Gerren Jerome - Enumeration

Scenario:

- You are an ethical hacker with a large organization (EC-Council).
- You must demonstrate knowledge of enumeration, as gaining competitive advantage over your target significantly enhances your ability to perceive and bypass security measures.

Objectives:

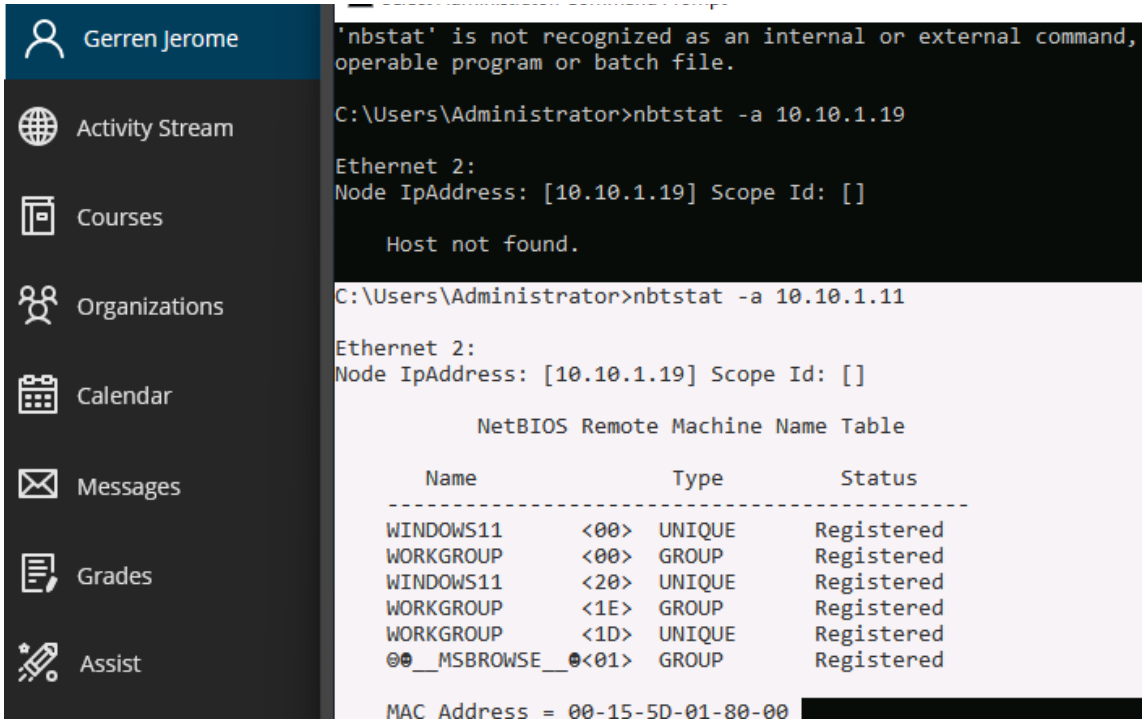
- Extraction various pieces of information about the target
    - e.g.: machine names/ports/OS/services, network resources and shares, usernames/user groups, policies and passwords, routing tables, audit and service settings, etc.

TASKS (XX items total):

Ethical hackers and pentesters use various tools and techniques to enumerate a target network.

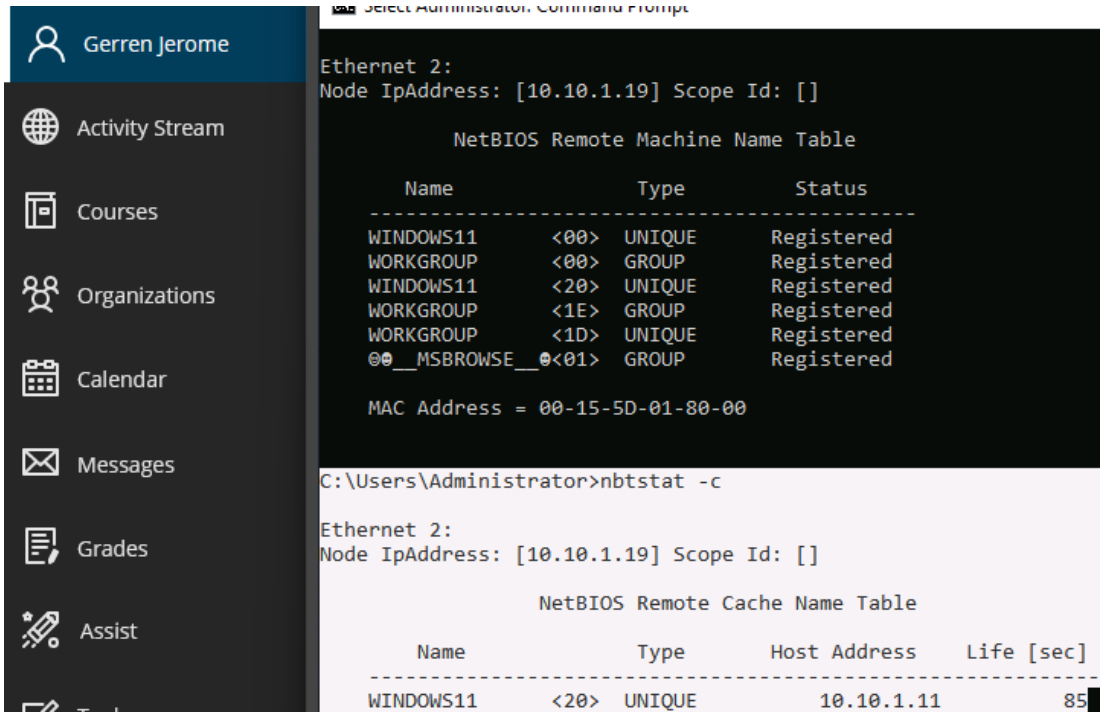
The following tasks will assist you in learning various enumeration techniques:

1) Perform enumeration (NetBIOS) (7 tasks)
    a) NetBIOS enumeration via Windows command line (3 tasks)
        i) **Screengrab: Step 5** – nbtstat result

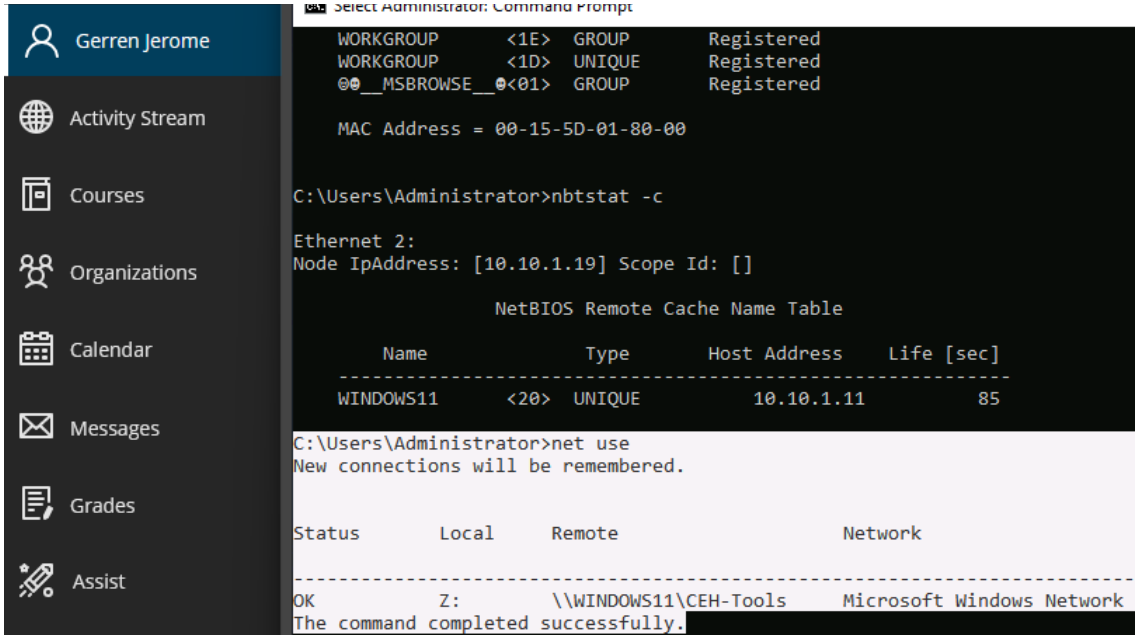


Gerren Jerome - Enumeration

ii) **Screengrab: Step 7** – nbtstat result



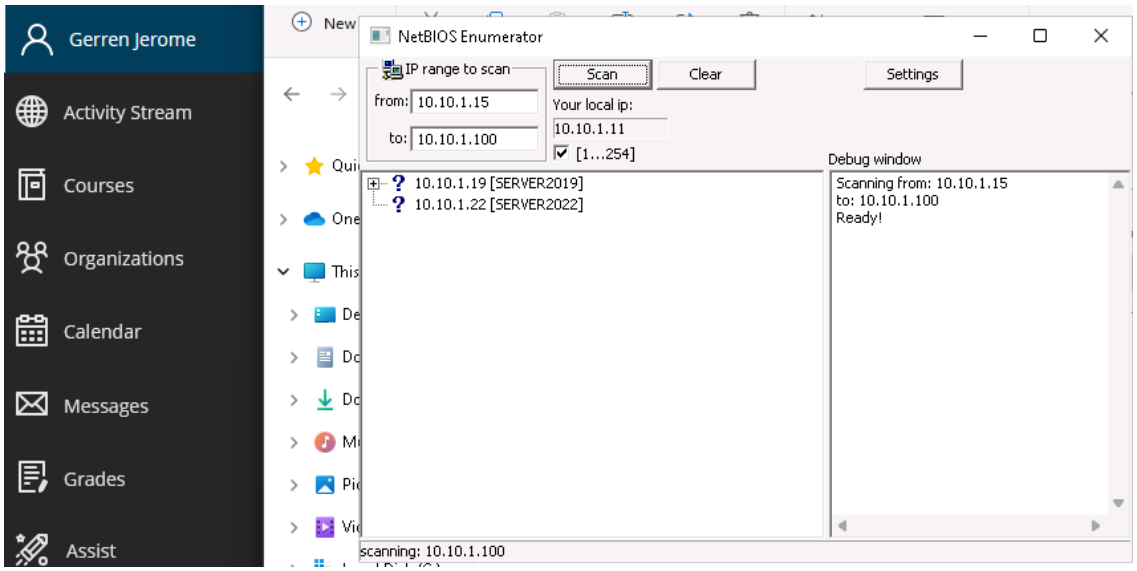
iii) **Screengrab: Step 9** – net use result



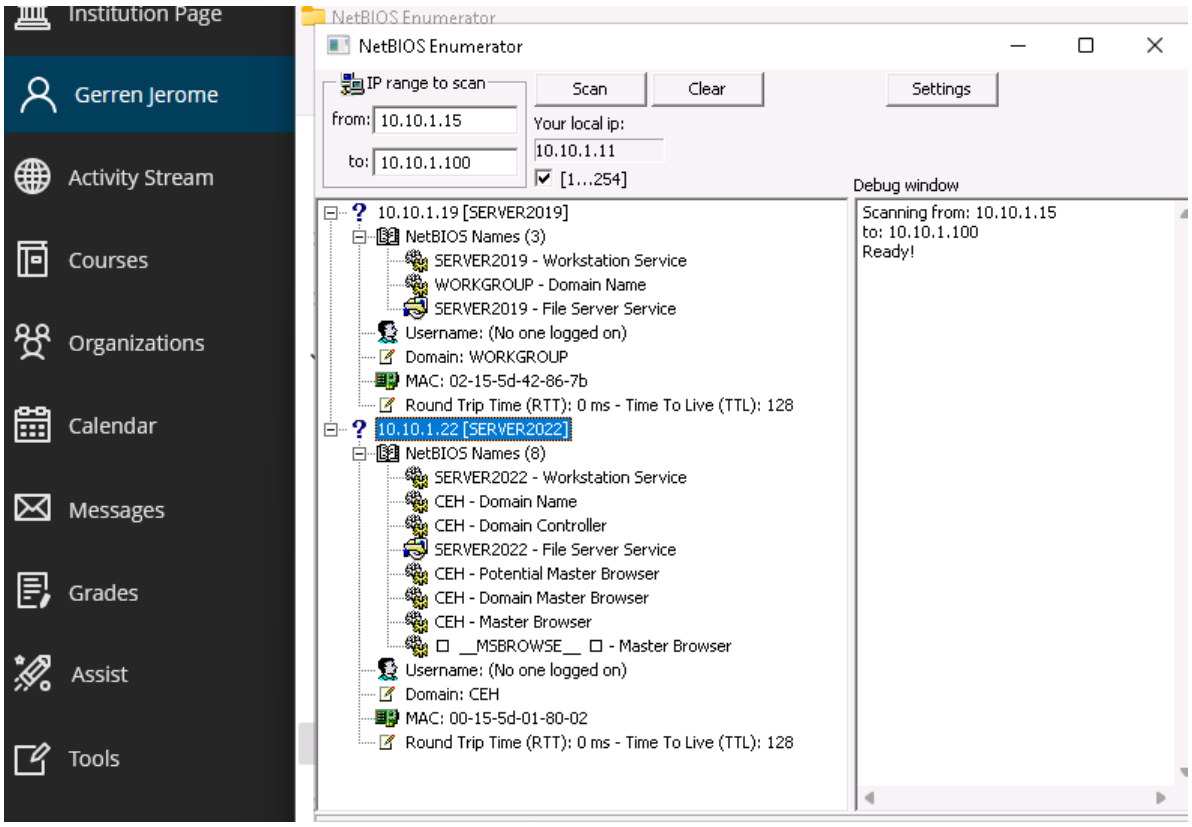
Gerren Jerome - Enumeration

b) NetBIOS enumeration via NetBIOS enumerator (2 tasks)

i) **Screengrab: Step 7** – NBE result (Debug)



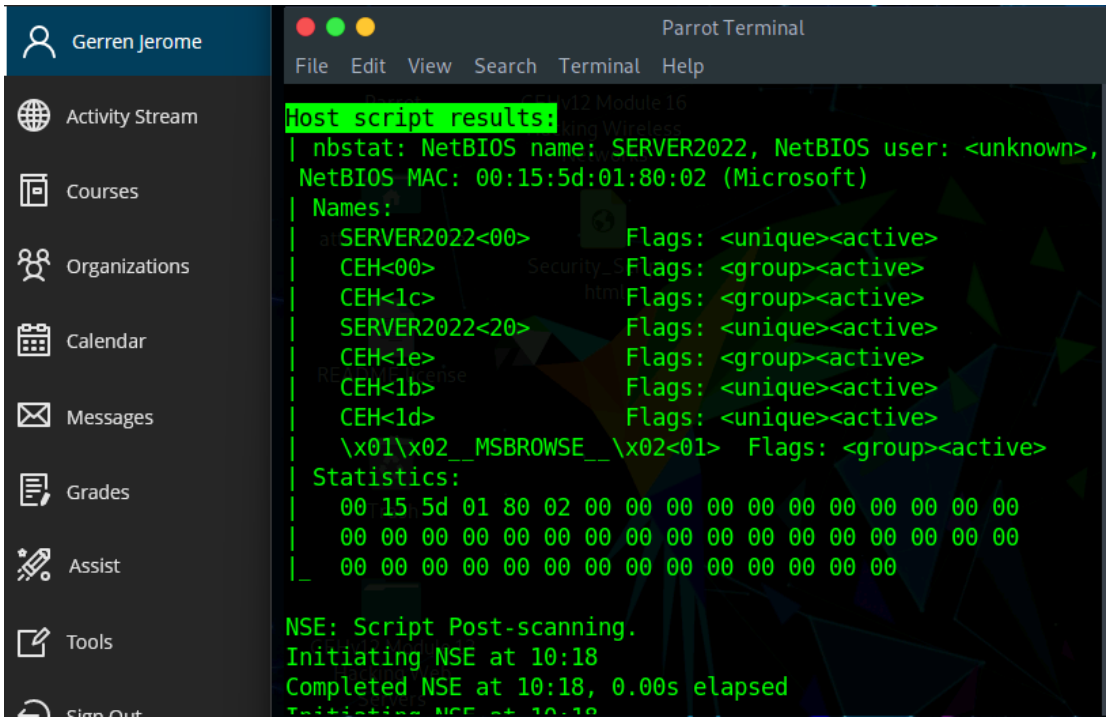
ii) **Screengrab: Step 8** – Expanded result



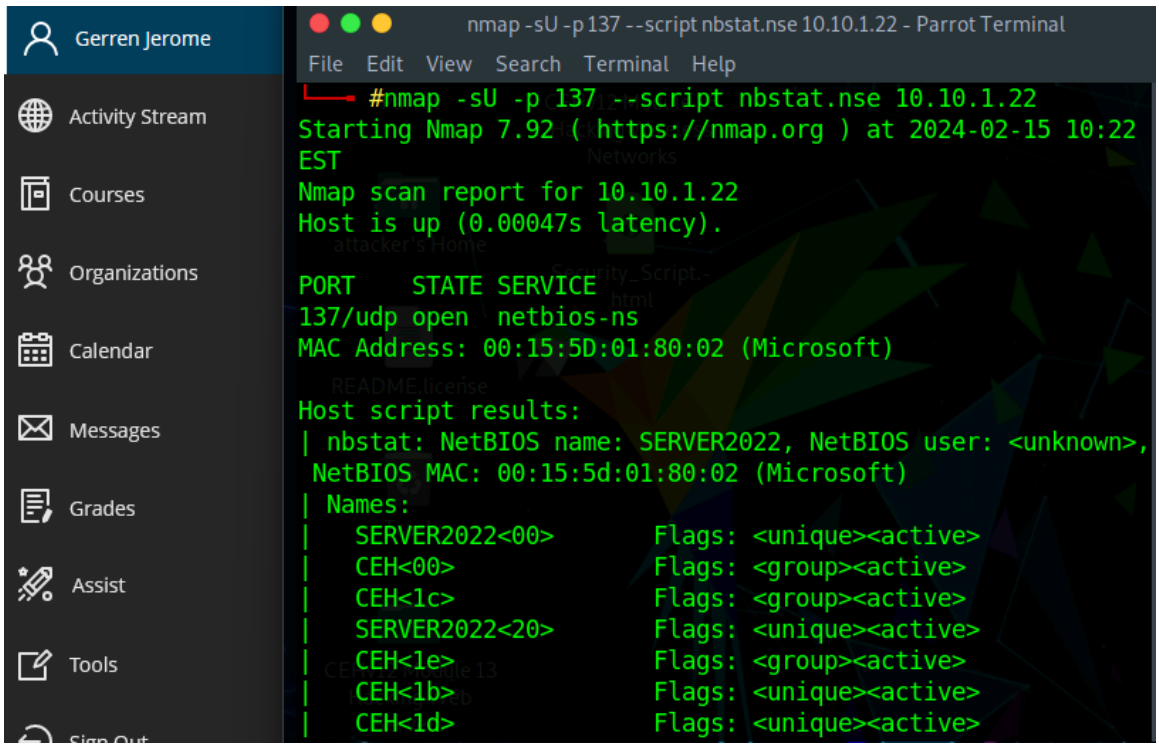
Gerren Jerome - Enumeration

c) NetBIOS enumeration via NSE Script (2 tasks)

i) **Screengrab: Step 7** – Nmap scan (-sV)



ii) **Screengrab: Step 9** – Nmap scan (-sU)

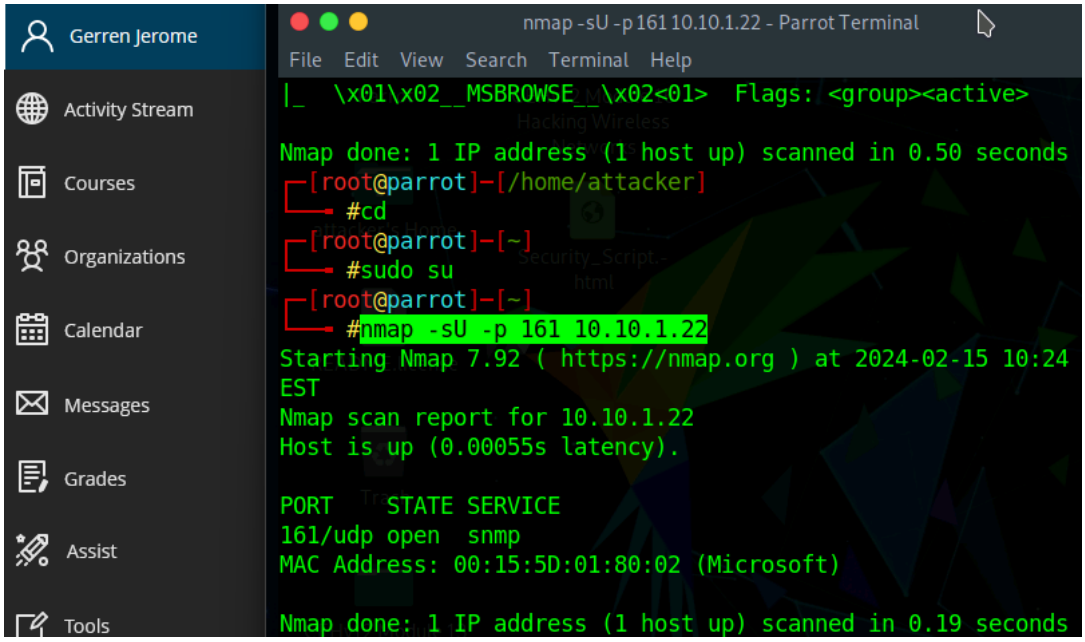


Gerren Jerome - Enumeration

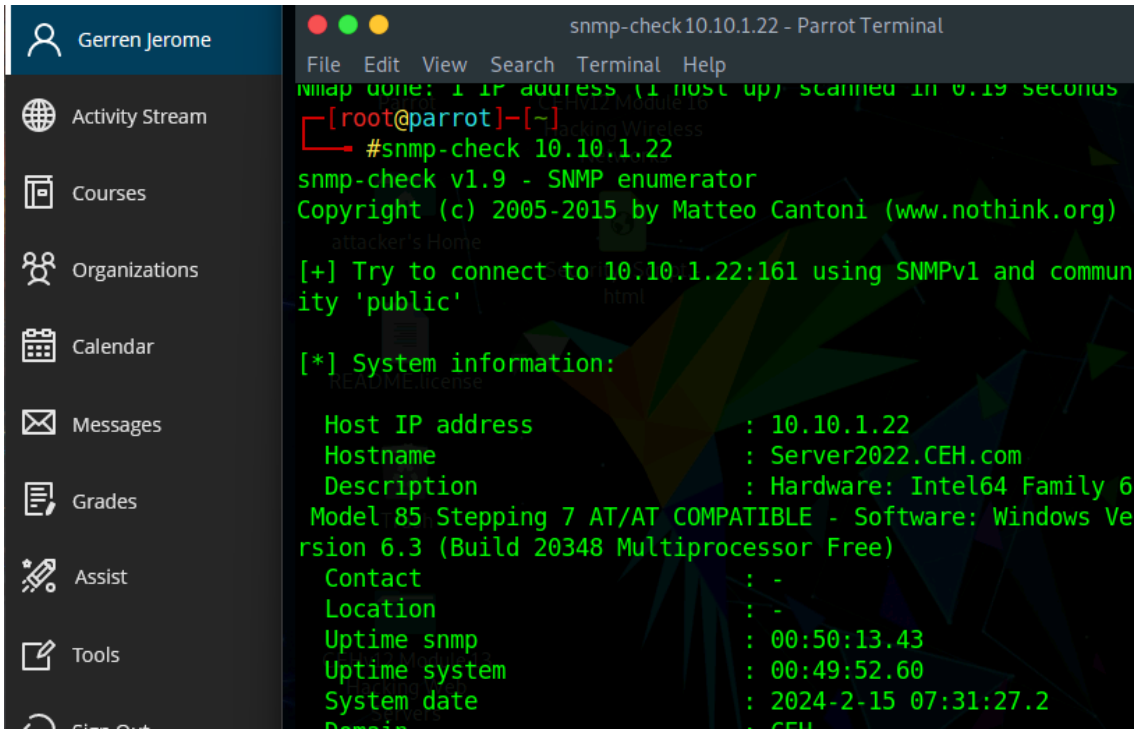
2) Perform enumeration (SNMP) (13 tasks)

a) SNMP enumeration via snmp-check (4 tasks)

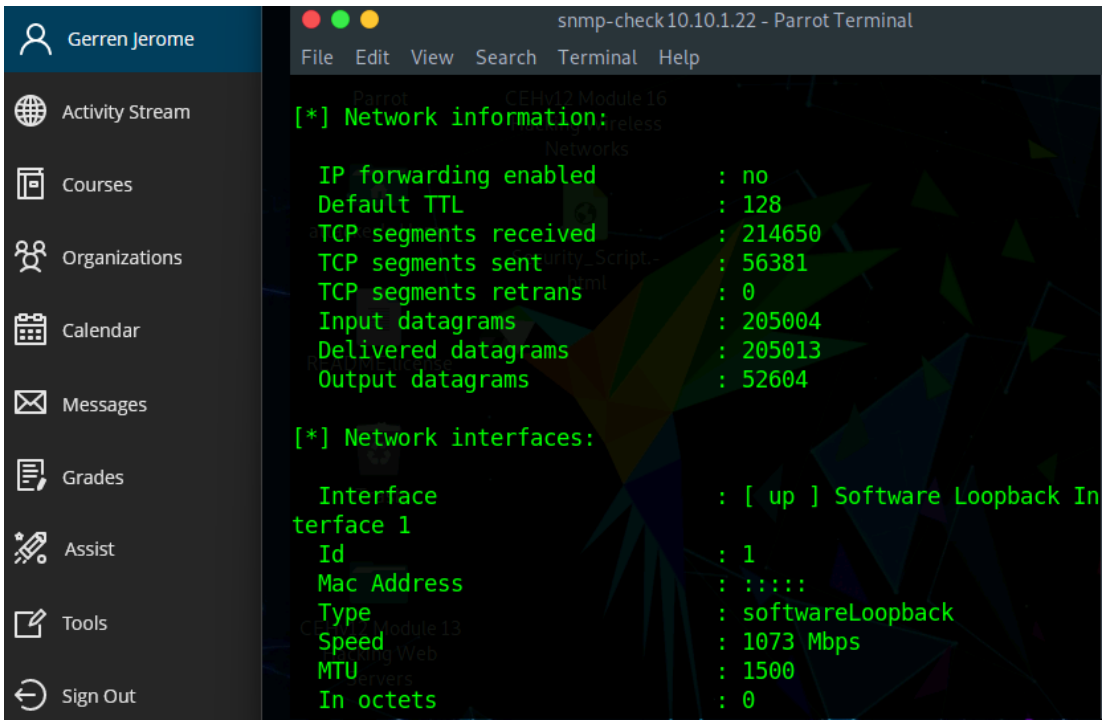
i) **Screengrab: Step 8** – Nmap scan (-sU)



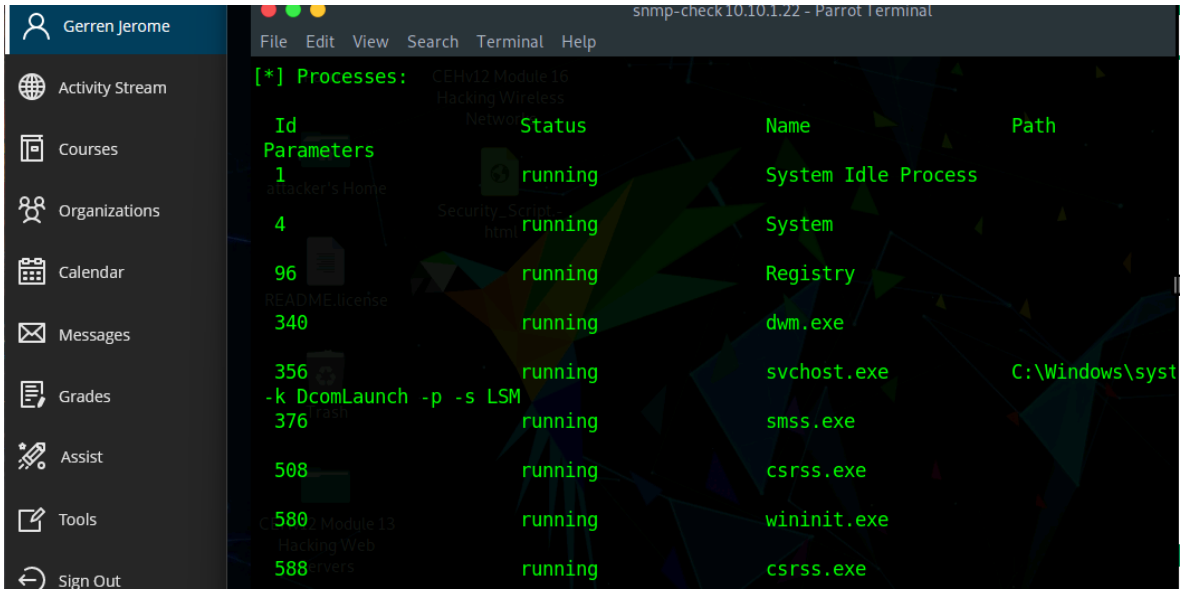
ii) **Screengrab: Step 12** – snmp-check results (1 of 3)



iii) **Screengrab: Step 13** – snmp-check results (2 of 3)



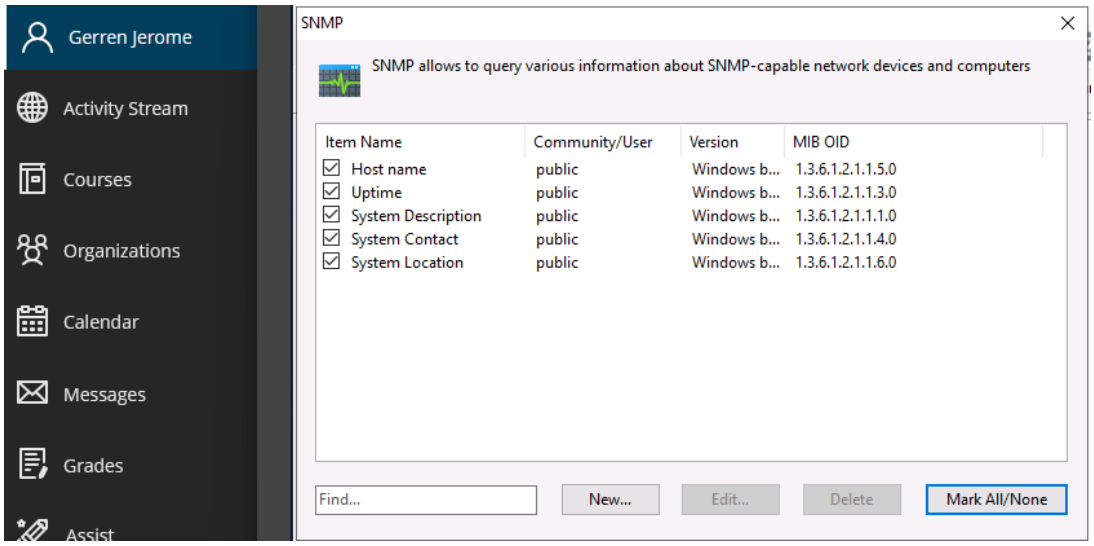
iv) **Screengrab: Step 14** – snmp-check results (3 of 3)



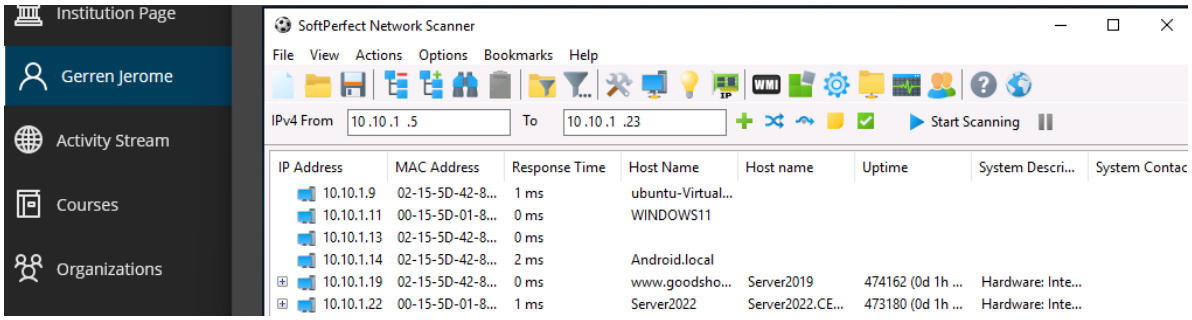
Gerren Jerome - Enumeration

b) SNMP enumeration via SoftPerfect Network Scanner (3 tasks)

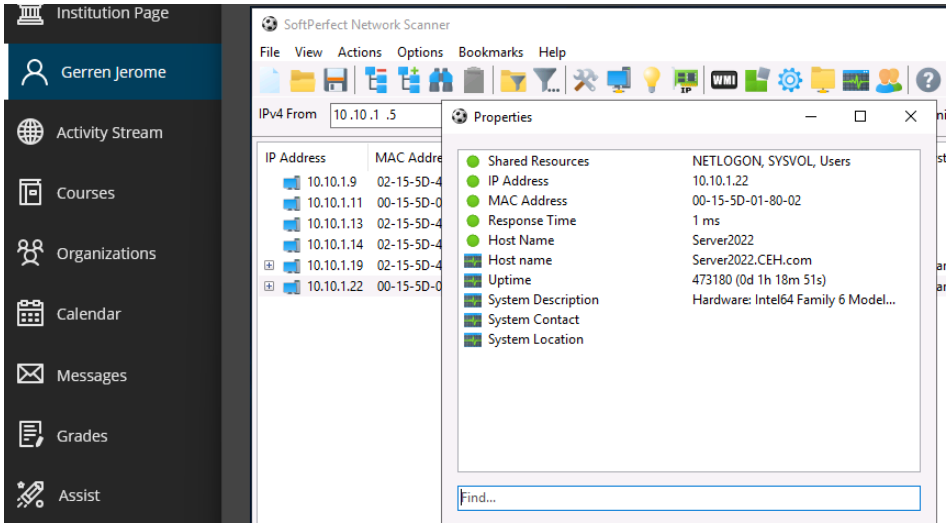
i) **Screengrab: Step 6** – prescan config



ii) **Screengrab: Step 9** – SPNS scan results



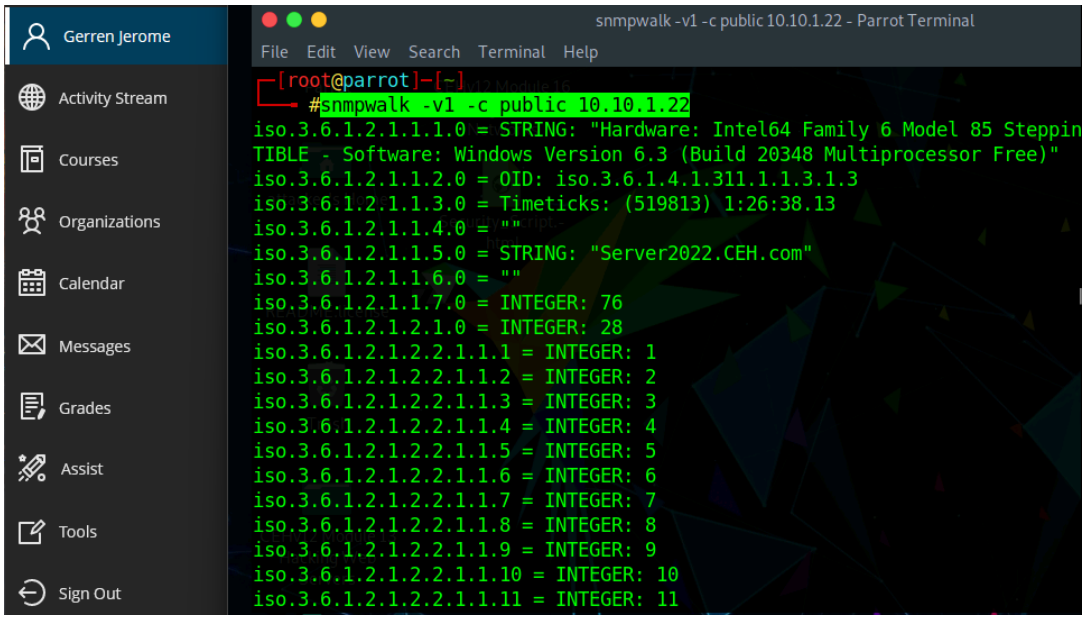
iii) **Screengrab: Step 11** – properties of target machine (10.10.1.22)



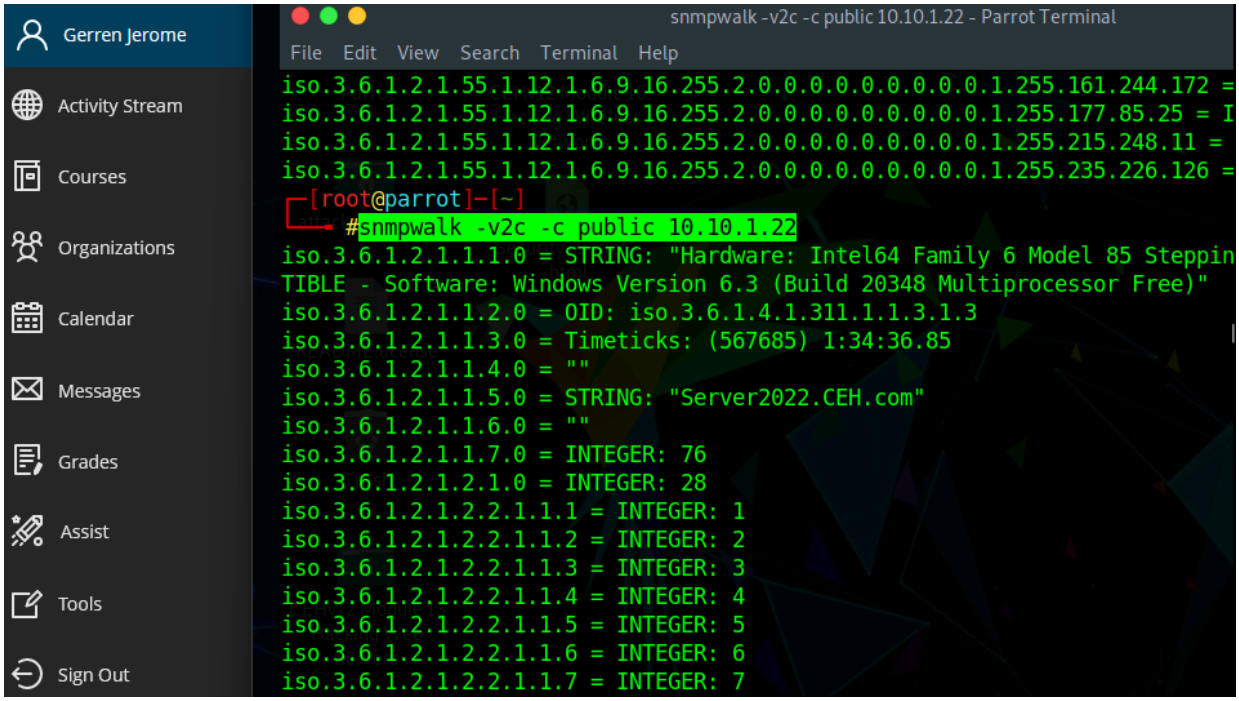
Gerren Jerome - Enumeration

c) SNMP enumeration via SnmpWalk (2 tasks)

i) **Screengrab: Step 6** – scan result (snmpwalk -v1)



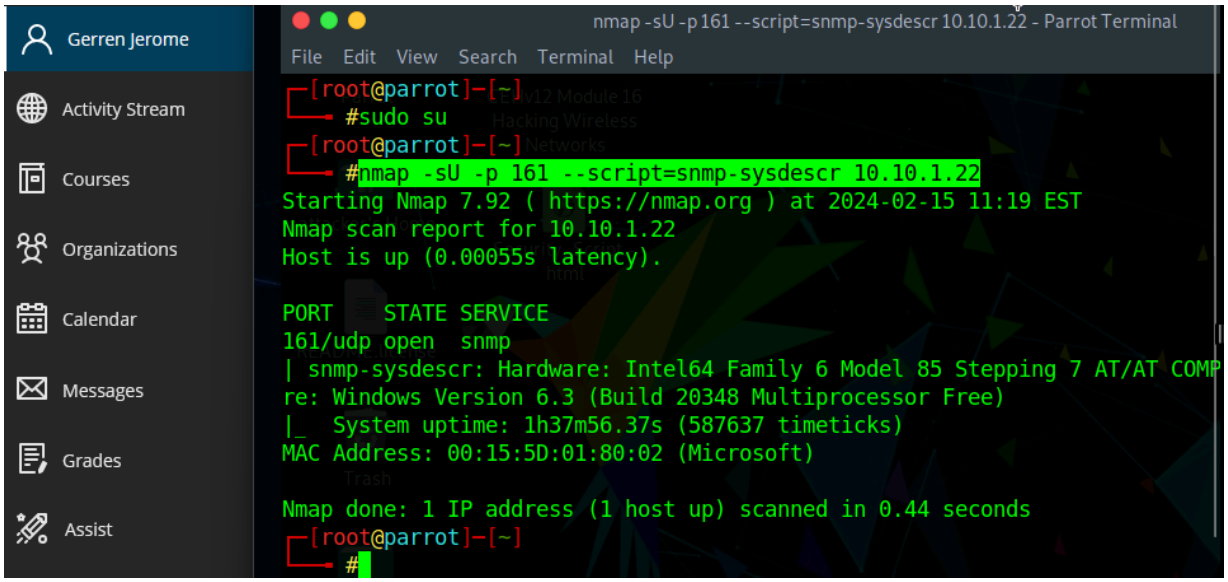
ii) **Screengrab: Step 8** – scan result (snmpwalk -v2c)



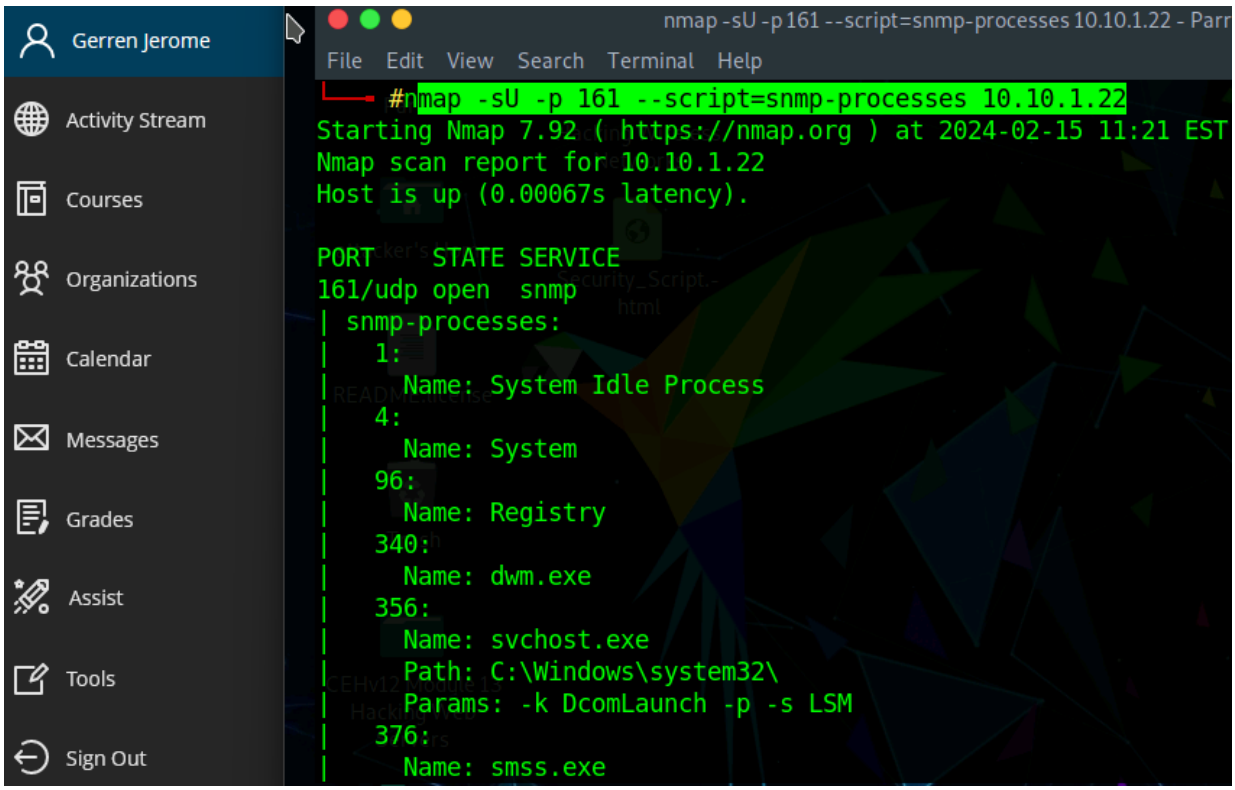
Gerren Jerome - Enumeration

d) SNMP enumeration via Nmap (4 tasks)

i) **Screengrab: Step 5** – scan result (type and description)

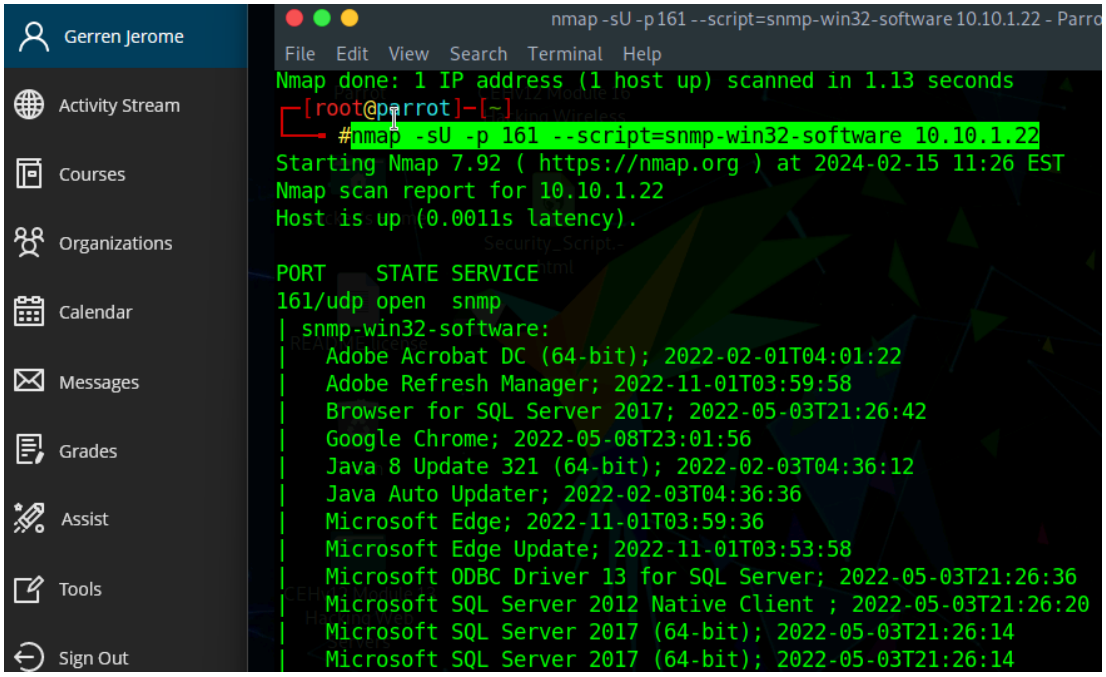


ii) **Screengrab: Step 7** – scan result (ports and processes)

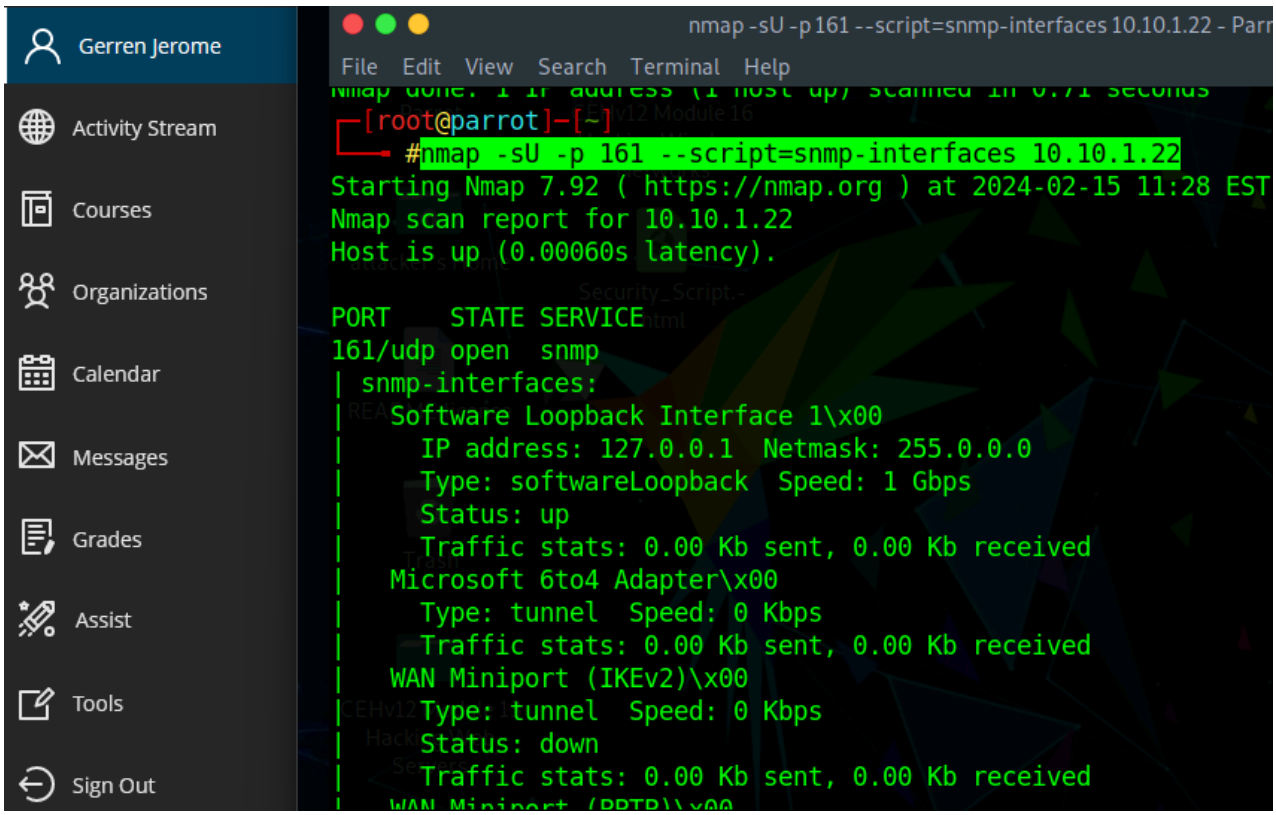


Gerren Jerome - Enumeration

iii) **Screengrab: Step 9** – scan result (applications)



iv) **Screengrab: Step 11** – scan result (interfaces)

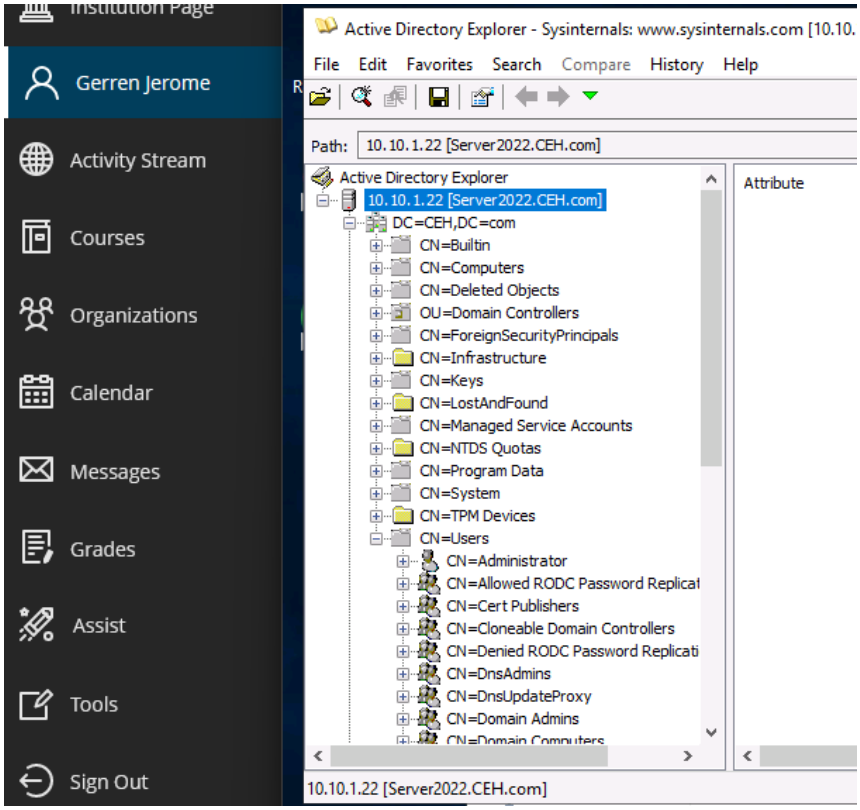


Gerren Jerome - Enumeration

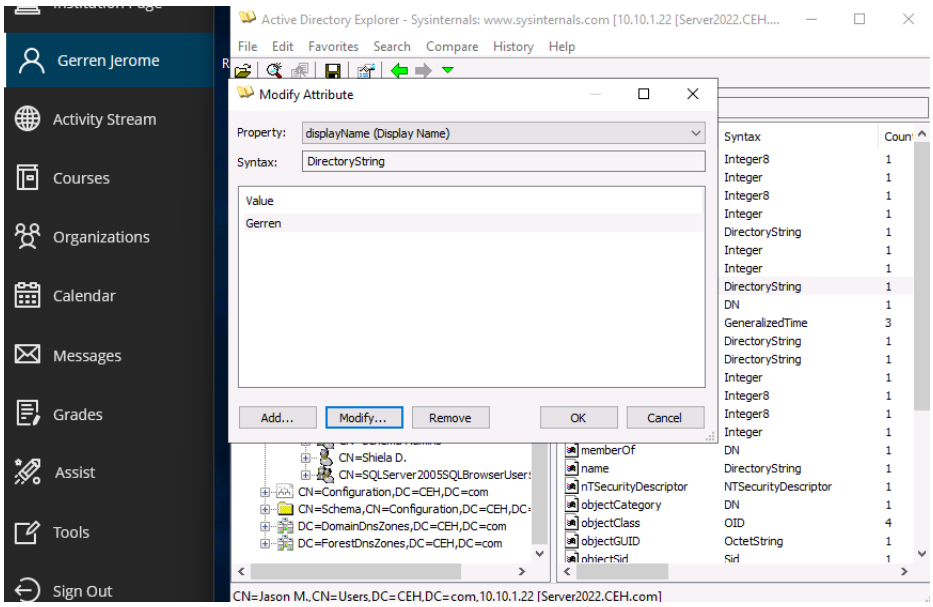
3) Perform enumeration (LDAP) (11 tasks)

a) Perform LDAP enumeration using Active Directory Explorer (AD Explorer) (2 tasks)

i) **Screengrab: Step 7** – Navigating ADExplorer



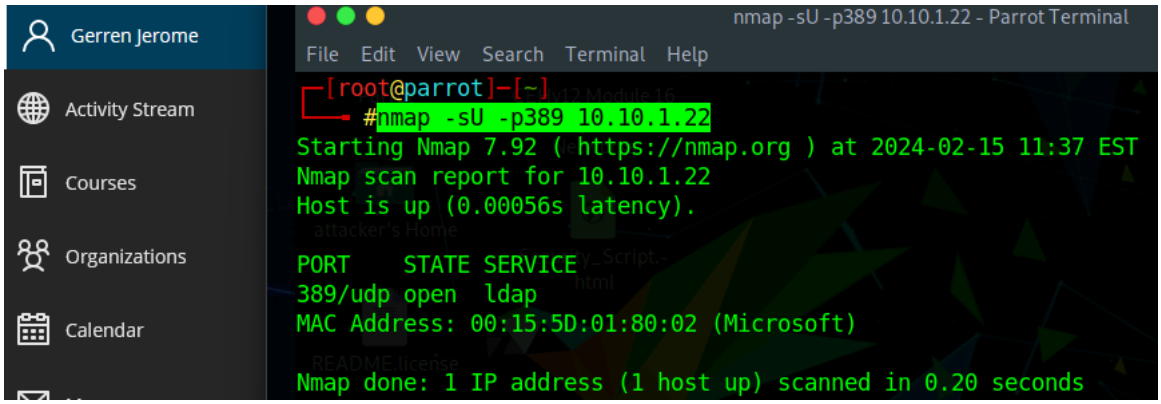
ii) **Screengrab: Step 10** – user attribute modification



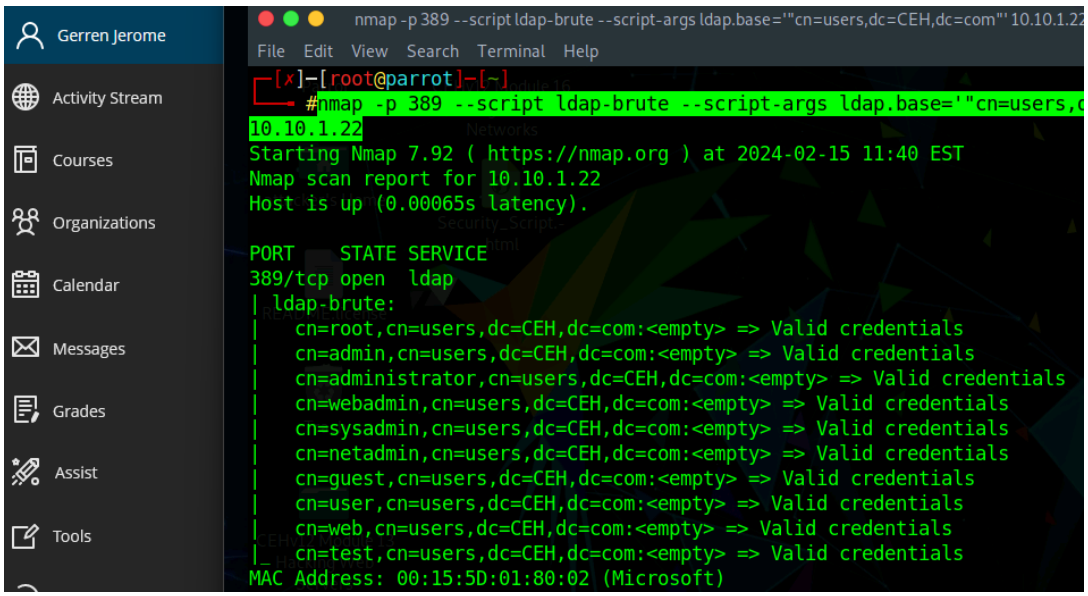
Gerren Jerome - Enumeration

b) Perform LDAP enumeration using Python and Nmap (6 tasks)

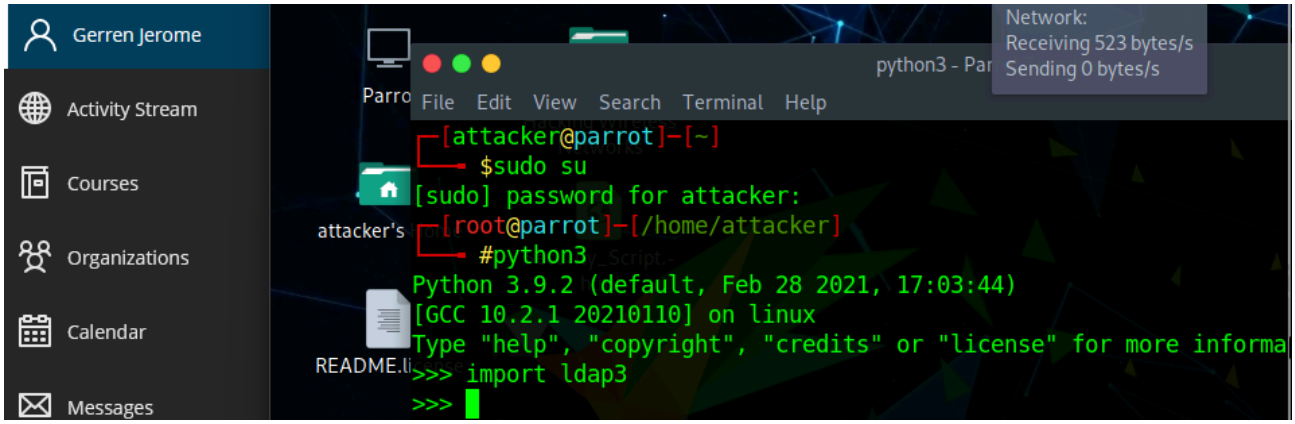
i) **Screengrab: Step 6** – scan result (Nmap -sU)



ii) **Screengrab: Step 9** – result (Nmap LDAP bruteforce)

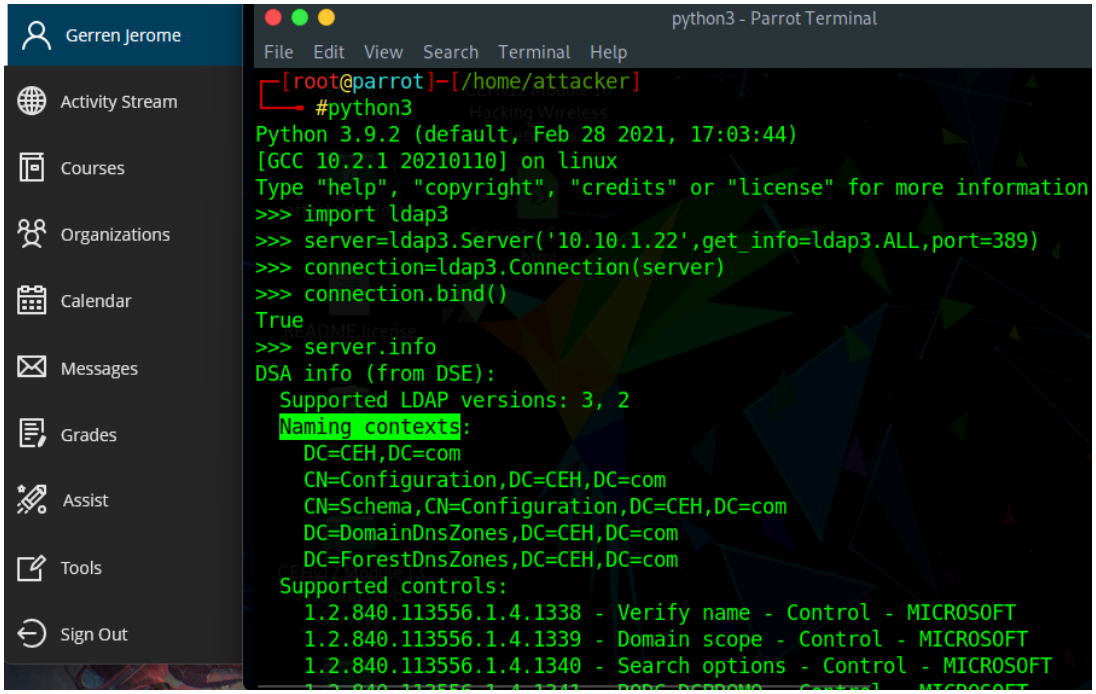


iii) **Screengrab: Step 15** – import ldap3 into Python

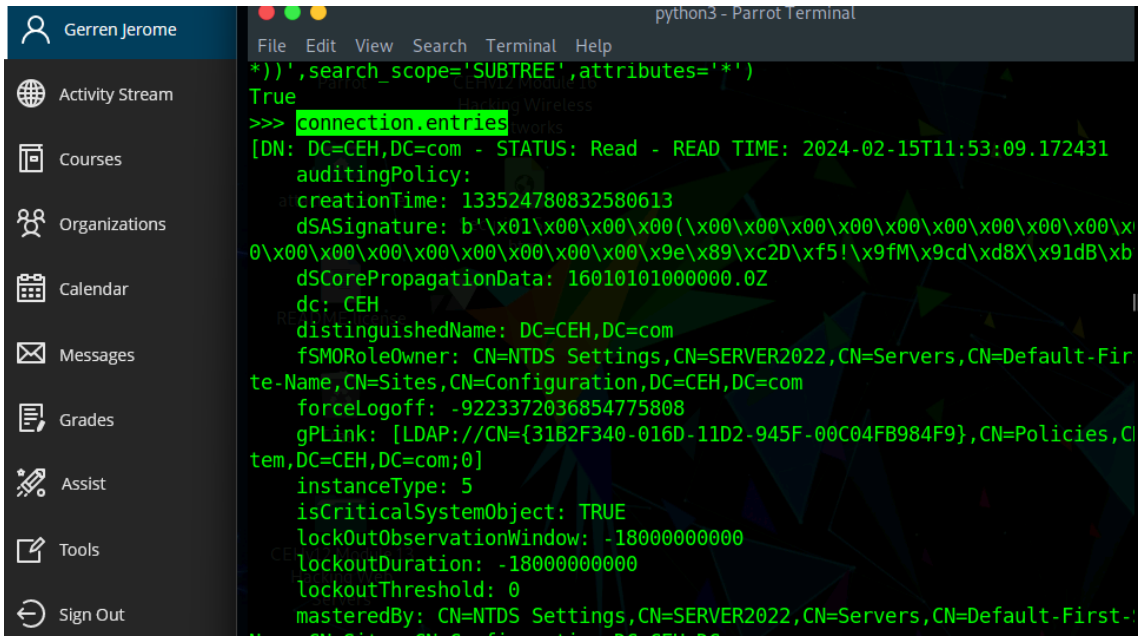


Gerren Jerome - Enumeration

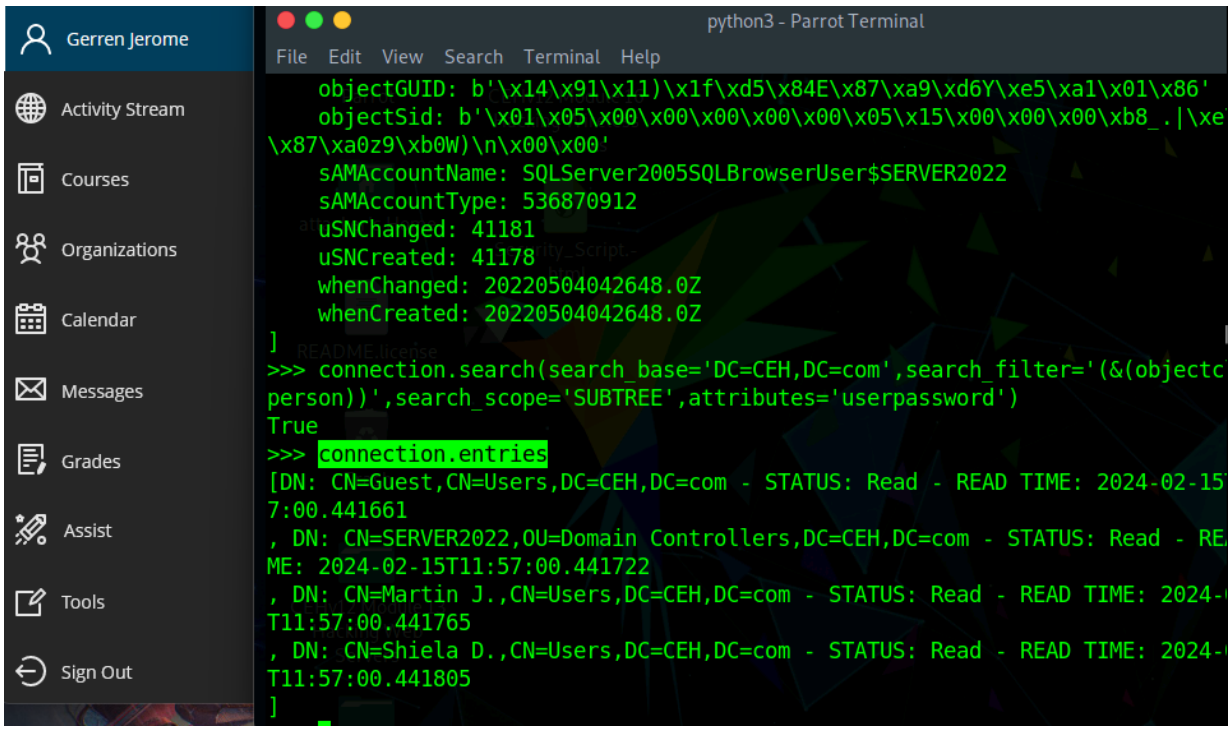
iv) **Screengrab: Step 21** – gain naming context



v) **Screengrab: Step 23** – retrieve directory objects

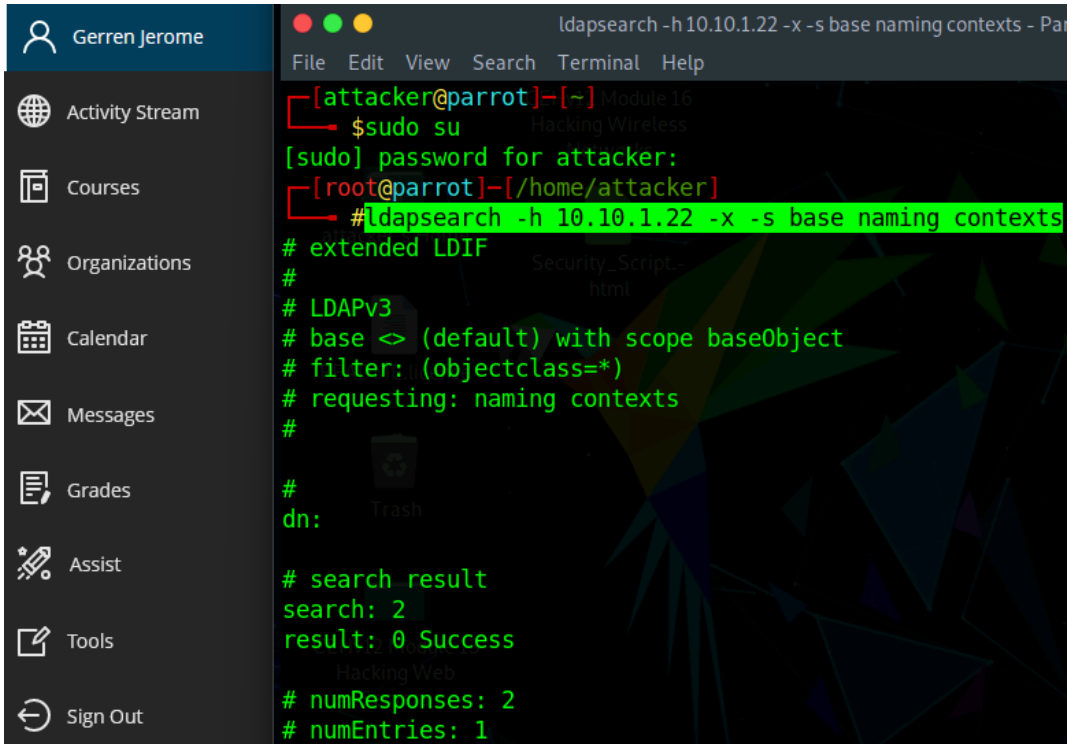


vi) **Screengrab: Step 25** – result (LDAP dump)



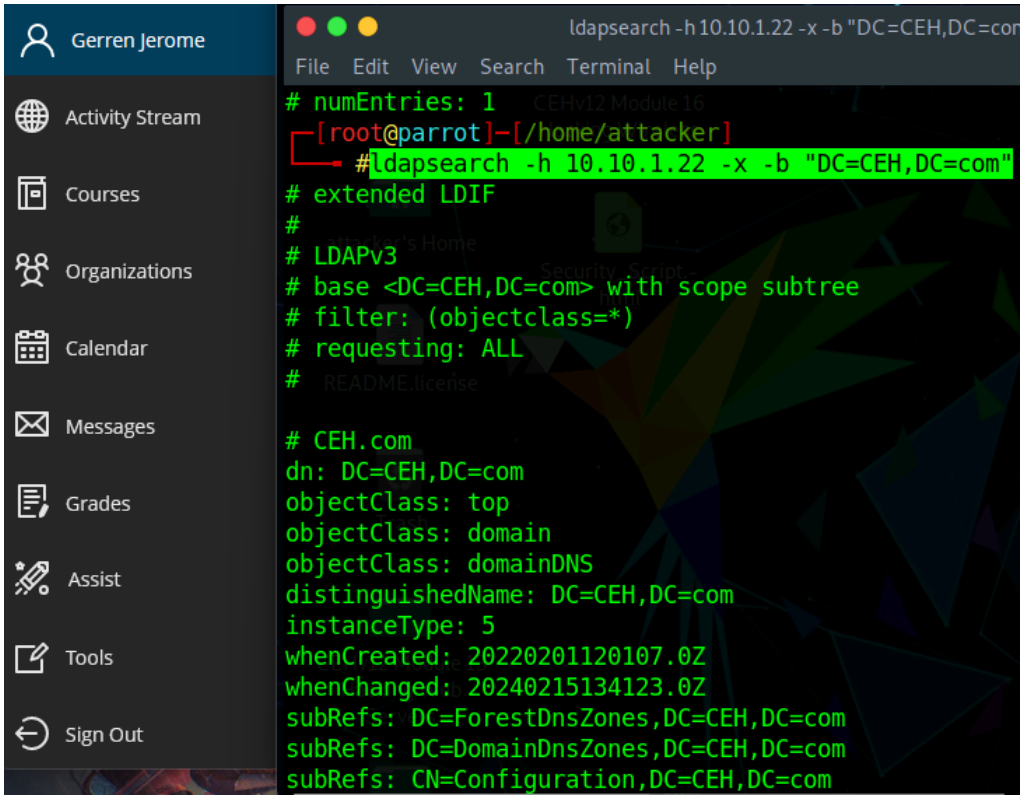
c) Perform LDAP enumeration using ldapsearch (3 tasks)

i) **Screengrab: Step 4** – gain naming context via ldapsearch

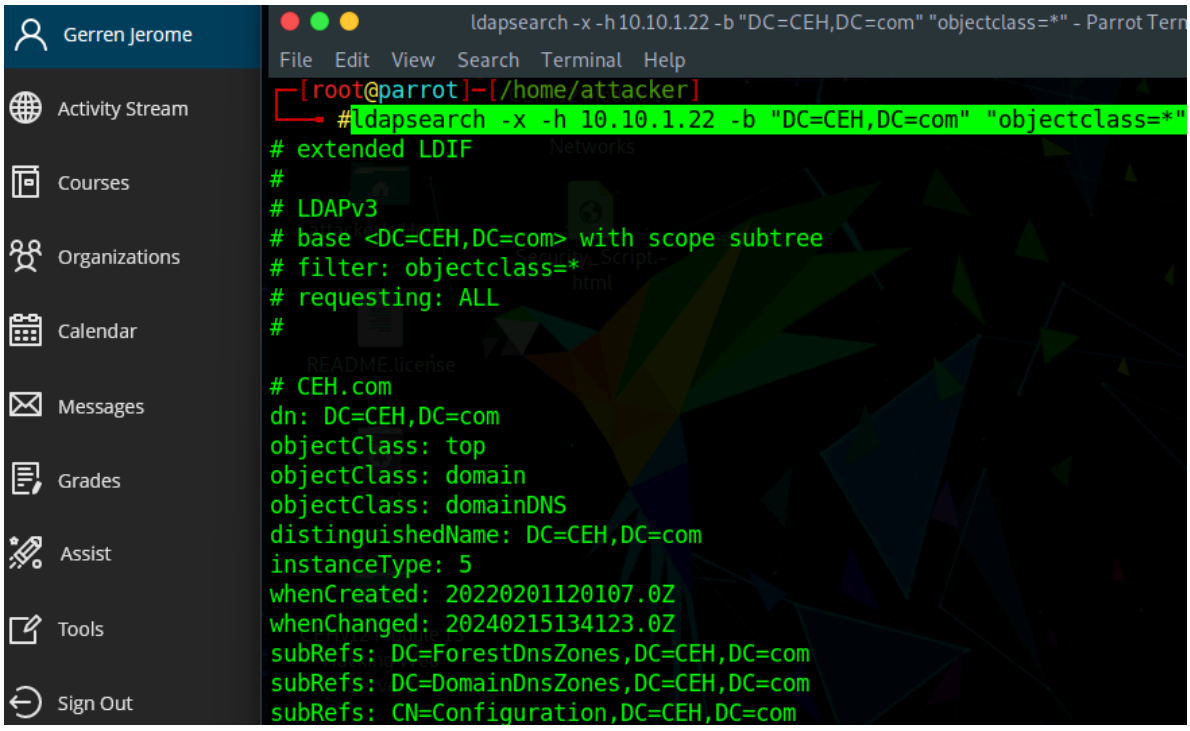


Gerren Jerome - Enumeration

ii) **Screengrab: Step 5** – more information about primary domain



iii) **Screengrab: Step 6** – retrieve info about objects in directory tree

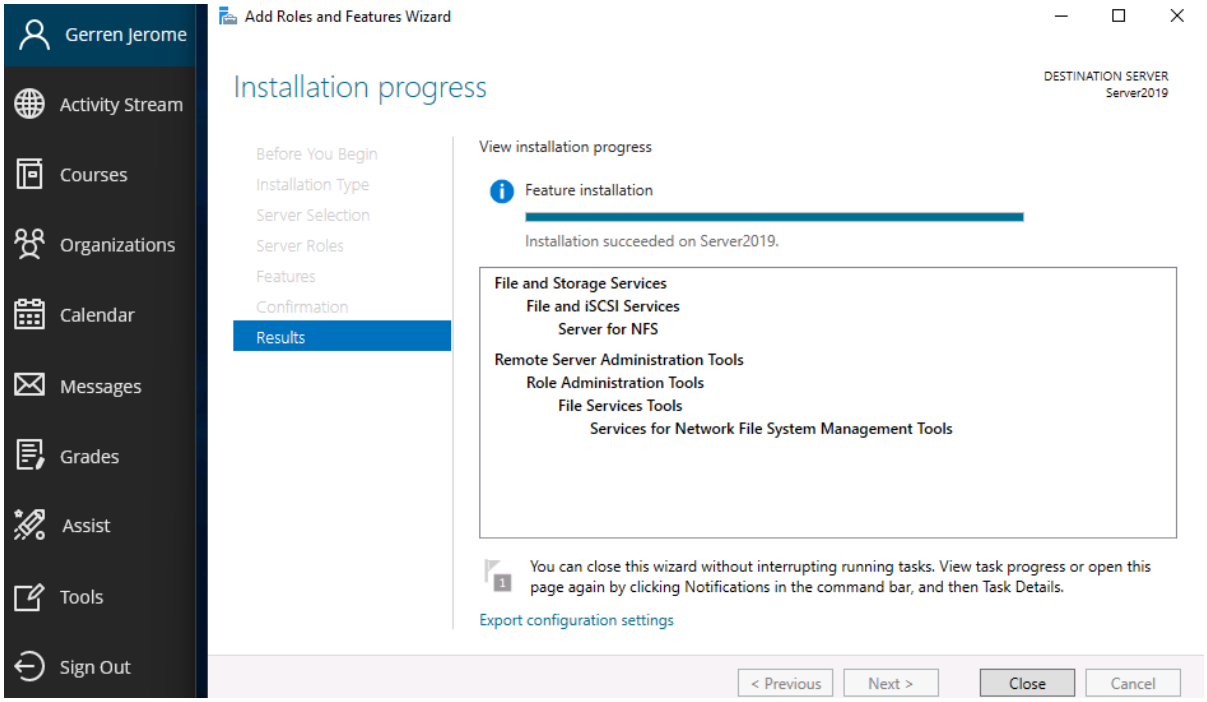


Gerren Jerome - Enumeration

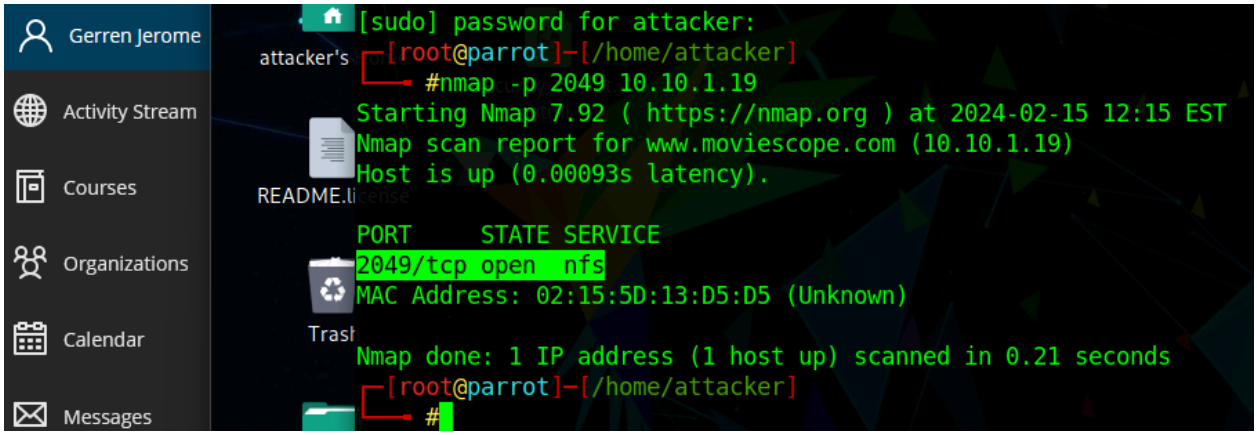
4) Perform enumeration (NFS) (4 tasks)

a) Perform NFS enumeration using RPCScan and SuperEnum (4 tasks)

i) **Screengrab: Step 6** – confirm install/enable of NFS service in Windows

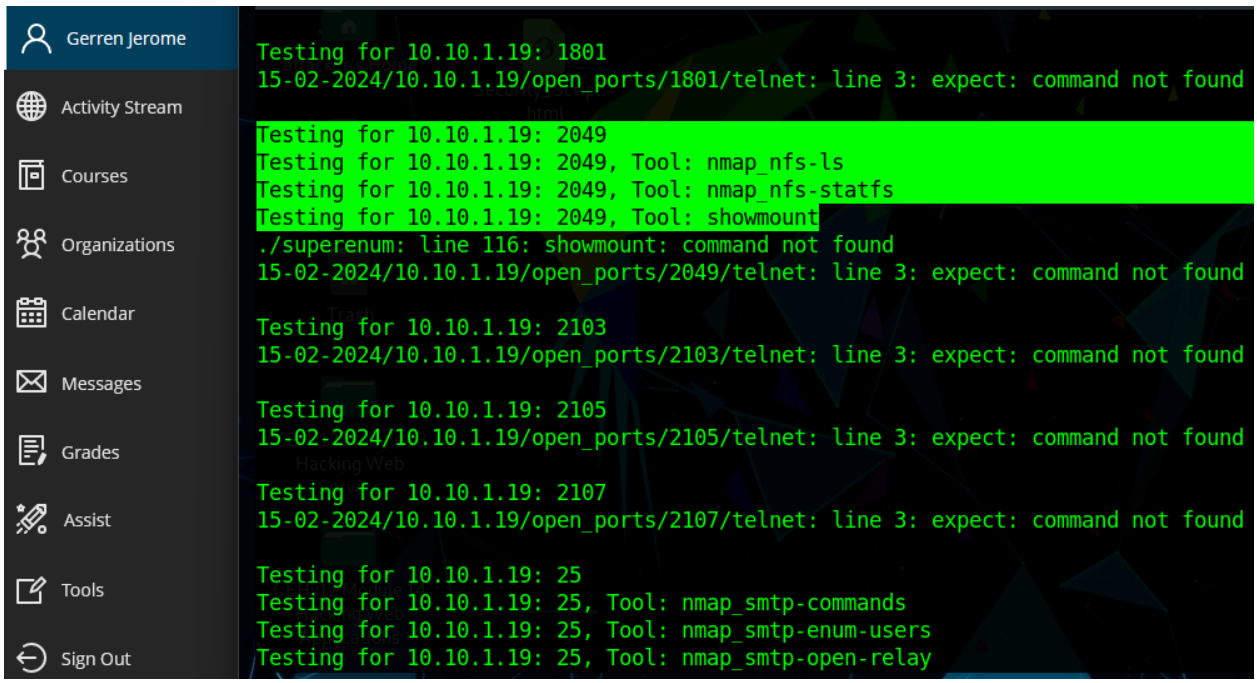


ii) **Screengrab: Step 13** – scan result (NFS running?)

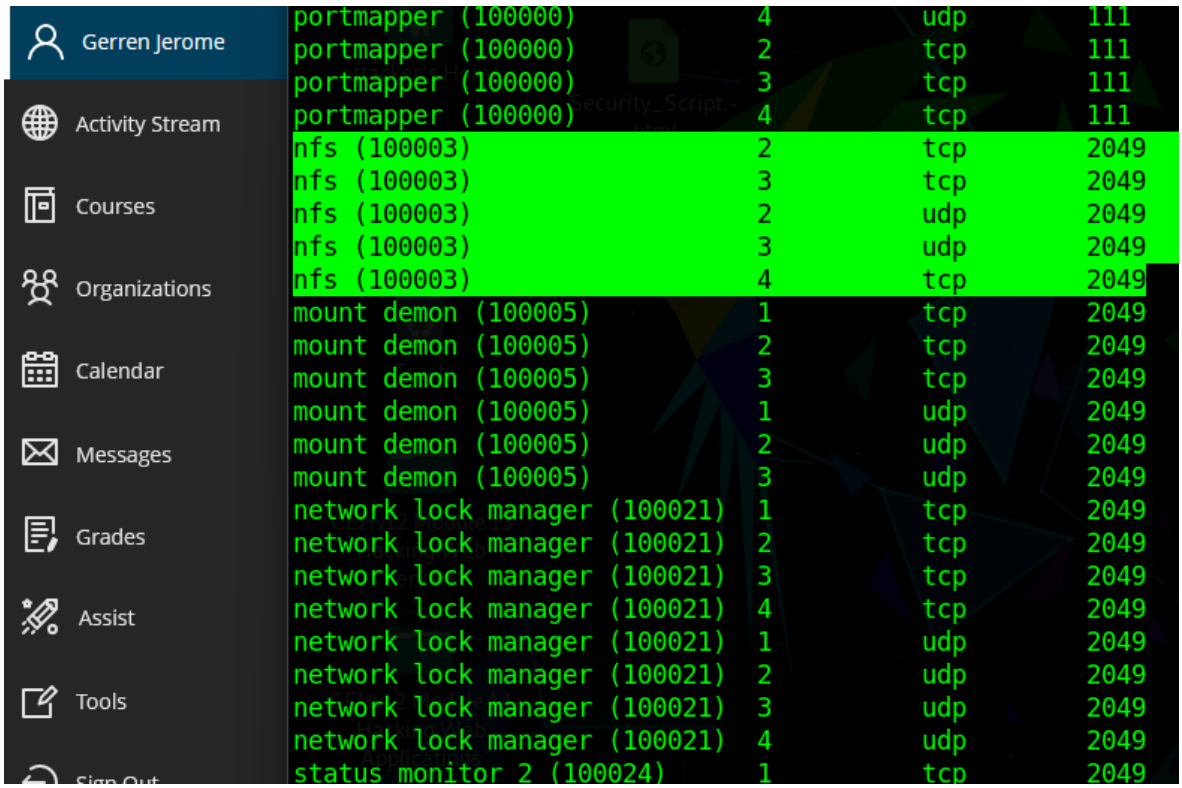


Gerren Jerome - Enumeration

iii) **Screengrab: Step 18** – scan result (SuperEnum)



iv) **Screengrab: Step 23** – scan result (RPCScan)

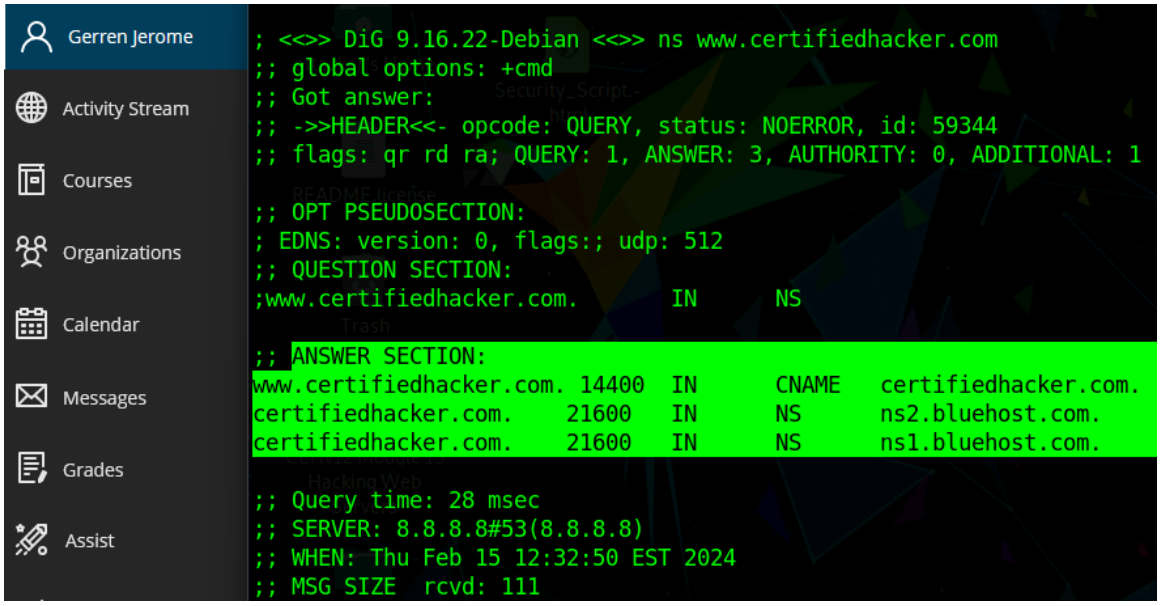


Gerren Jerome - Enumeration

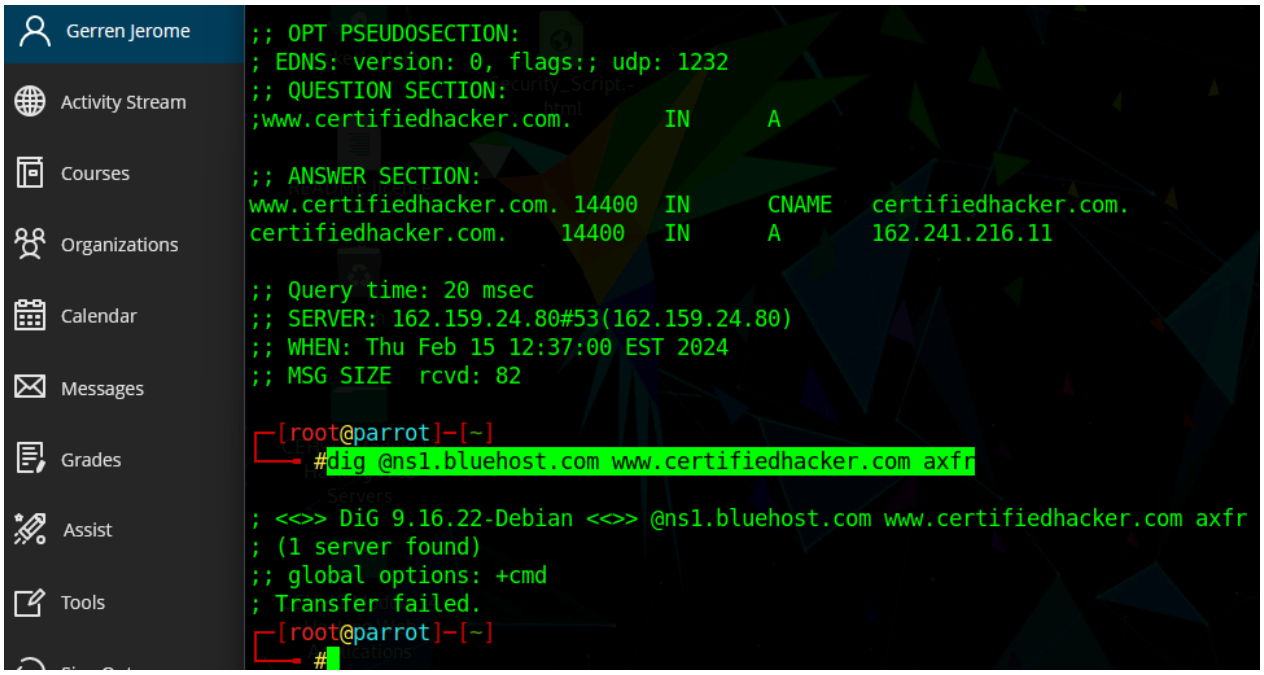
5) Perform enumeration (DNS) (8 tasks)

a) Perform DNS enumeration using zone transfer (4 tasks)

i) **Screengrab: Step 7** – scan result (dig ns www.certifiedhacker.com)

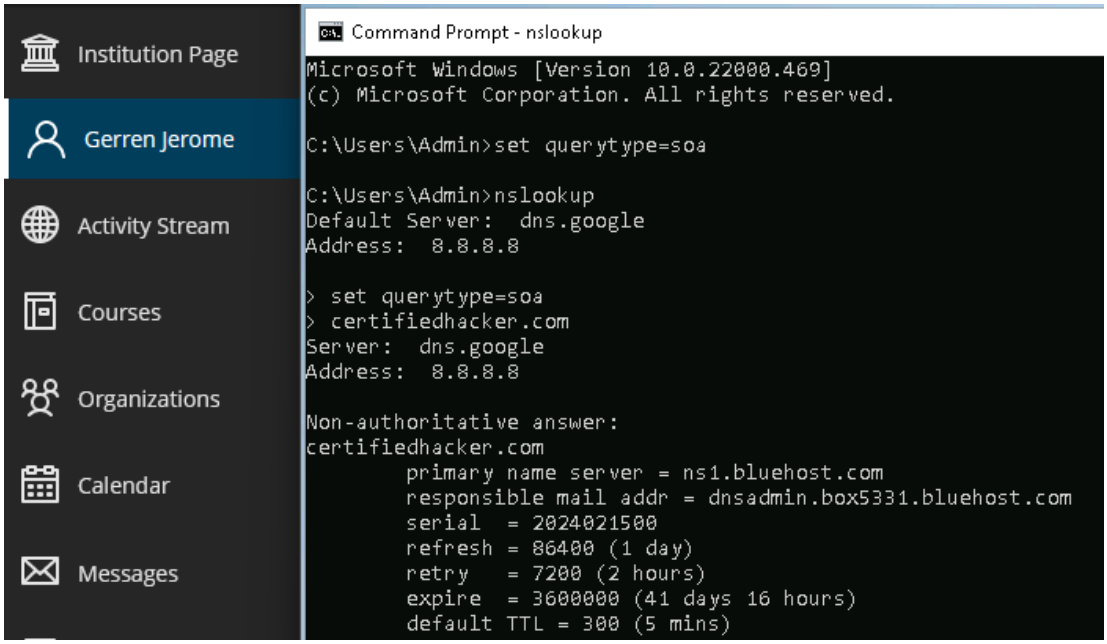


ii) **Screengrab: Step 9** – scan result (dig transfer failed?)

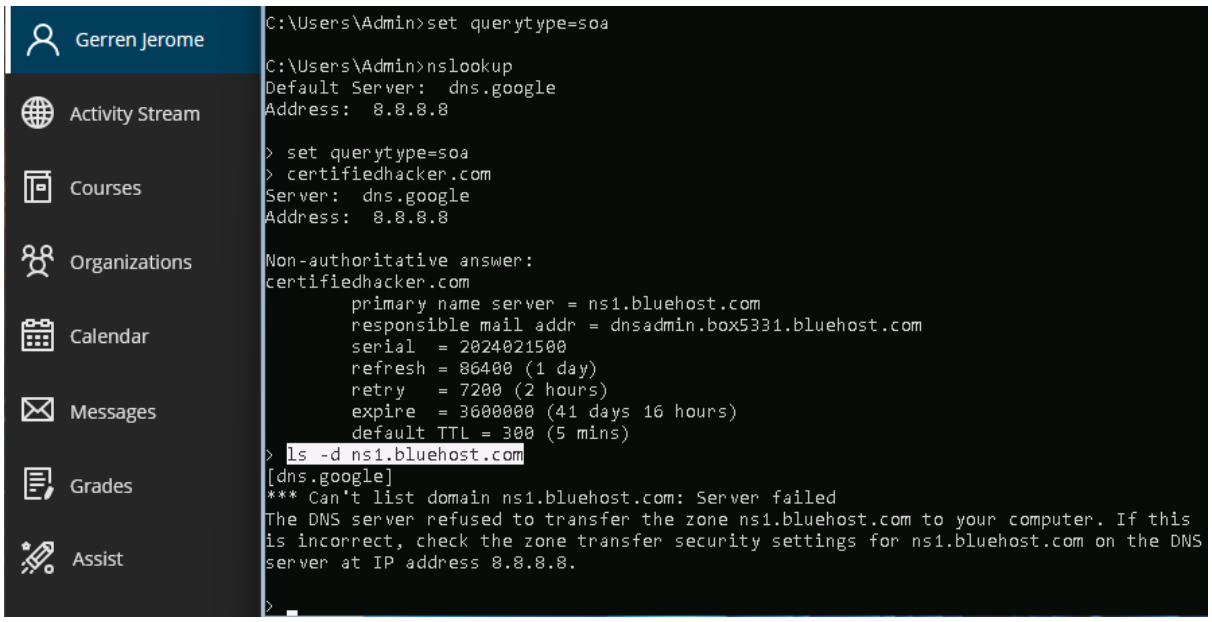


Gerren Jerome - Enumeration

iii) **Screengrab: Step 17** – scan result (nslookup (interactive mode) – certifiedhacker)



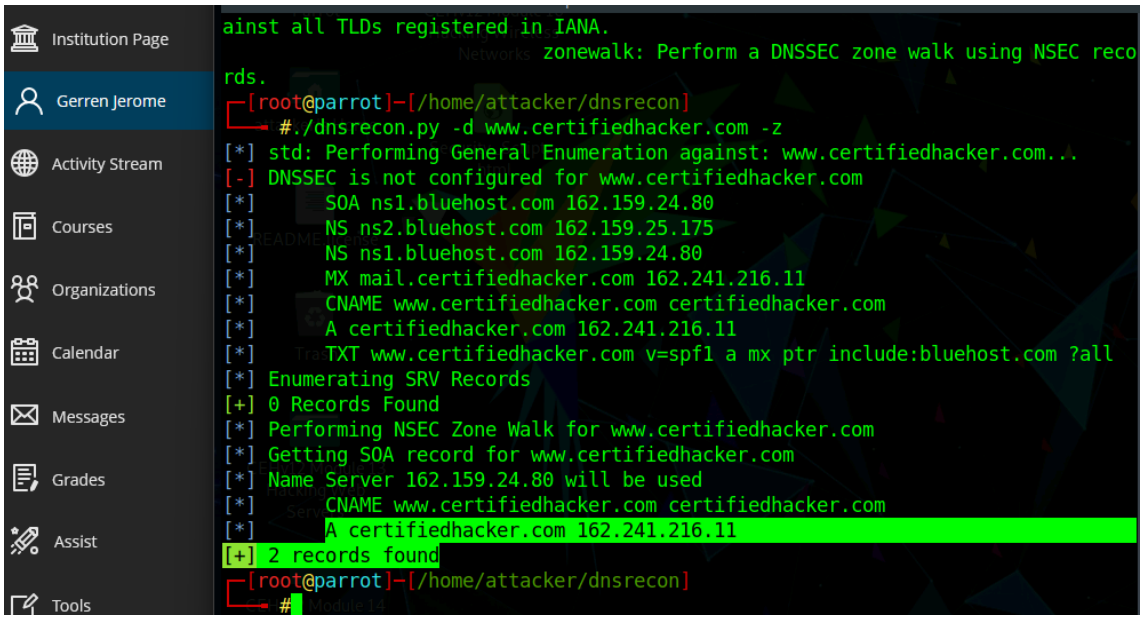
iv) **Screengrab: Step 19** – scan result (nslookup (interactive mode) – bluehost)



Gerren Jerome - Enumeration

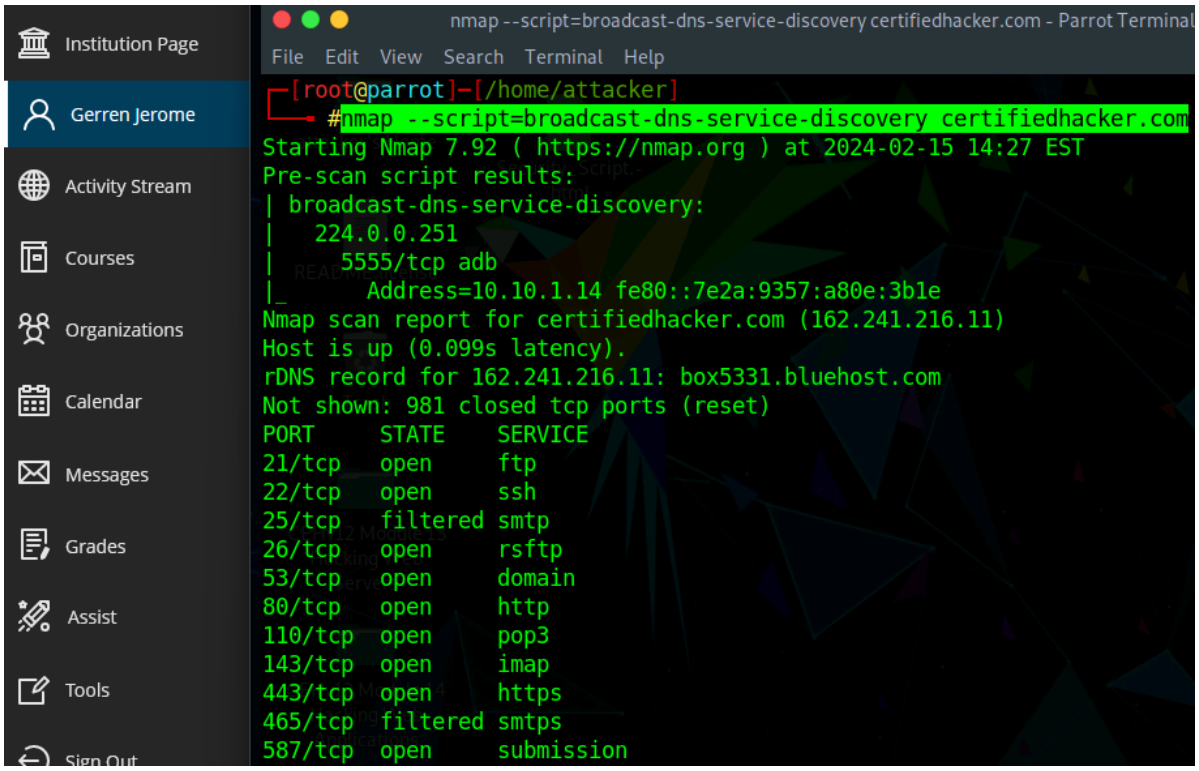
b) Perform DNS enumeration using DNSSEC zone walking (1 task)

i) **Screengrab: Step 8** – result (dnsrecon – certifiedhacker)



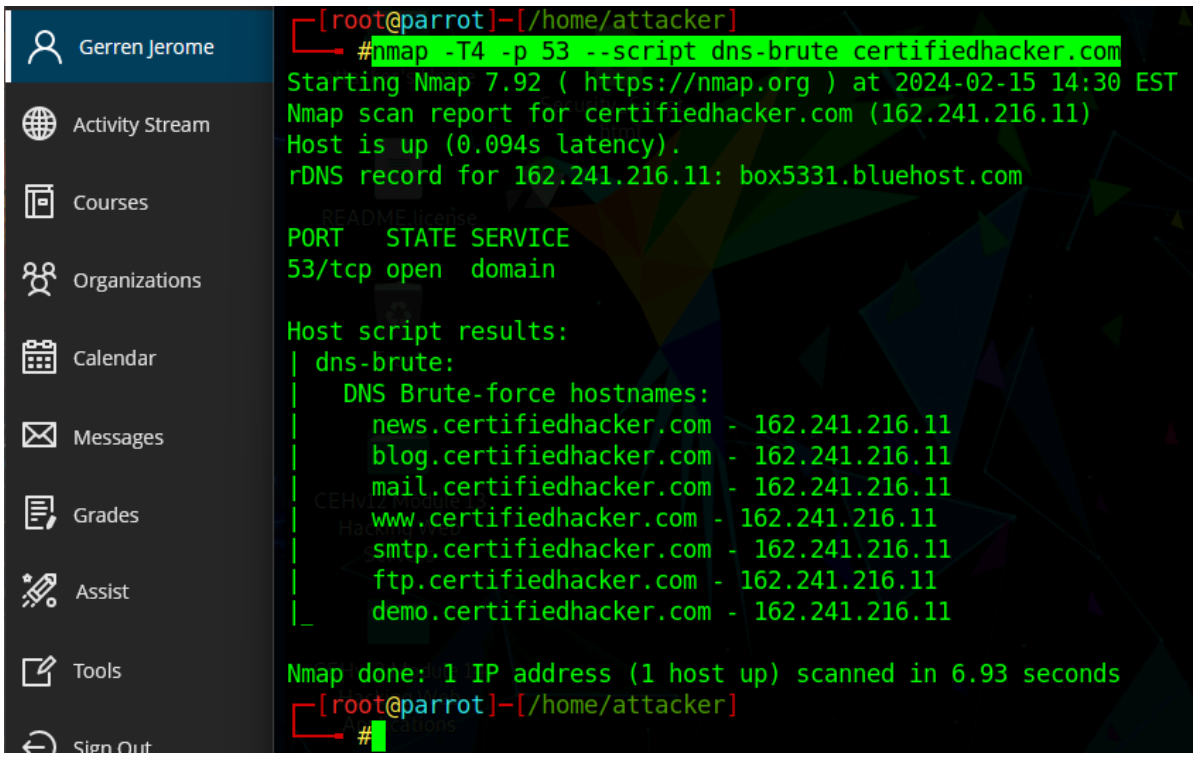
c) Perform DNS enumeration using Nmap (3 tasks)

i) **Screengrab: Step 5** – scan result (nmap service discovery)

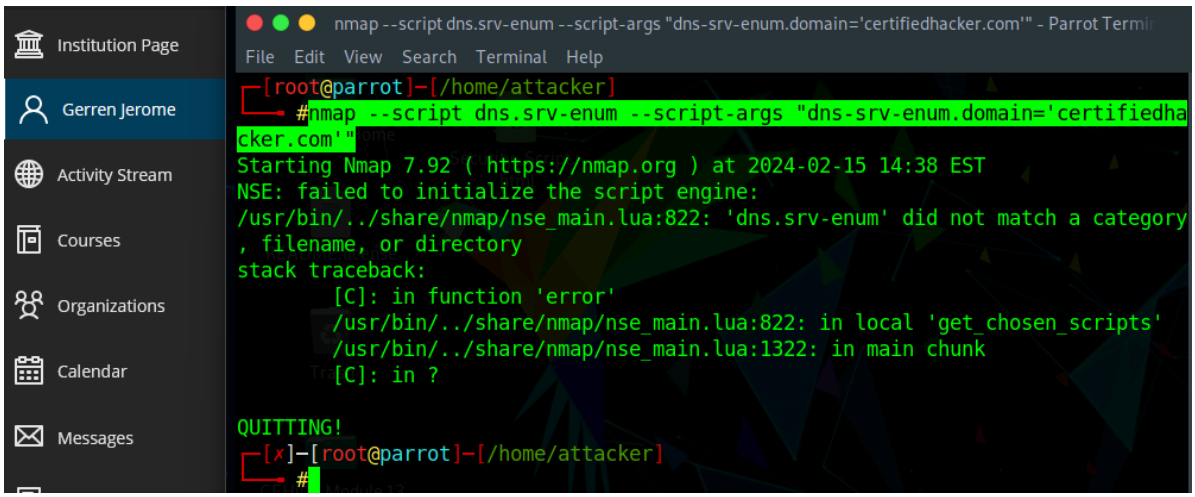


Gerren Jerome - Enumeration

ii) **Screengrab: Step 7** – scan result (associated subdomains)



iii) **Screengrab: Step 9** – scan result (SRV records)

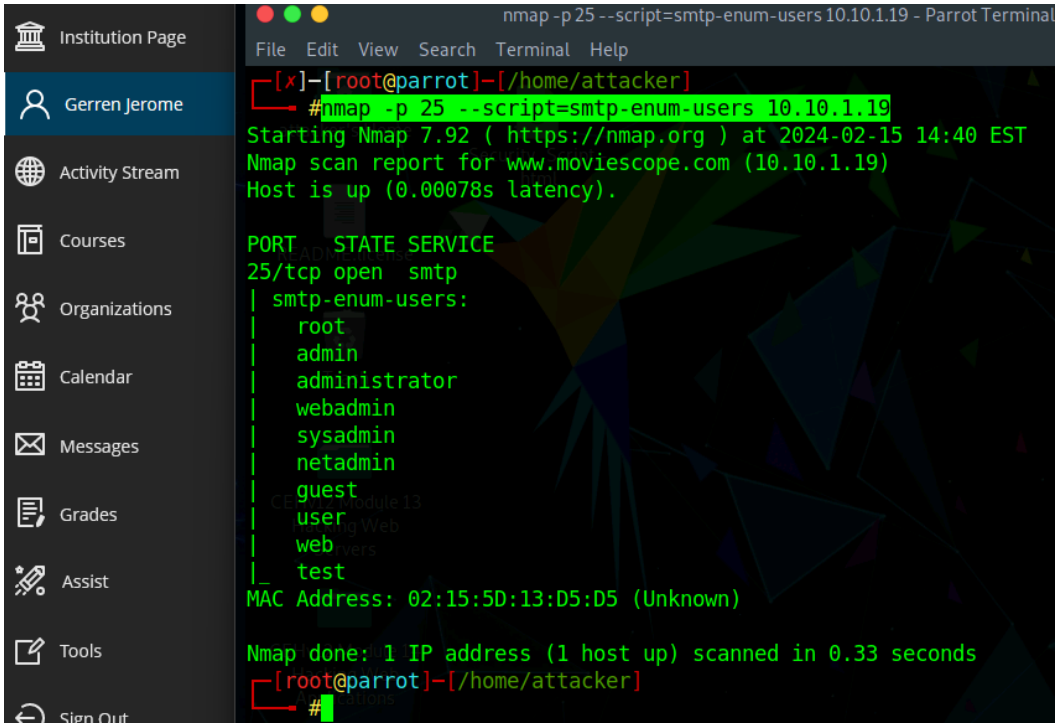


Gerren Jerome - Enumeration

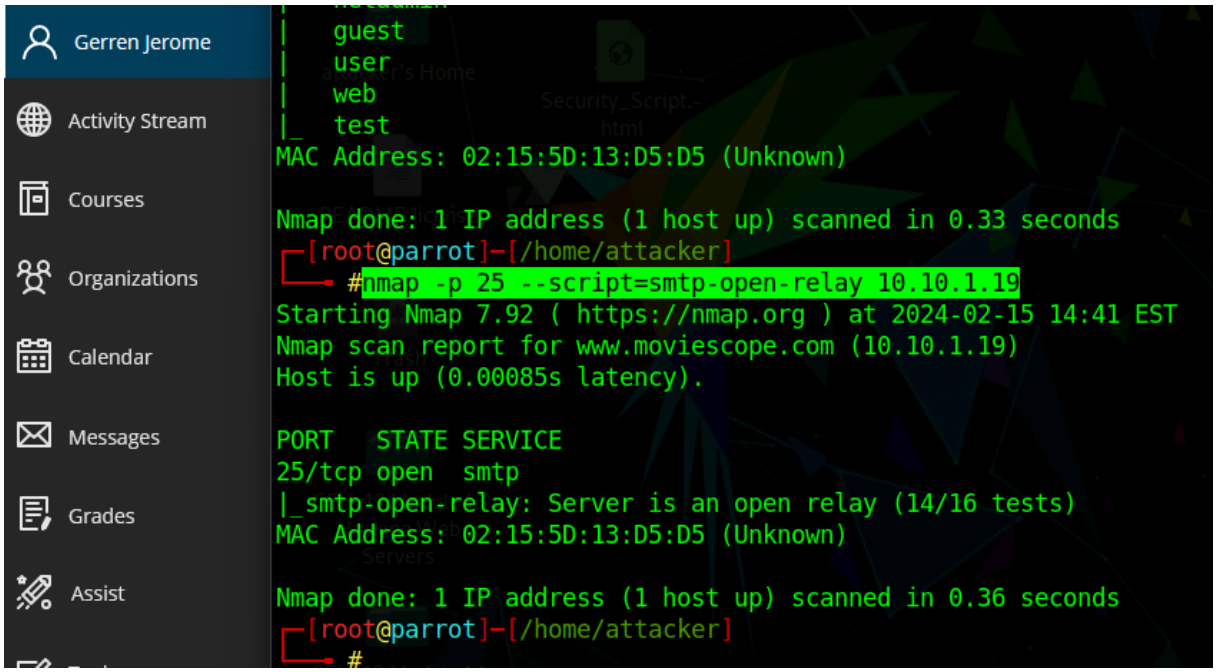
6) Perform enumeration (SMTP) (2 tasks)

a) Perform SMTP enumeration using Nmap (2 tasks)

i) **Screengrab: Step 5** – list all mail users



ii) **Screengrab: Step 7** – list open SMTP relays

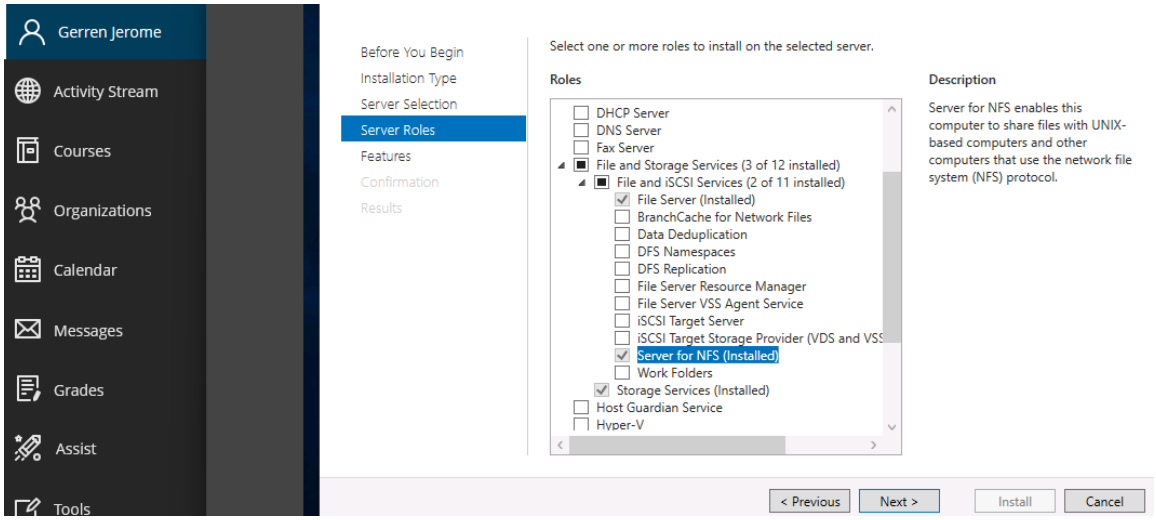


Gerren Jerome - Enumeration

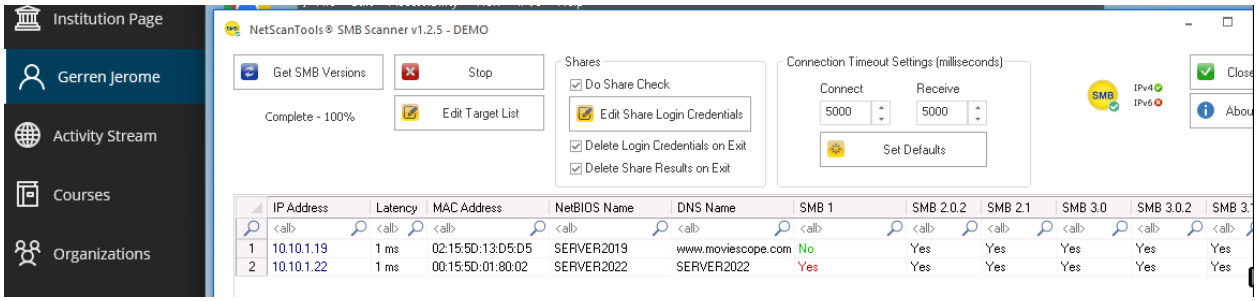
7) Perform enumeration (RPC, SMB, and FTP) (8 tasks)

a) Perform SMB and RPC enumeration using NetScanTools Pro (3 tasks)

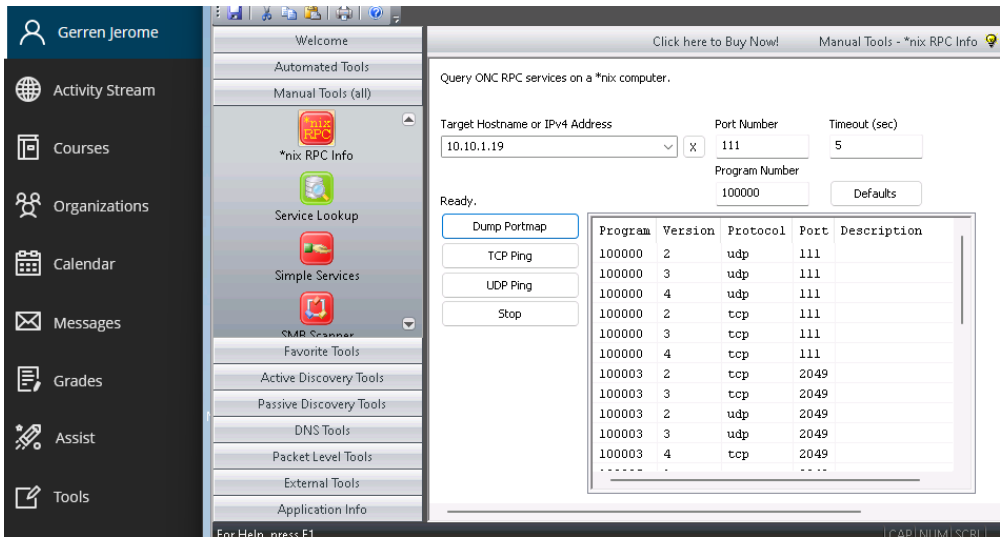
i) **Screengrab: Step 6** – confirm install/enable NFS services



ii) **Screengrab: Step 22** – SMB scanner results



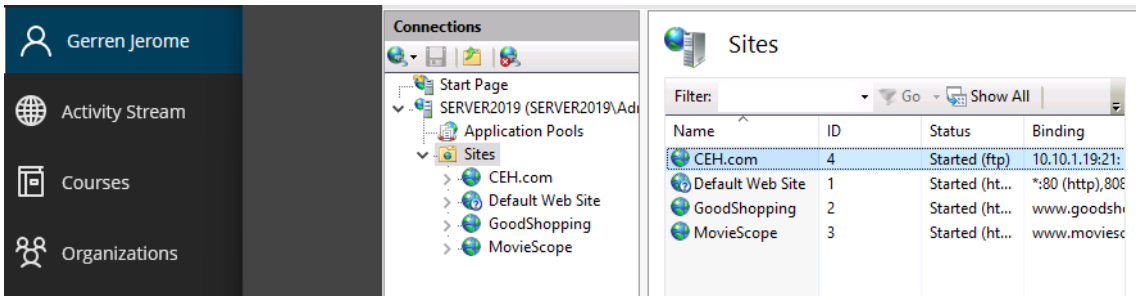
iii) **Screengrab: Step 28** – portmap dump (WIN_SVR_19)



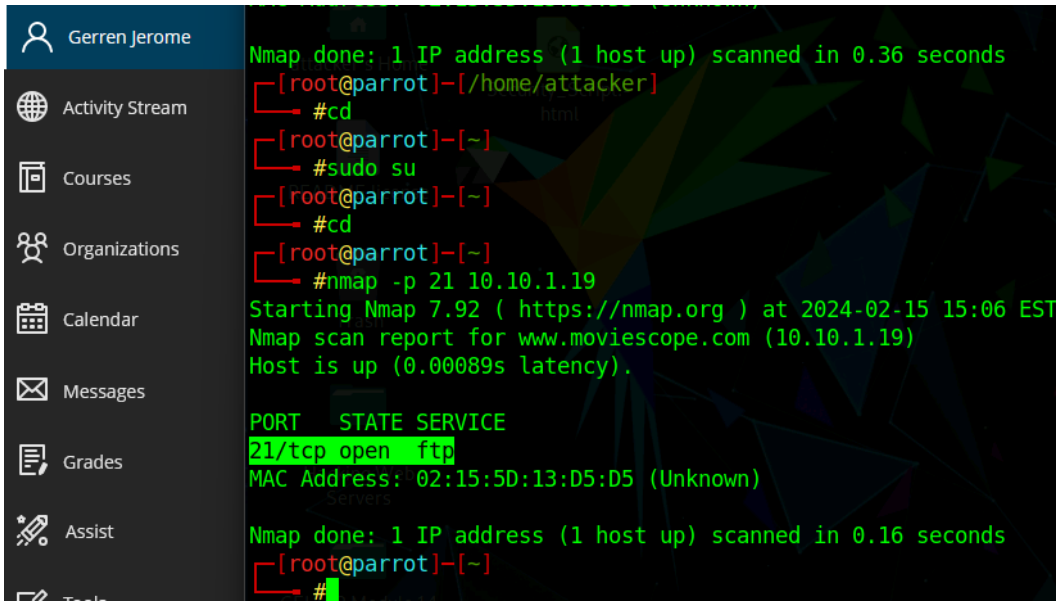
Gerren Jerome - Enumeration

b) Perform RPC, SMB, and FTP enumeration using Nmap (5 tasks)

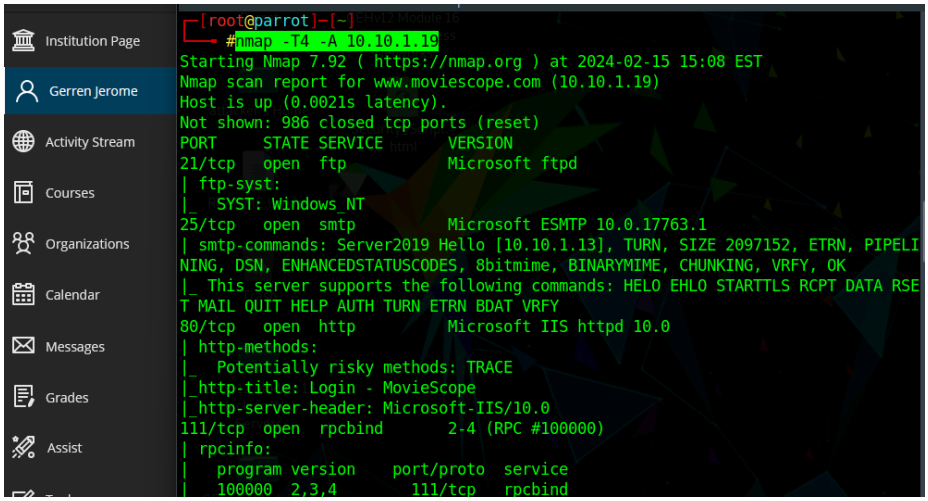
i) **Screengrab: Step 10** – confirm addition of CEH.com FTP site to IIS



ii) **Screengrab: Step 18** – nmap scan (Port 21 - FTP)

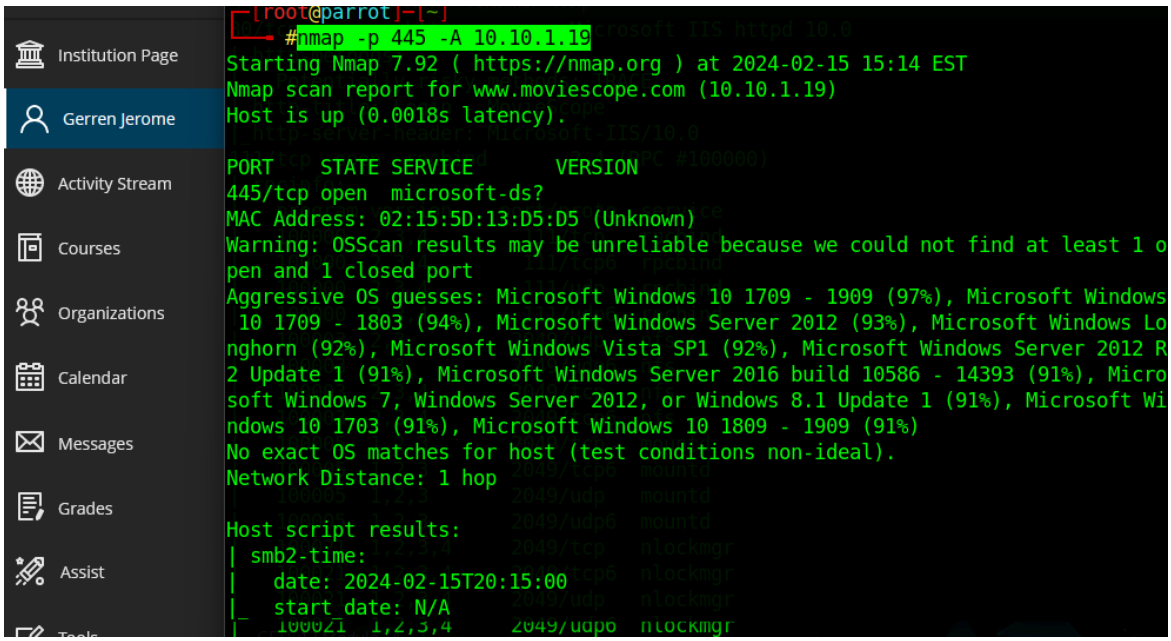


iii) **Screengrab: Step 20** – nmap scan (other services and ports)

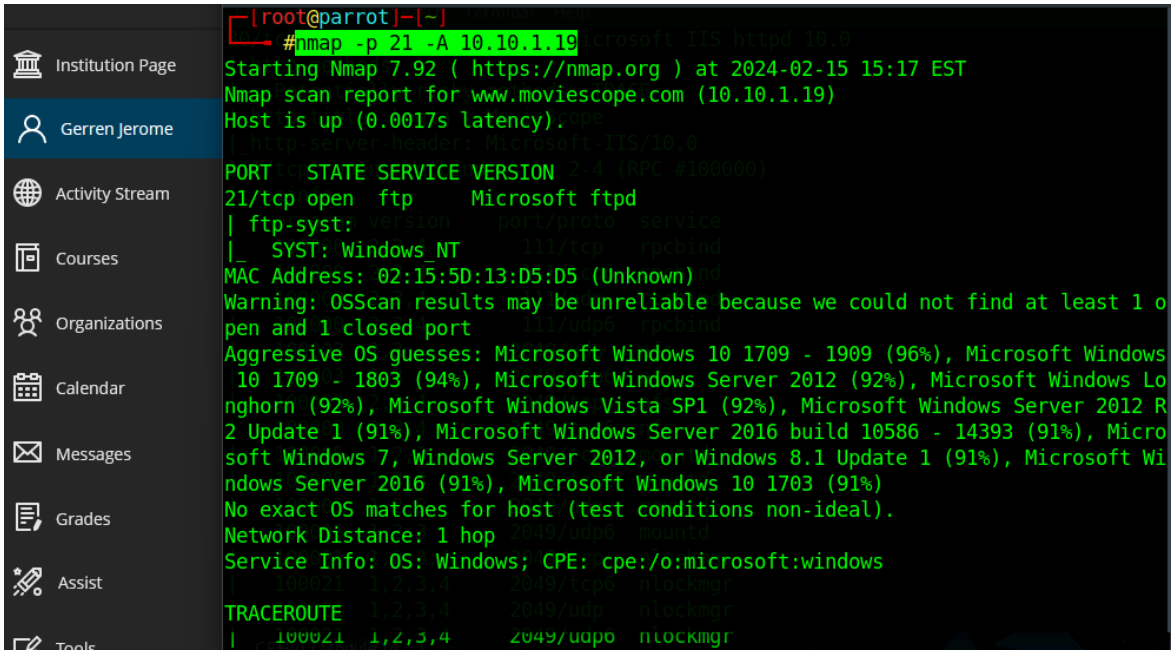


Gerren Jerome - Enumeration

iv) **Screengrab: Step 25** – nmap scan (Port 445 – SMB)



v) **Screengrab: Step 28** – nmap scan (Port 21 + traceroute)

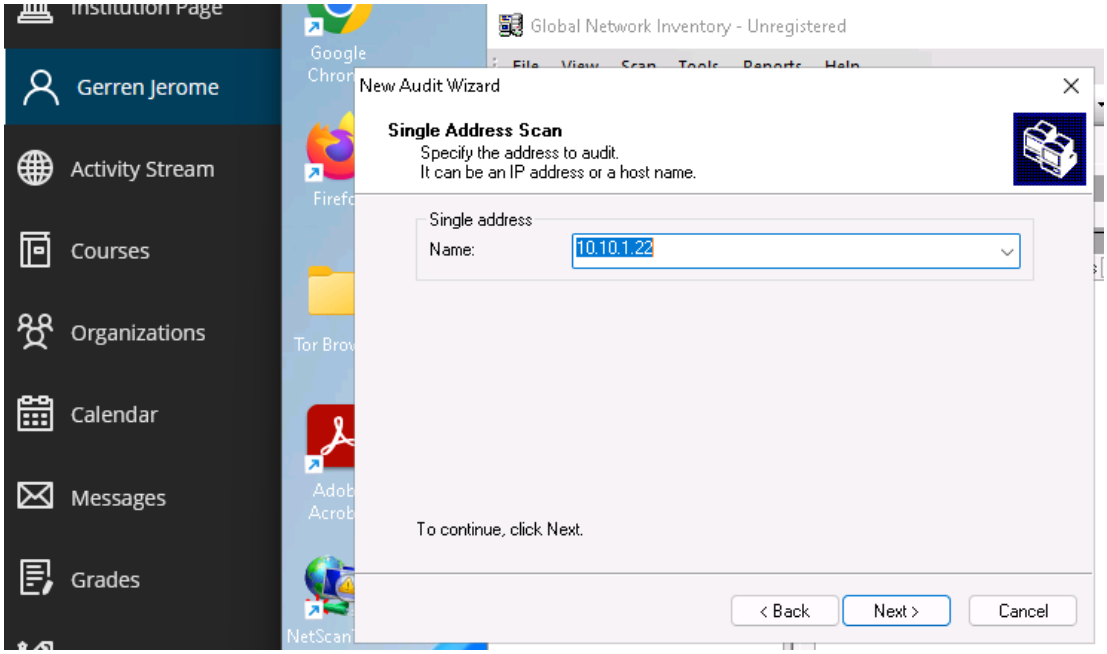


Gerren Jerome - Enumeration

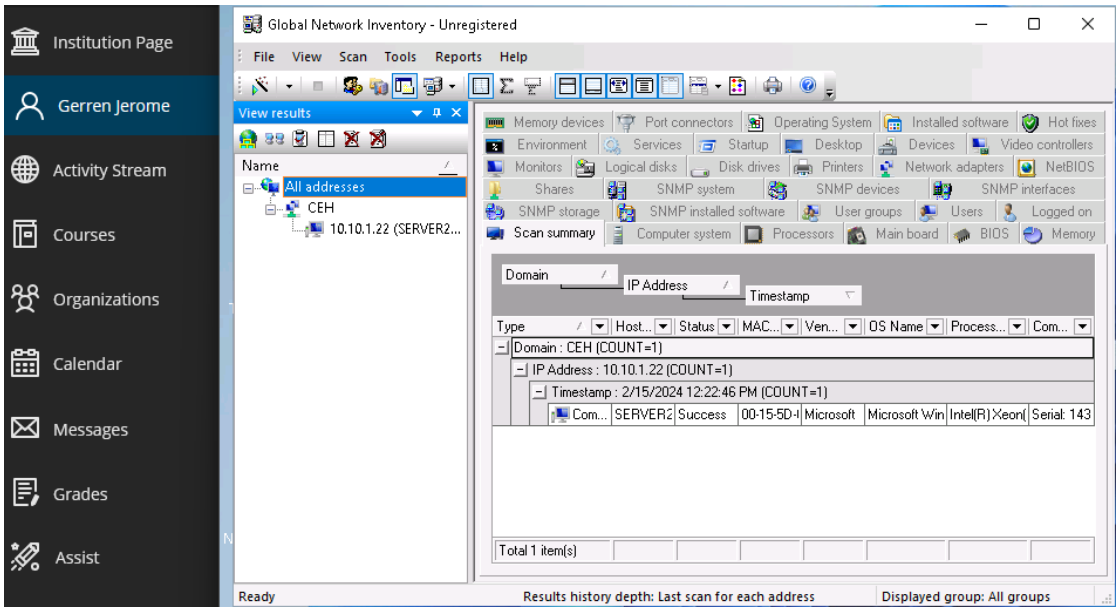
8) Perform enumeration using various enumeration tools (XX tasks)

a) Enumerate information using Global Network Inventory (6 tasks)

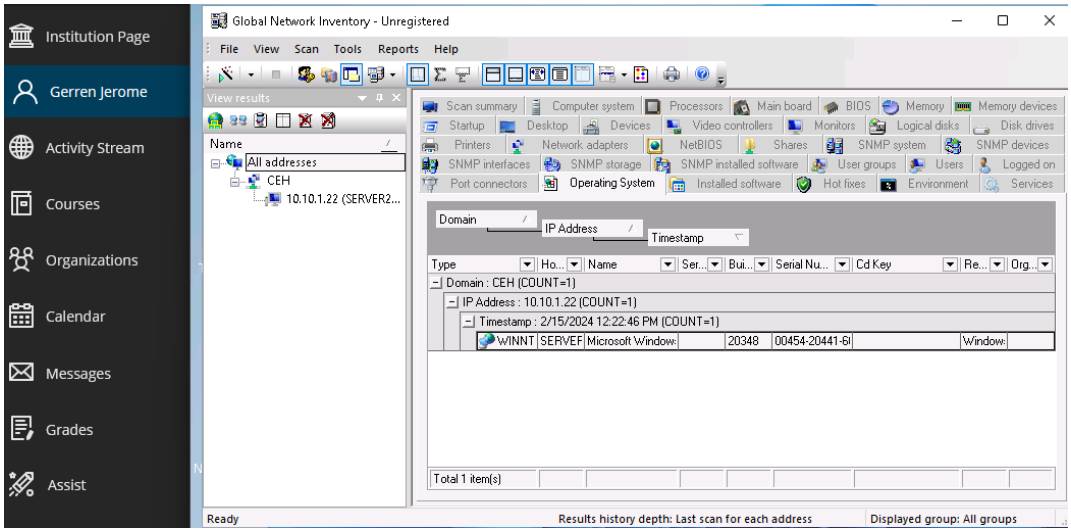
i) **Screengrab: Step 6** – confirm settings (GNI single address scan)



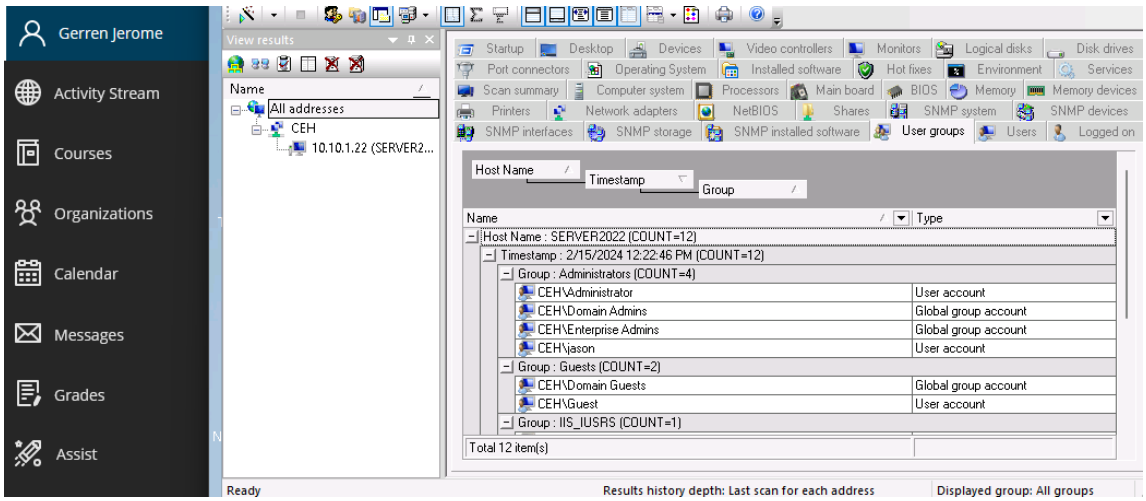
ii) **Screengrab: Step 10** – Scan summary (GNI)



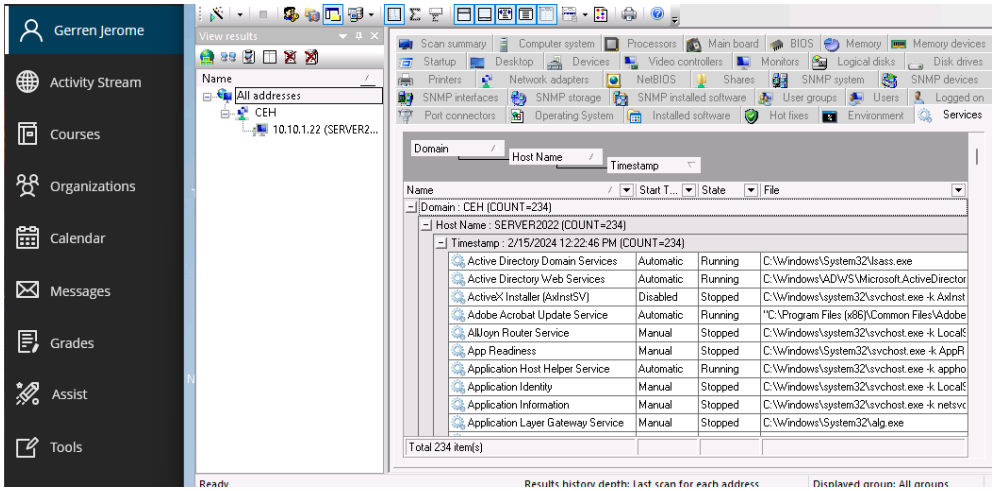
iii) **Screengrab: Step 12** – GNI Scan Result (Operating System)



iv) **Screengrab: Step 15** – GNI Scan Result (User Groups)

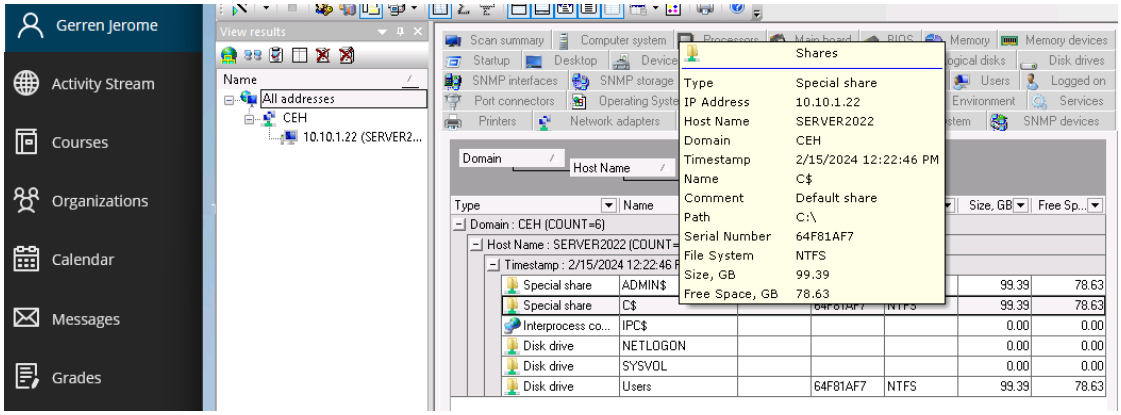


v) **Screengrab: Step 17** – GNI Scan Result (Services)



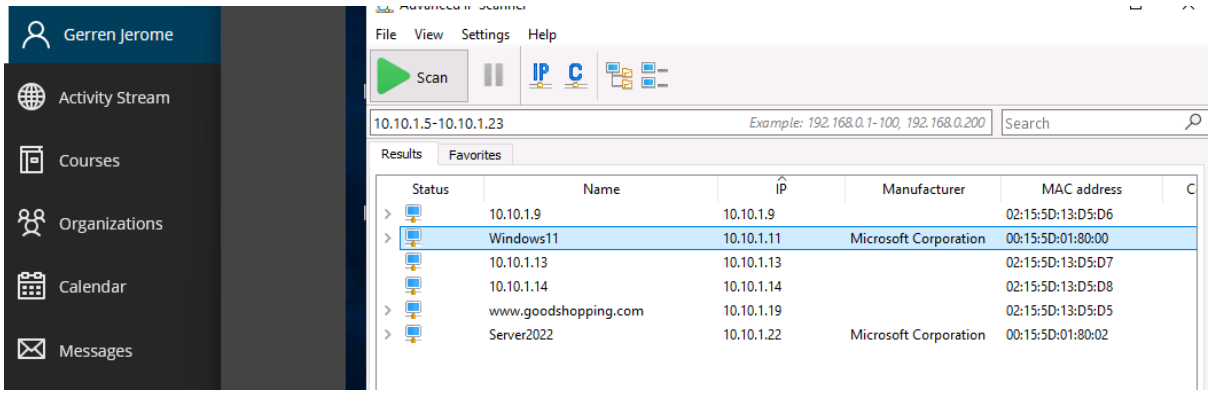
Gerren Jerome - Enumeration

vi) **Screengrab: Step 19** – GNI Scan Result (Shares)



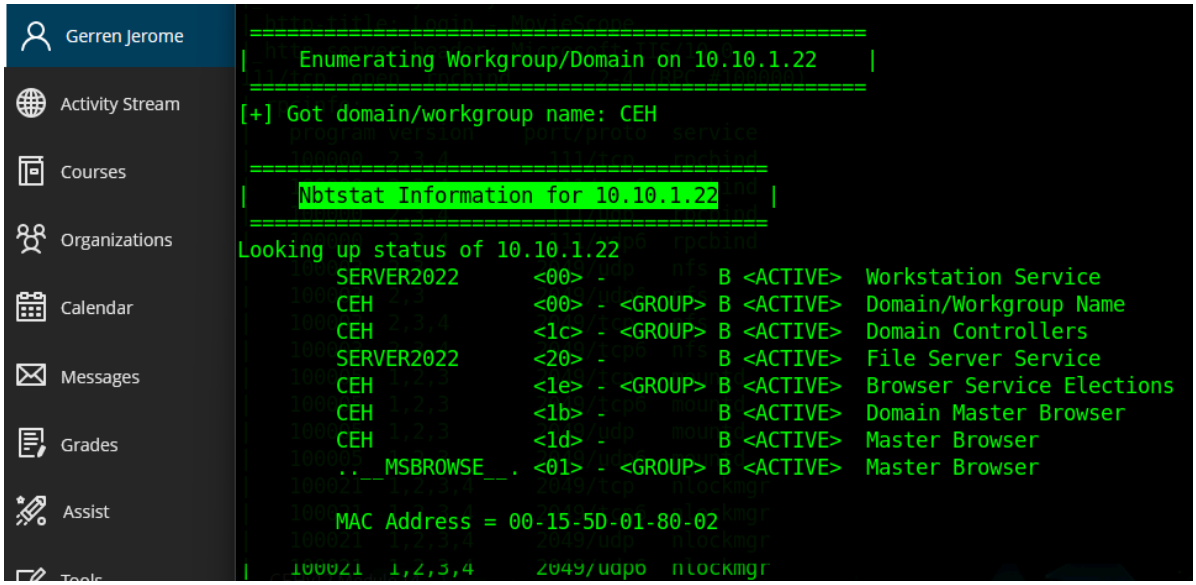
b) Enumerate network resources using Advanced IP Scanner (1 task)

i) **Screengrab: Step 6** – Advanced IP Scanner results



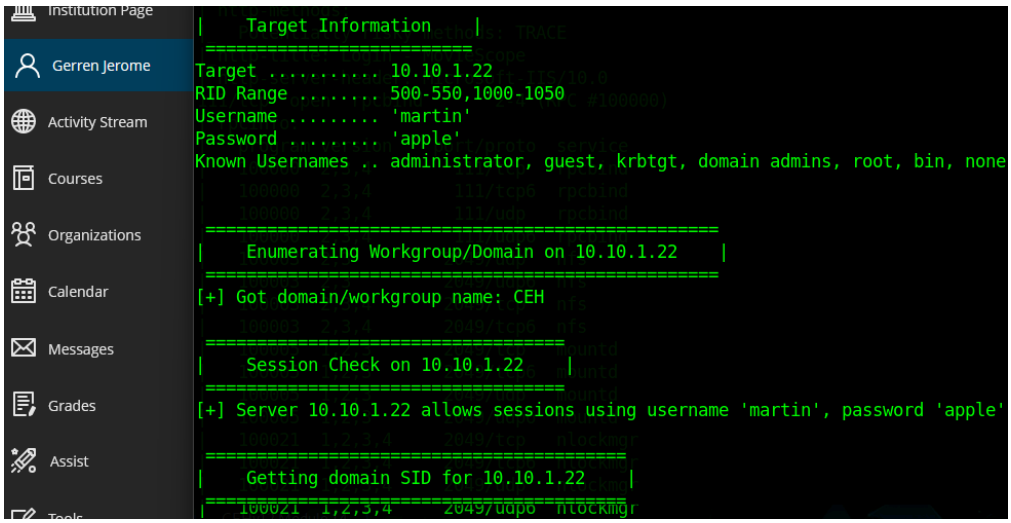
c) Enumerate information from Windows and Samba hosts using Enum4linux (X tasks)

i) **Screengrab: Step 9** – NetBIOS scan (10.10.1.22)

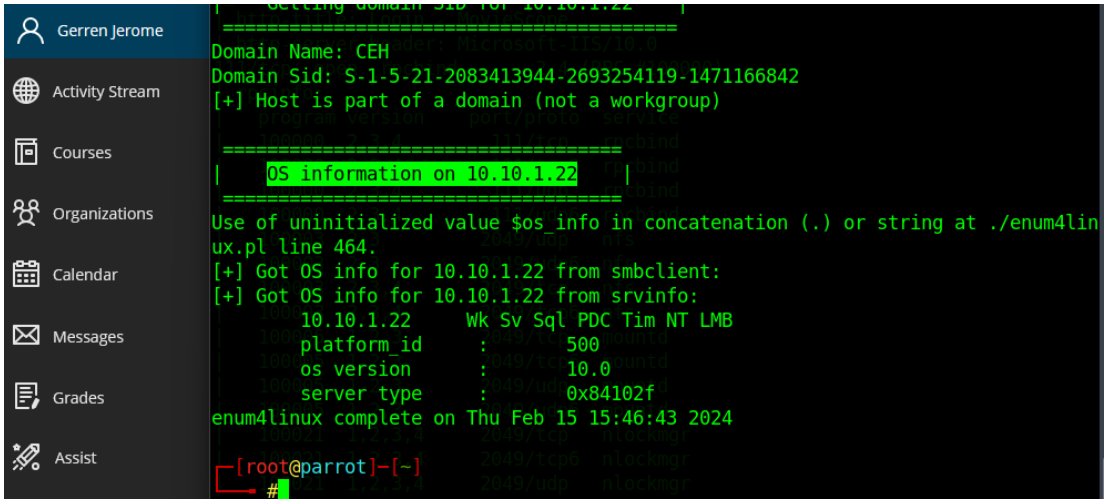


Gerren Jerome - Enumeration

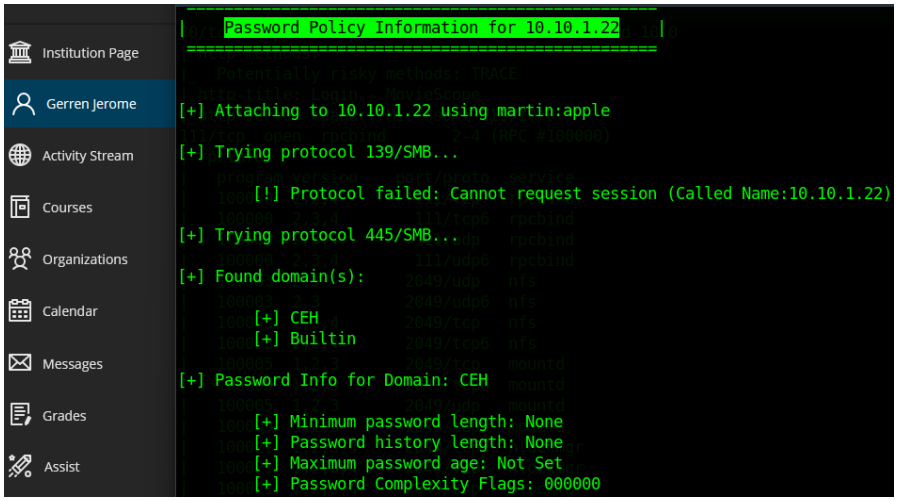
ii) **Screengrab: Step 11** – SID/RID info (10.10.1.22)



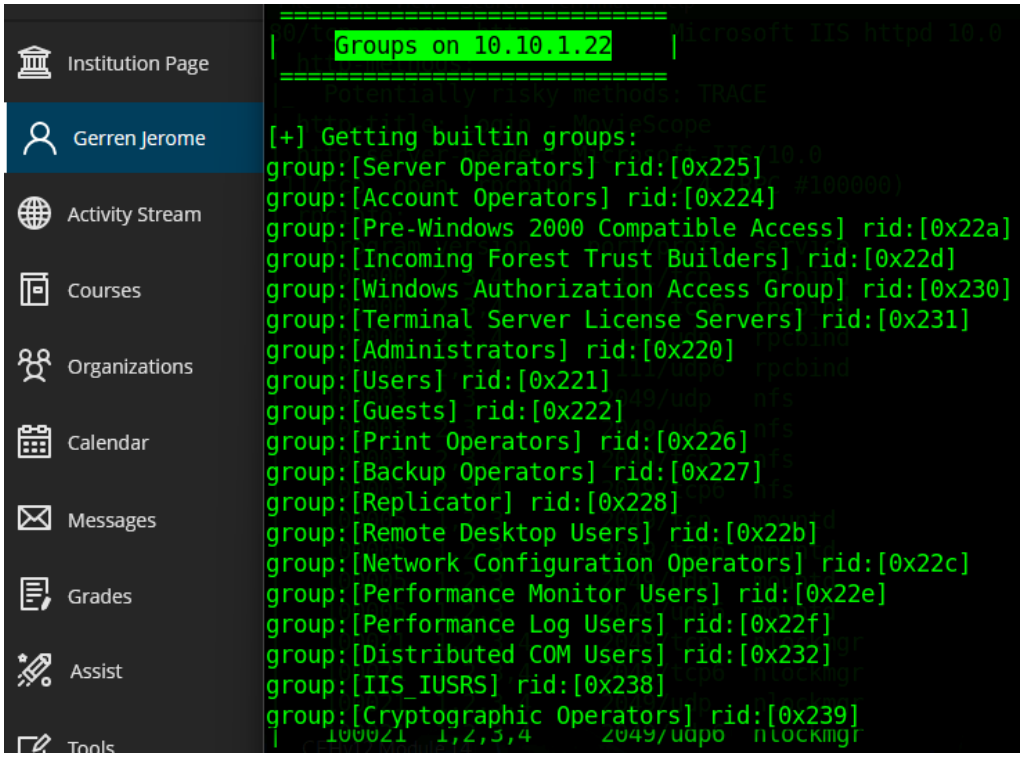
iii) **Screengrab: Step 13** – OS Details (10.10.1.22)



iv) **Screengrab: Step 15** – Password policy (10.10.1.22)



v) **Screengrab: Step 17** – Group Policy (10.10.1.22)



vi) **Screengrab: Step 19** – Shares (10.10.1.22)