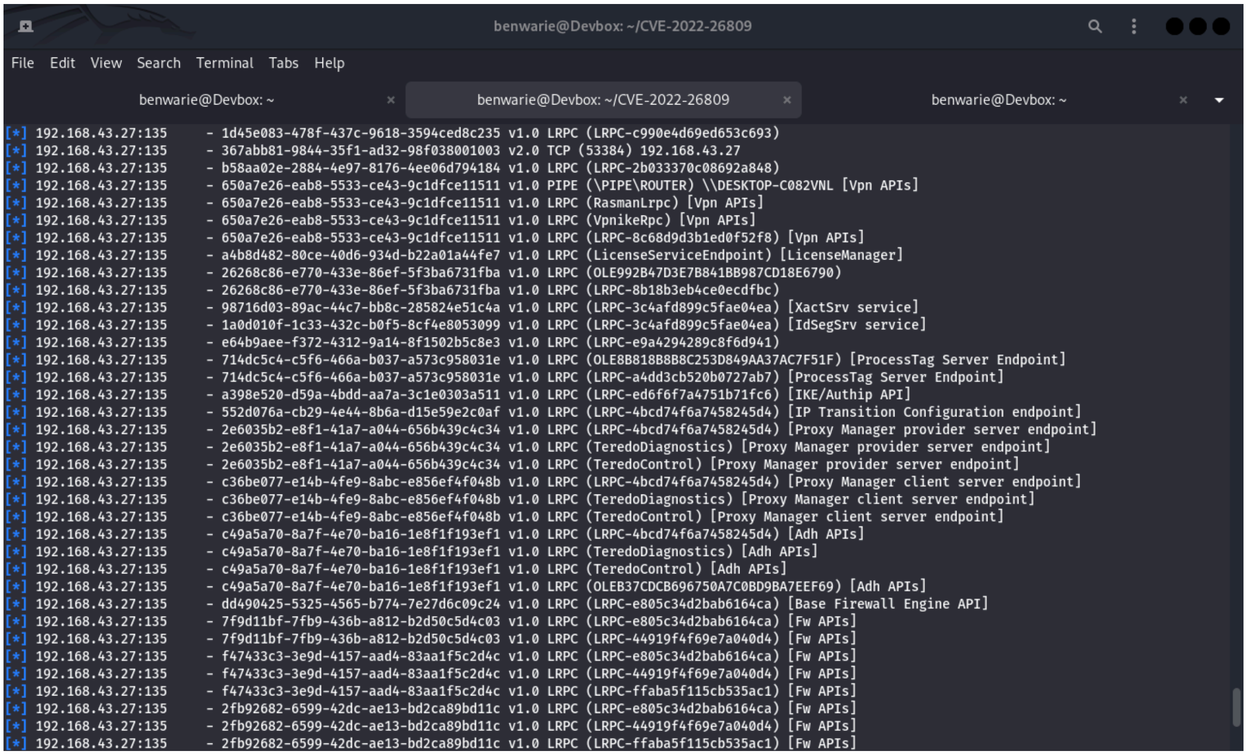
Port 135 running Msrpc allowed for enumeration of rpc bindings wich we interacted with using rpcclient, although the vulnerability is of low severity as privileged actions could not be carried out



```
 deletetrustdom         Delete Trusted Domain
---------------         ----------------------
GENERAL OPTIONS
           help         Get help on commands
              ?         Get help on commands
     debuglevel         Set debug level
          debug         Set debug level
           list         List available commands on <pipe>
           exit         Exit program
           quit         Exit program
           sign         Force RPC pipe connections to be signed
           seal         Force RPC pipe connections to be sealed
         packet         Force RPC pipe connections with packet authentication le
vel
       schannel         Force RPC pipe connections to be sealed with 'schannel'.
 Assumes valid machine account to this domain controller.
    schannelsign        Force RPC pipe connections to be signed (not sealed) wit
h 'schannel'.  Assumes valid machine account to this domain controller.
        timeout         Set timeout (in milliseconds) for RPC operations
      transport         Choose ncacn transport for RPC operations
           none         Force RPC pipe connections to have no special properties
rpcclient $> sign
Setting NTLMSSP - sign: NT_STATUS_OK
rpcclient $> 
```



```
[*] 192.168.43.27:135     - Connecting to the endpoint mapper service...
[*] 192.168.43.27:135     - EPM unknown type: 33 46353837393746362d433946332d344436332d394244342d4535353241433032304535383600
[*] 192.168.43.27:135     - EPM unknown type: 32 65306531363139372d646435362d346131302d393139352d35656537613135356138333800
[*] 192.168.43.27:135     - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 TCP (49664) 192.168.43.27 [Ngc Pop Key Service]
[*] 192.168.43.27:135     - ae2dc901-312d-41df-8b79-e835e63db874 v1.0 LRPC (LRPC-31a5e6d268a6e52094) [appxsvc]
[*] 192.168.43.27:135     - ff9fd3c4-742e-45e0-91dd-2f5bc632a1df v1.0 LRPC (LRPC-31a5e6d268a6e52094) [appxsvc]
[*] 192.168.43.27:135     - 9435cc56-1d9c-4924-ac7d-b60a2c3520e1 v1.0 LRPC (SPPCTransportEndpoint-00001) [SPPSVC Default RPC Interface]
[*] 192.168.43.27:135     - bf4dc912-e52f-4904-8ebe-9317c1bdd497 v1.0 LRPC (OLE76B7AB7E7C2ED19DCFF2D83FD11C)
[*] 192.168.43.27:135     - bf4dc912-e52f-4904-8ebe-9317c1bdd497 v1.0 LRPC (LRPC-7ed21e22e6696e10b0)
[*] 192.168.43.27:135     - c0e9671e-33c6-4438-9464-56b2e1b1c7b4 v1.0 LRPC (LRPC-4d2a23ec132f3e17c8) [wbiosrvc]
[*] 192.168.43.27:135     - 4be96a0f-9f52-4729-a51d-c70610f118b0 v1.0 LRPC (LRPC-4d2a23ec132f3e17c8) [wbiosrvc]
[*] 192.168.43.27:135     - 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC (LRPC-23d6190b898a94d5fa) [PcaSvc]
[*] 192.168.43.27:135     - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-aa84ec80e24b62230b)
[*] 192.168.43.27:135     - ba4aa15a-be94-47fb-9bfb-fef110e7efad v1.0 LRPC (LRPC-e5b7eb673a8f4768a4) [DevQueryBroker client query RPC interface]
[*] 192.168.43.27:135     - 0497b57d-2e66-424f-a0c6-157cd5d41700 v1.0 LRPC (LRPC-3eec8d91a9a5aa61c4) [AppInfo]
[*] 192.168.43.27:135     - 201ef99a-7fa0-444c-9399-19ba84f12a1a v1.0 LRPC (LRPC-3eec8d91a9a5aa61c4) [AppInfo]
[*] 192.168.43.27:135     - 5f54ce7d-5b79-4175-8584-cb65313a0e98 v1.0 LRPC (LRPC-3eec8d91a9a5aa61c4) [AppInfo]
[*] 192.168.43.27:135     - fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 v1.0 LRPC (LRPC-3eec8d91a9a5aa61c4) [AppInfo]
[*] 192.168.43.27:135     - 58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 LRPC (LRPC-3eec8d91a9a5aa61c4) [AppInfo]
[*] 192.168.43.27:135     - d2716e94-25cb-4820-bc15-537866578562 v1.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - d2716e94-25cb-4820-bc15-537866578562 v1.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd v1.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd v1.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - 923c9623-db7f-4b34-9e6d-e86580f8ca2a v1.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - 923c9623-db7f-4b34-9e6d-e86580f8ca2a v1.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - e8748f69-a2a4-40df-9366-62dbeb696e26 v0.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - e8748f69-a2a4-40df-9366-62dbeb696e26 v0.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - c8ba73d2-3d55-429c-8e9a-c44f006f69fc v0.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - c8ba73d2-3d55-429c-8e9a-c44f006f69fc v0.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - 43890c94-bfd7-4655-ad6a-b4a68397cdcb v0.0 LRPC (OLE4D68FE27D70D242770B7AF09FAAF)
[*] 192.168.43.27:135     - 43890c94-bfd7-4655-ad6a-b4a68397cdcb v0.0 LRPC (LRPC-798041e9c0c1114307)
[*] 192.168.43.27:135     - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLEBF7FB8ABAE53412E6ECCBF41EB79)
[*] 192.168.43.27:135     - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-b383fb75b421480aff)
[*] 192.168.43.27:135     - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLEBF7FB8ABAE53412E6ECCBF41EB79)
[*] 192.168.43.27:135     - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-b383fb75b421480aff)
```

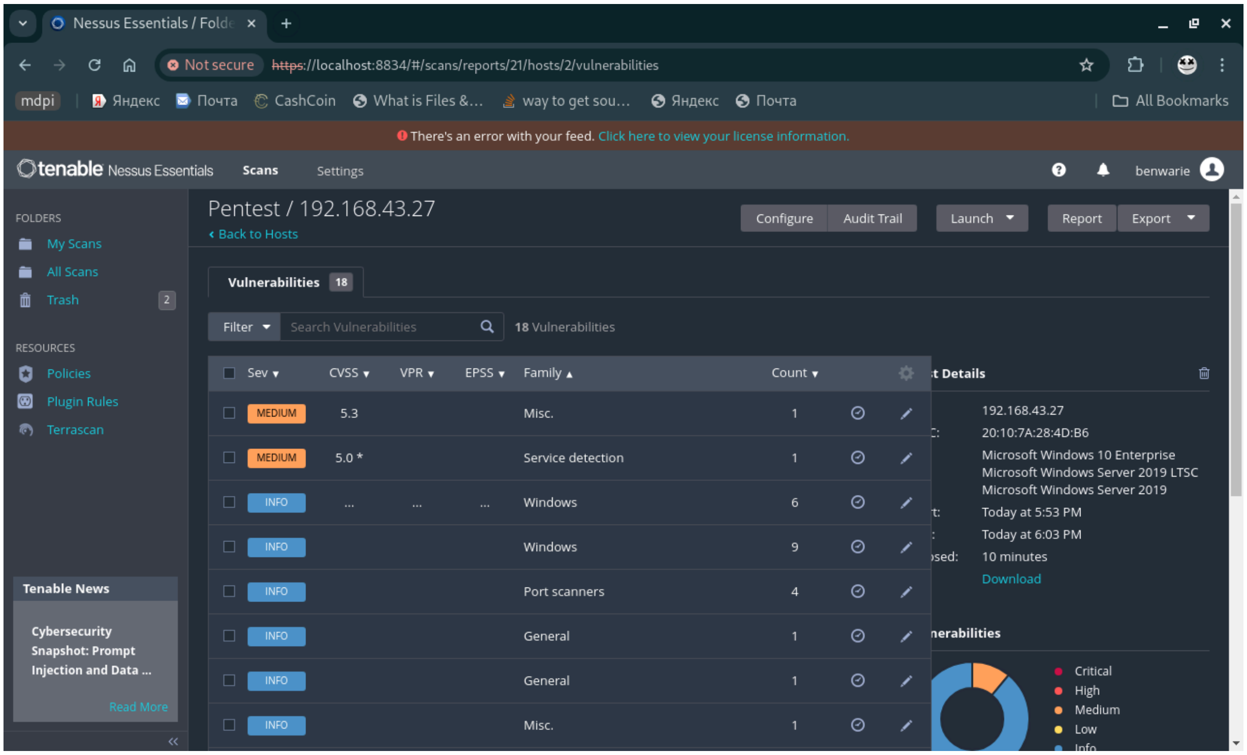


benwarie@Devbox: ~/CVE-2022-26809
File Edit View Search Terminal Tabs Help
benwarie@Devbox: ~
benwarie@Devbox: ~/CVE-2022-26809
benwarie@Devbox: ~

```
[*] 192.168.43.27:135     - 1d45e083-478f-437c-9618-3594ced8c235 v1.0 LRPC (LRPC-c990e4d69ed653c693)
[*] 192.168.43.27:135     - 367abb81-9844-35f1-ad32-98f038001003 v2.0 TCP (53384) 192.168.43.27
[*] 192.168.43.27:135     - b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (LRPC-2b033370c08692a848)
[*] 192.168.43.27:135     - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 PIPE (\PIPE\ROUTER) \\DESKTOP-C082VNL [Vpn APIs]
[*] 192.168.43.27:135     - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (RasmanLrpc) [Vpn APIs]
[*] 192.168.43.27:135     - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (VpnikeRpc) [Vpn APIs]
[*] 192.168.43.27:135     - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (LRPC-8c68d9d3b1ed0f52f8) [Vpn APIs]
[*] 192.168.43.27:135     - a4b8d482-80ce-40d6-934d-b22a01a44fe7 v1.0 LRPC (LicenseServiceEndpoint) [LicenseManager]
[*] 192.168.43.27:135     - 26268c86-e770-433e-86ef-5f3ba6731fba v1.0 LRPC (OLE992B47D3E7B841BB987CD18E6790)
[*] 192.168.43.27:135     - 26268c86-e770-433e-86ef-5f3ba6731fba v1.0 LRPC (LRPC-8b18b3eb4ce0ecdfbc)
[*] 192.168.43.27:135     - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC (LRPC-3c4afd899c5fae04ea) [XactSrv service]
[*] 192.168.43.27:135     - 1a0d010f-1c33-432c-b0f5-8cf4e8053099 v1.0 LRPC (LRPC-3c4afd899c5fae04ea) [IdSegSrv service]
[*] 192.168.43.27:135     - e64b9aee-f372-4312-9a14-8f1502b5c8e3 v1.0 LRPC (LRPC-e9a4294289c8f6d941)
[*] 192.168.43.27:135     - 714dc5c4-c5f6-466a-b037-a573c958031e v1.0 LRPC (OLE8B818B8B8C253D849AA37AC7F51F) [ProcessTag Server Endpoint]
[*] 192.168.43.27:135     - 714dc5c4-c5f6-466a-b037-a573c958031e v1.0 LRPC (LRPC-a4dd3cb520b0727ab7) [ProcessTag Server Endpoint]
[*] 192.168.43.27:135     - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 LRPC (LRPC-ed6f6f7a4751b71fc6) [IKE/Authip API]
[*] 192.168.43.27:135     - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 LRPC (LRPC-4bcd74f6a7458245d4) [IP Transition Configuration endpoint]
[*] 192.168.43.27:135     - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (LRPC-4bcd74f6a7458245d4) [Proxy Manager provider server endpoint]
[*] 192.168.43.27:135     - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (TeredoDiagnostics) [Proxy Manager provider server endpoint]
[*] 192.168.43.27:135     - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (TeredoControl) [Proxy Manager provider server endpoint]
[*] 192.168.43.27:135     - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (LRPC-4bcd74f6a7458245d4) [Proxy Manager client server endpoint]
[*] 192.168.43.27:135     - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (TeredoDiagnostics) [Proxy Manager client server endpoint]
[*] 192.168.43.27:135     - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (TeredoControl) [Proxy Manager client server endpoint]
[*] 192.168.43.27:135     - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (LRPC-4bcd74f6a7458245d4) [Adh APIs]
[*] 192.168.43.27:135     - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (TeredoDiagnostics) [Adh APIs]
[*] 192.168.43.27:135     - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (TeredoControl) [Adh APIs]
[*] 192.168.43.27:135     - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (OLEB37CDCB696750A7C0BD9BA7EEF69) [Adh APIs]
[*] 192.168.43.27:135     - dd490425-5325-4565-b774-7e27d6c09c24 v1.0 LRPC (LRPC-e805c34d2bab6164ca) [Base Firewall Engine API]
[*] 192.168.43.27:135     - 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 v1.0 LRPC (LRPC-e805c34d2bab6164ca) [Fw APIs]
[*] 192.168.43.27:135     - 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 v1.0 LRPC (LRPC-44919f4f69e7a040d4) [Fw APIs]
[*] 192.168.43.27:135     - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-e805c34d2bab6164ca) [Fw APIs]
[*] 192.168.43.27:135     - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-44919f4f69e7a040d4) [Fw APIs]
[*] 192.168.43.27:135     - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-ffaba5f115cb535ac1) [Fw APIs]
[*] 192.168.43.27:135     - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-e805c34d2bab6164ca) [Fw APIs]
[*] 192.168.43.27:135     - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-44919f4f69e7a040d4) [Fw APIs]
[*] 192.168.43.27:135     - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-ffaba5f115cb535ac1) [Fw APIs]
```

How the vulnerability was exploited, and the tools used to exploit it. Vulnerability Scanning

Enumeration of vulnerabilities is done on the target system using Tenable nessus and nmap to ascertain any vulnerability to gain entry into the system. We discovered Mdns which was revealing excess information such as Hostname, Domain name, Smb which did not enforce signing on its $IPC shares and several other informational.
Below is the result of the scan.



There's an error with your feed. Click here to view your license information.

Pentest / 192.168.43.27

‹ Back to Hosts

Vulnerabilities 18

18 Vulnerabilities

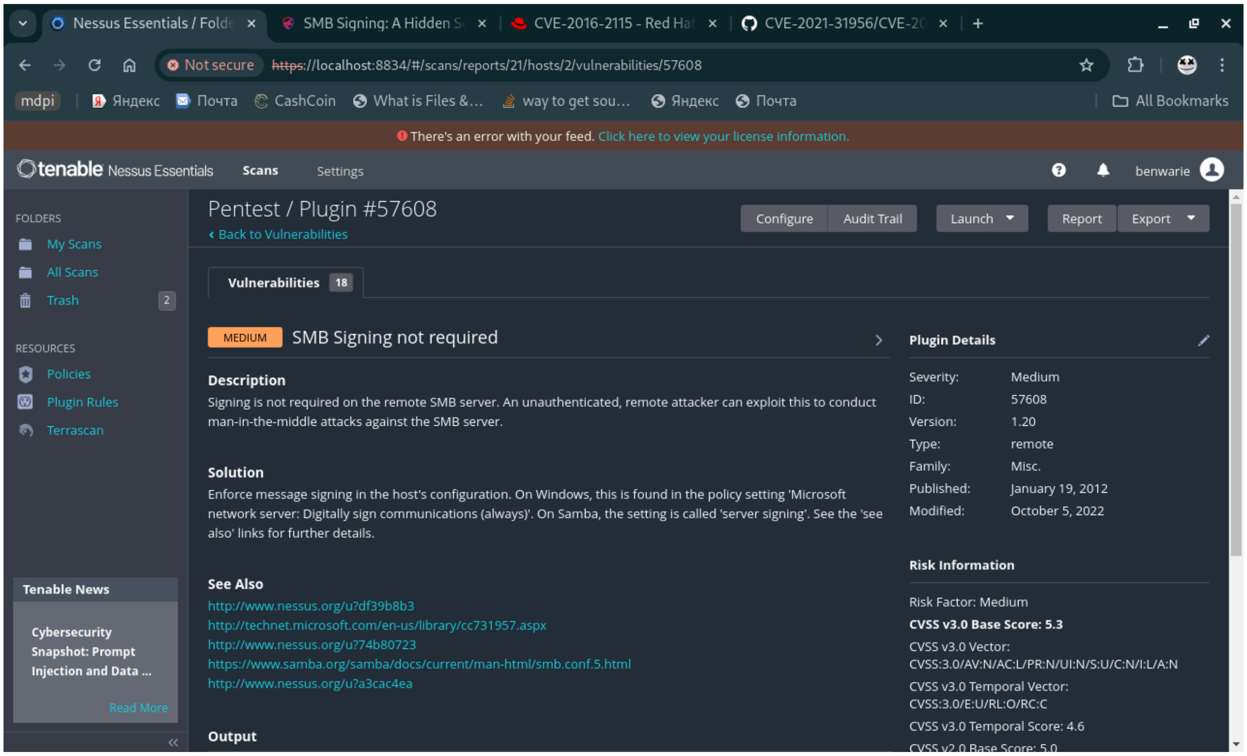
□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Family ▴	Count ▾
□	MEDIUM	5.3			Misc.	1
□	MEDIUM	5.0 *			Service detection	1
□	INFO	...	...	...	Windows	6
□	INFO				Windows	9
□	INFO				Port scanners	4
□	INFO				General	1
□	INFO				General	1
□	INFO				Misc.	1

t Details

	192.168.43.27
C:	20:10:7A:28:4D:B6
	Microsoft Windows 10 Enterprise Microsoft Windows Server 2019 LTSC Microsoft Windows Server 2019
t:	Today at 5:53 PM
:	Today at 6:03 PM
sed:	10 minutes
	Download

nerabilities

● Critical
● High
● Medium
● Low
● Info



There's an error with your feed. Click here to view your license information.

Pentest / Plugin #57608

‹ Back to Vulnerabilities

Vulnerabilities 18

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium

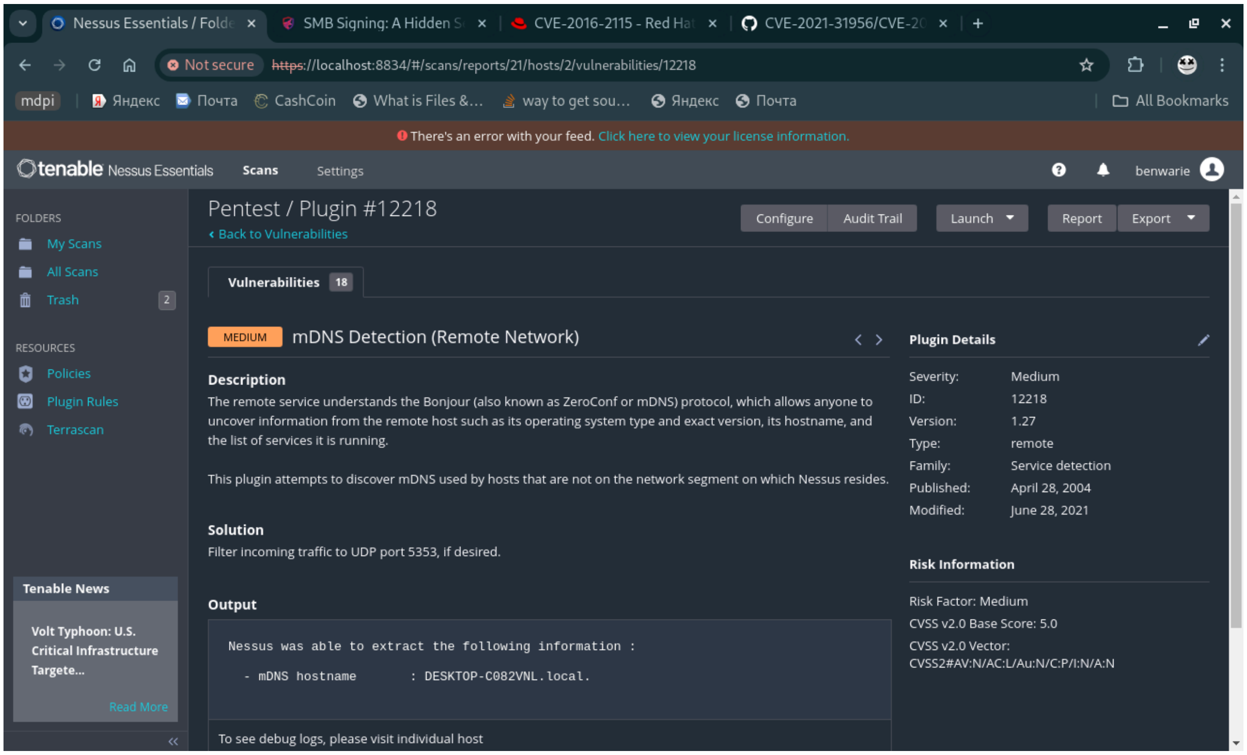
CVSS v3.0 Base Score: 5.3

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0



mDNS Detection (Remote Network)

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Output

```
Nessus was able to extract the following information :

  - mDNS hostname       : DESKTOP-C082VNL.local.
```

To see debug logs, please visit individual host

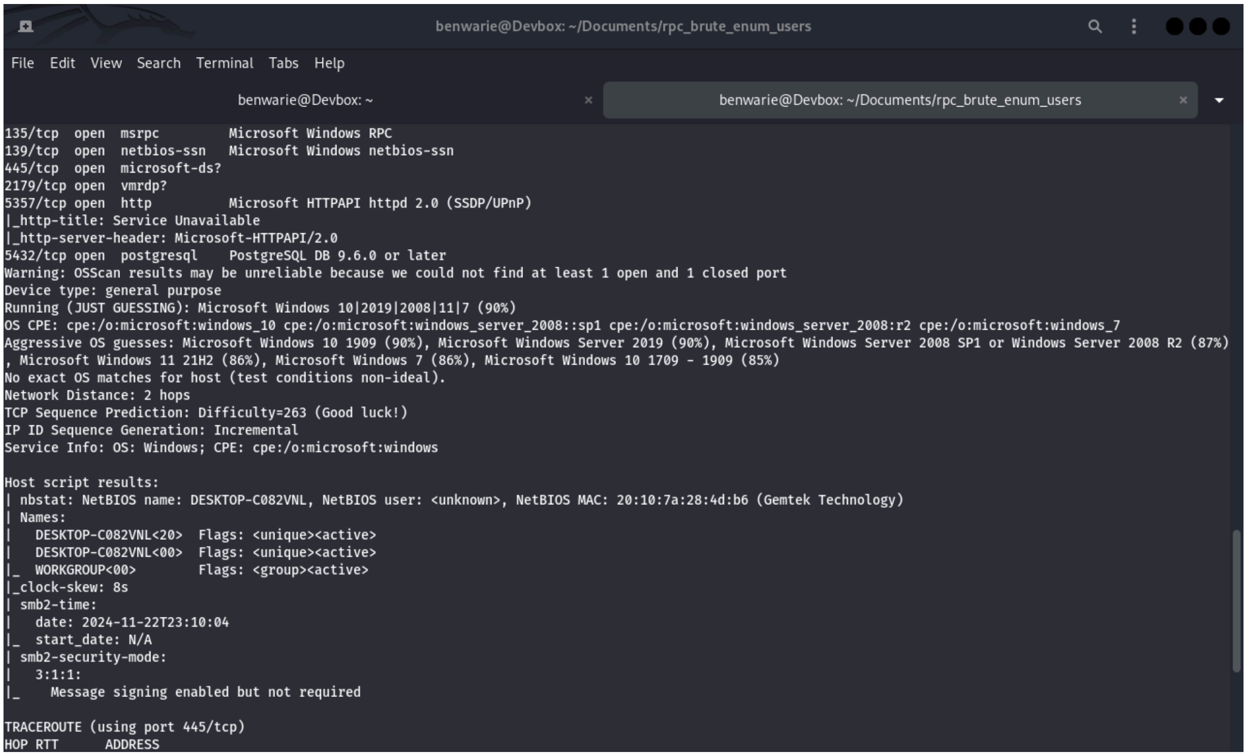
Plugin Details

Severity: Medium
ID: 12218
Version: 1.27
Type: remote
Family: Service detection
Published: April 28, 2004
Modified: June 28, 2021

Risk Information

Risk Factor: Medium
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Further enumeration with nmap scripting engine did not reveal any flaw which was also solidified by using several POC test scripts for individual CVE


benwarie@Devbox: ~/Documents/rpc_brute_enum_users
File Edit View Search Terminal Tabs Help
benwarie@Devbox: ~
benwarie@Devbox: ~/Documents/rpc_brute_enum_users

```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
5432/tcp open  postgresql    PostgreSQL DB 9.6.0 or later
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|2008|11|7 (90%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows 10 1909 (90%), Microsoft Windows Server 2019 (90%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (87%)
, Microsoft Windows 11 21H2 (86%), Microsoft Windows 7 (86%), Microsoft Windows 10 1709 - 1909 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DESKTOP-C082VNL, NetBIOS user: <unknown>, NetBIOS MAC: 20:10:7a:28:4d:b6 (Gemtek Technology)
| Names:
|   DESKTOP-C082VNL<20>  Flags: <unique><active>
|   DESKTOP-C082VNL<00>  Flags: <unique><active>
|_  WORKGROUP<00>        Flags: <group><active>
|_clock-skew: 8s
| smb2-time:
|   date: 2024-11-22T23:10:04
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
```

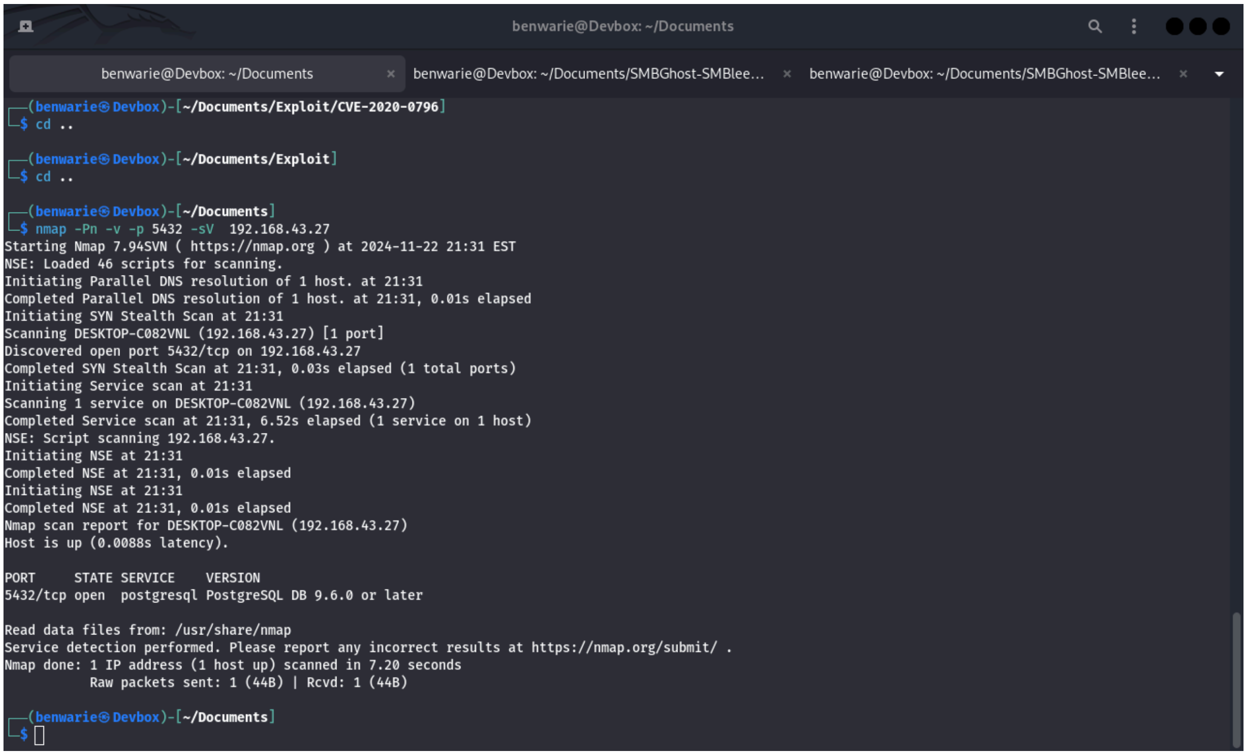
We were able to reveal the version of the smb using metasploit. Below is an extract of the auxiliary scanner, version information for smb

```
*] 192.168.43.27:445     - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1)
(compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM)
(signatures:optional) (guid:{d4c466e6-6ec7-45ca-b021-7d95ca4817fb}) (authentication
domain:DESKTOP-C082VNL)
[*] 192.168.43.27:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

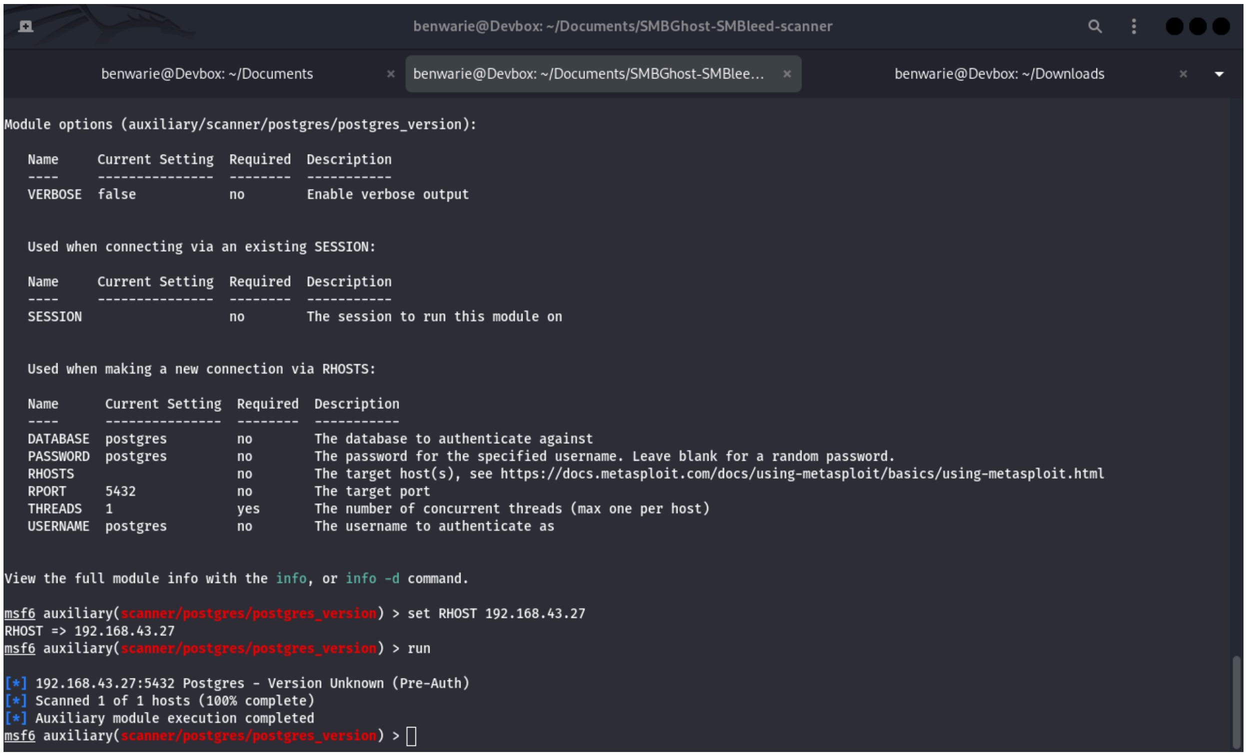
Below is a checklist used for CVE;

cve_2019_0708_bluekeep_rce
ms12_020_maxchannelids
ms12_020_check
cain_abel_4918_rdp
cve_2019_0708_bluekeep_rce
cve_2019_0708_bluekeep
CVE-2021-1675
CVE-2021-31956
CVE-2017-0144
PrintNightmare CVE-2021-34527
ZeroLogon CVE-2020-1472

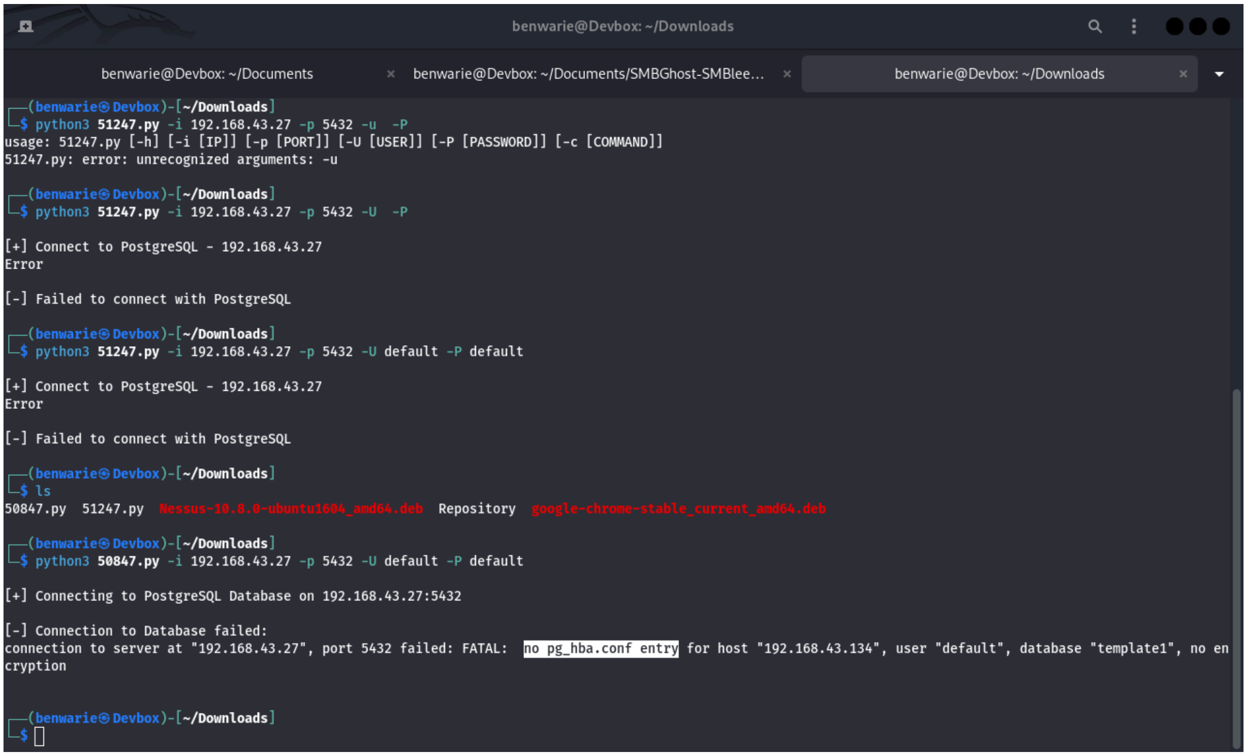
We proceeded to enumerate the Postgresql server for possible vulnerabilities and discovered that it doesn’t have encryption which is an impairment on confidentiality and integrity. However we didn’t exploit this vulnerability to the end dues to the cost of computation in running large wordlists to find a match.


benwarie@Devbox: ~/Documents
benwarie@Devbox: ~/Documents
benwarie@Devbox: ~/Documents/SMBGhost-SMBlee…
benwarie@Devbox: ~/Documents/SMBGhost-SMBlee…

```
┌──(benwarie㉿Devbox)-[~/Documents/Exploit/CVE-2020-0796]
└─$ cd ..

┌──(benwarie㉿Devbox)-[~/Documents/Exploit]
└─$ cd ..

┌──(benwarie㉿Devbox)-[~/Documents]
└─$ nmap -Pn -v -p 5432 -sV  192.168.43.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 21:31 EST
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 21:31
Completed Parallel DNS resolution of 1 host. at 21:31, 0.01s elapsed
Initiating SYN Stealth Scan at 21:31
Scanning DESKTOP-C082VNL (192.168.43.27) [1 port]
Discovered open port 5432/tcp on 192.168.43.27
Completed SYN Stealth Scan at 21:31, 0.03s elapsed (1 total ports)
Initiating Service scan at 21:31
Scanning 1 service on DESKTOP-C082VNL (192.168.43.27)
Completed Service scan at 21:31, 6.52s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.43.27.
Initiating NSE at 21:31
Completed NSE at 21:31, 0.01s elapsed
Initiating NSE at 21:31
Completed NSE at 21:31, 0.01s elapsed
Nmap scan report for DESKTOP-C082VNL (192.168.43.27)
Host is up (0.0088s latency).

PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.20 seconds
           Raw packets sent: 1 (44B) | Rcvd: 1 (44B)

┌──(benwarie㉿Devbox)-[~/Documents]
└─$ 
```


benwarie@Devbox: ~/Documents/SMBGhost-SMBleed-scanner
benwarie@Devbox: ~/Documents
benwarie@Devbox: ~/Documents/SMBGhost-SMBlee…
benwarie@Devbox: ~/Downloads

```
Module options (auxiliary/scanner/postgres/postgres_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME  postgres         no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/postgres/postgres_version) > set RHOST 192.168.43.27
RHOST => 192.168.43.27
msf6 auxiliary(scanner/postgres/postgres_version) > run

[*] 192.168.43.27:5432 Postgres - Version Unknown (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_version) > 
```


benwarie@Devbox: ~/Downloads
benwarie@Devbox: ~/Documents
benwarie@Devbox: ~/Documents/SMBGhost-SMBlee…
benwarie@Devbox: ~/Downloads

```
┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ python3 51247.py -i 192.168.43.27 -p 5432 -u  -P
usage: 51247.py [-h] [-i [IP]] [-p [PORT]] [-U [USER]] [-P [PASSWORD]] [-c [COMMAND]]
51247.py: error: unrecognized arguments: -u

┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ python3 51247.py -i 192.168.43.27 -p 5432 -U  -P

[+] Connect to PostgreSQL - 192.168.43.27
Error

[-] Failed to connect with PostgreSQL

┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ python3 51247.py -i 192.168.43.27 -p 5432 -U default -P default

[+] Connect to PostgreSQL - 192.168.43.27
Error

[-] Failed to connect with PostgreSQL

┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ ls
50847.py  51247.py  Nessus-10.8.0-ubuntu1604_amd64.deb  Repository  google-chrome-stable_current_amd64.deb

┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ python3 50847.py -i 192.168.43.27 -p 5432 -U default -P default

[+] Connecting to PostgreSQL Database on 192.168.43.27:5432

[-] Connection to Database failed:
connection to server at "192.168.43.27", port 5432 failed: FATAL:  no pg_hba.conf entry for host "192.168.43.134", user "default", database "template1", no en
cryption


┌──(benwarie㉿Devbox)-[~/Downloads]
└─$ 
```

Overview of the Vulnerability Identified and tools used to identify it.

The Vulnerability discovered on our target machine is “open ports” which we escalated to get

1. rpc sessions with the target device.
2. Encryption status of Postgres
3. Smb client status

Potential risks and Impact of exploiting this vulnerability on real-world IT Infrastructure

The potential risk of this vulnerability in real world iT infrastructure include:

1. Information disclosure with regards to confidentiality and integrity compromise of database
2. Dos/DDos
3. Remote code execution from disclosure of hostname and device service versions.

Recommendation on Prevention and Mitigation Strategies

Recommendations for mitigation include

1. Use of firewall to block ip-addresses and close open ports
2. Deploying IT infrastructure in different network segments to prevent access to critical assets
3. Encryption of Database
4. Implementation of Authentication and Authorization policies e.g network access controls
5. Implementation of Patch management to handle outdated software running on devices.
6. Implementation of network or host based Intrusion detection and intrusion prevention systems

Conclusion

In conclusion we have been able to demonstrate practical skill for network penetration testing to identify hosts on a network and target a specific machine to reveal open ports and enumerate them for services leading to access on these machines. This is an example of how attackers can gain access to devices and access personal information.

References

1. Manasha Saqib, & Ayaz Hassan Moon. (2023). A systematic security assessment and review of Internet of Things in the context of authentication. *Computers & Security, 125*, 103053. https://doi.org/10.1016/j.cose.2022.103053
2. Johnson, L. (2020). Chapter 10 - System and network assessments. In L. Johnson (Ed.), *Security controls evaluation, testing, and assessment handbook* (2nd ed., pp. 447–469). Academic Press. https://doi.org/10.1016/B978-0-12-818427-1.00010-0
3. Wilhelm, T. (2010). Running a PenTest. In T. Wilhelm (Ed.), *Professional penetration testing* (p. 217). Syngress. https://doi.org/10.1016/B978-1-59749-425-0.00013-0