Enumeration Methods: Comprehensive Network Analysis

Introduction

In my role as an ethical hacker with the EC-Council, I embarked on a detailed enumeration project to demonstrate my ability to extract vital information from a target network. Enumeration is a critical phase in penetration testing, providing insights that significantly enhance the ability to perceive and bypass security measures. This project showcases my proficiency in using various enumeration techniques and tools to gather comprehensive information about a target network.

Objectives

The primary objectives of this project included the extraction of various pieces of information about the target, such as:

- Machine names, ports, operating systems, and services.
- Network resources and shares.
- Usernames, user groups, policies, and passwords.
- Routing tables, audit settings, and service configurations.

Tasks and Techniques

This project involved performing a series of tasks using a variety of tools and techniques to achieve thorough enumeration. The tasks included:

1. **NetBIOS Enumeration:**
    - Using Windows command line and tools like nbtstat to gather NetBIOS information.
    - Employing NetBIOS Enumerator for detailed results.
    - Conducting NetBIOS scans with Nmap's NSE scripts.
2. **SNMP Enumeration:**
    - Using tools like snmp-check, SoftPerfect Network Scanner, and snmpwalk to extract SNMP information.
    - Performing SNMP scans with Nmap for additional insights.

3. **LDAP Enumeration:**
    - Utilizing Active Directory Explorer (AD Explorer) and Python with ldap3 to explore LDAP directories.
    - Performing LDAP brute force and directory object retrieval with Nmap.
4. **NFS Enumeration:**
    - Conducting NFS scans using RPCScan and SuperEnum tools.
5. **DNS Enumeration:**
    - Performing DNS zone transfers, DNSSEC zone walking, and service discovery with tools like dig, dnsrecon, and Nmap.
6. **SMTP Enumeration:**
    - Listing mail users and open SMTP relays with Nmap.
7. **RPC, SMB, and FTP Enumeration:**
    - Using tools like NetScanTools Pro and Nmap to enumerate RPC, SMB, and FTP services.

General Enumeration Tools:

- Employing tools like Global Network Inventory, Advanced IP Scanner, and Enum4linux to gather information from network resources, Windows, and Samba hosts.

Tools Utilized

Throughout this project, I utilized several key tools to perform enumeration tasks, including:

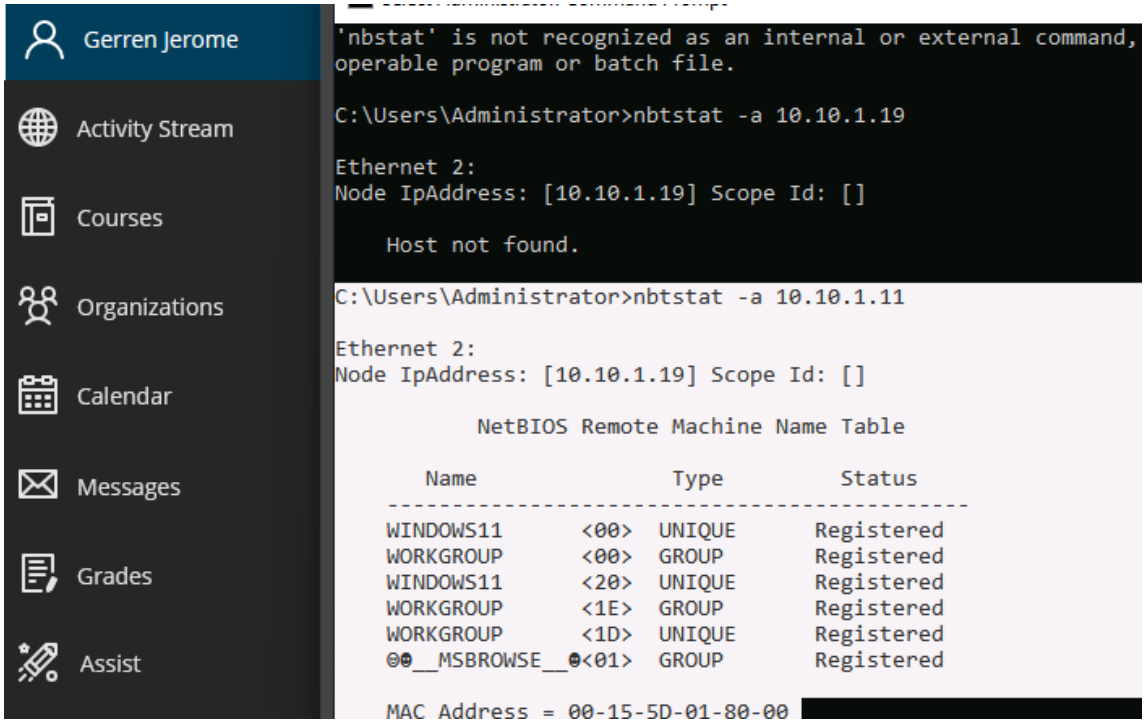
- **Nmap:** For scanning and service discovery.
- **NetBIOS Enumerator:** For detailed NetBIOS information.
- **snmp-check and snmpwalk:** For SNMP enumeration.
- **Active Directory Explorer and Python (ldap3):** For LDAP exploration.
- **RPCScan and SuperEnum:** For NFS enumeration.
- **dig, dnsrecon:** For DNS enumeration.
- **Global Network Inventory and Advanced IP Scanner:** For comprehensive network resource enumeration.
- **Enum4linux:** For extracting information from Windows and Samba hosts.

Gerren Jerome - Enumeration

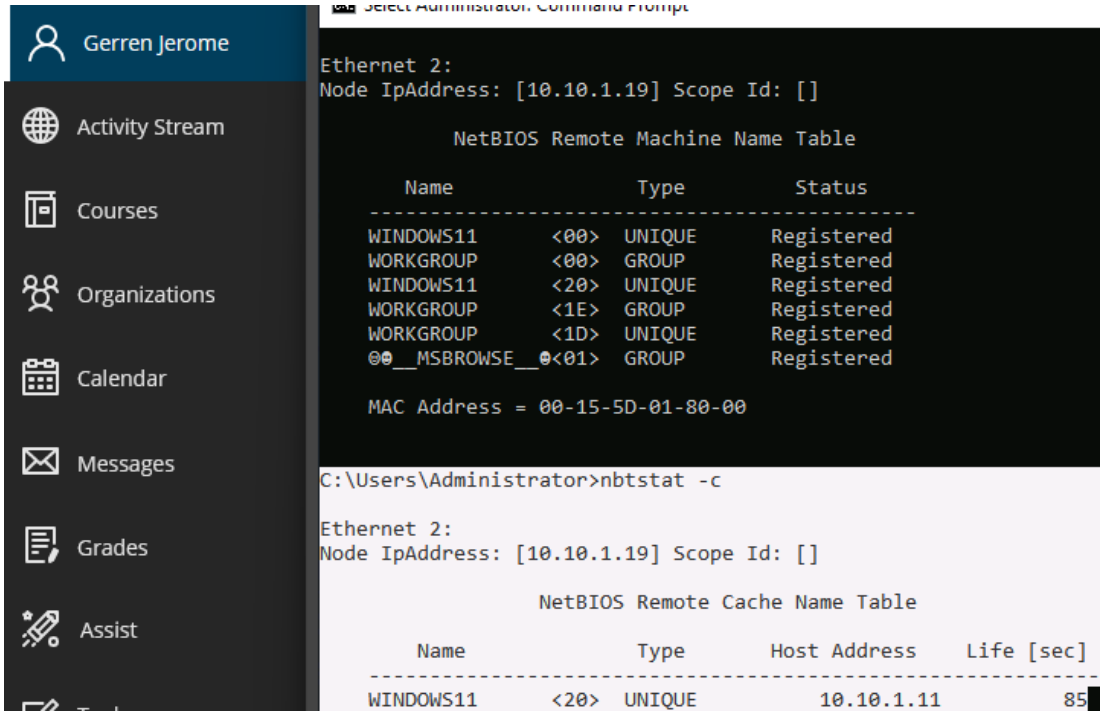
Perform enumeration (NetBIOS)

NetBIOS enumeration via Windows command line

nbtstat result

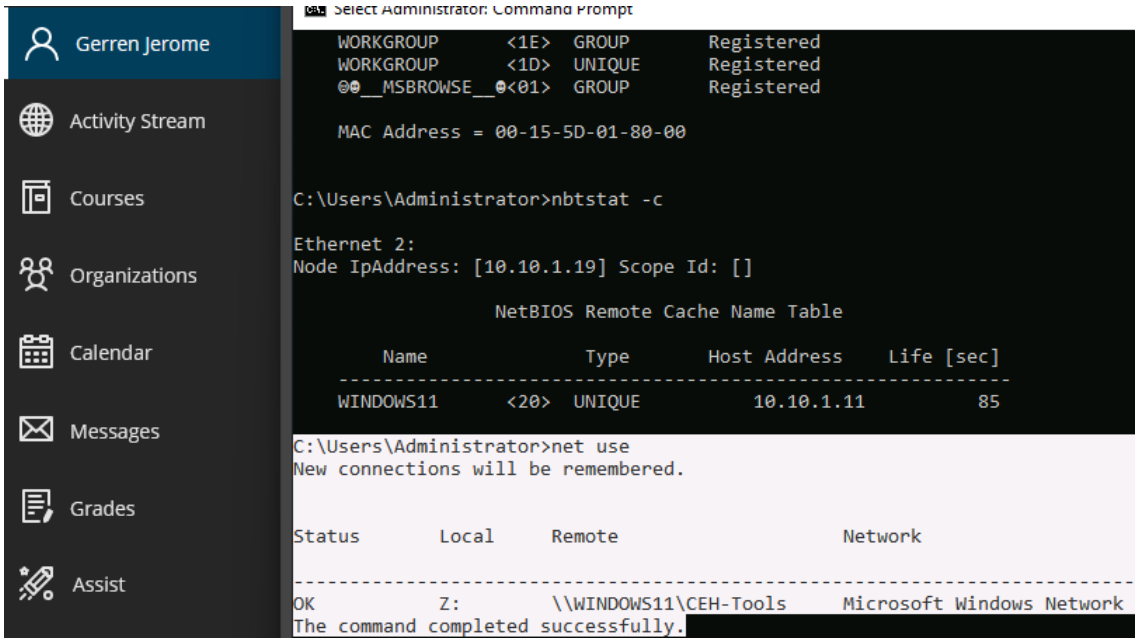


nbtstat result



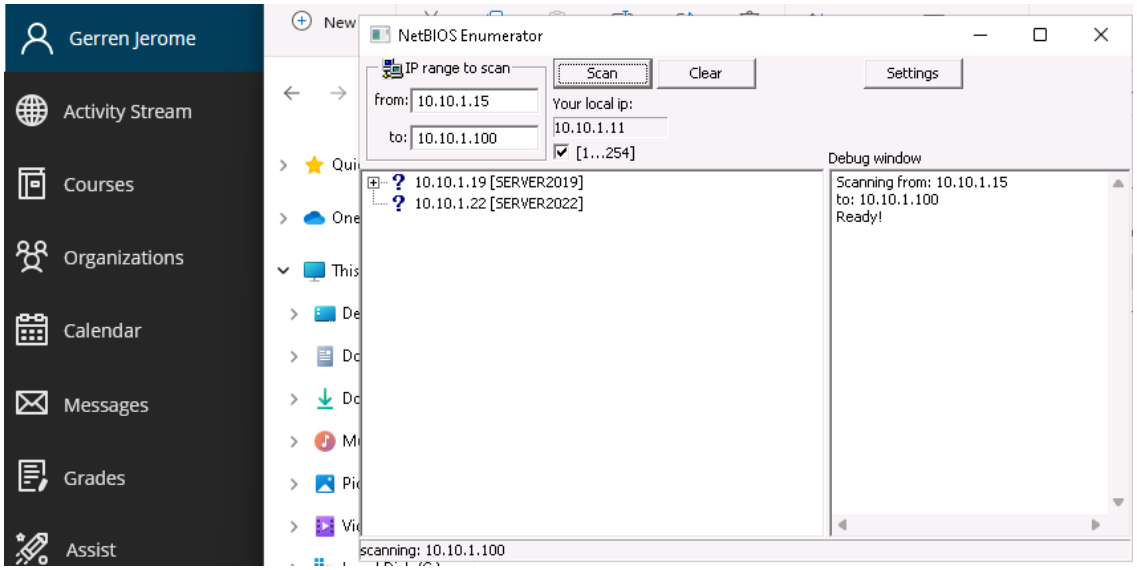
Gerren Jerome - Enumeration

net use result



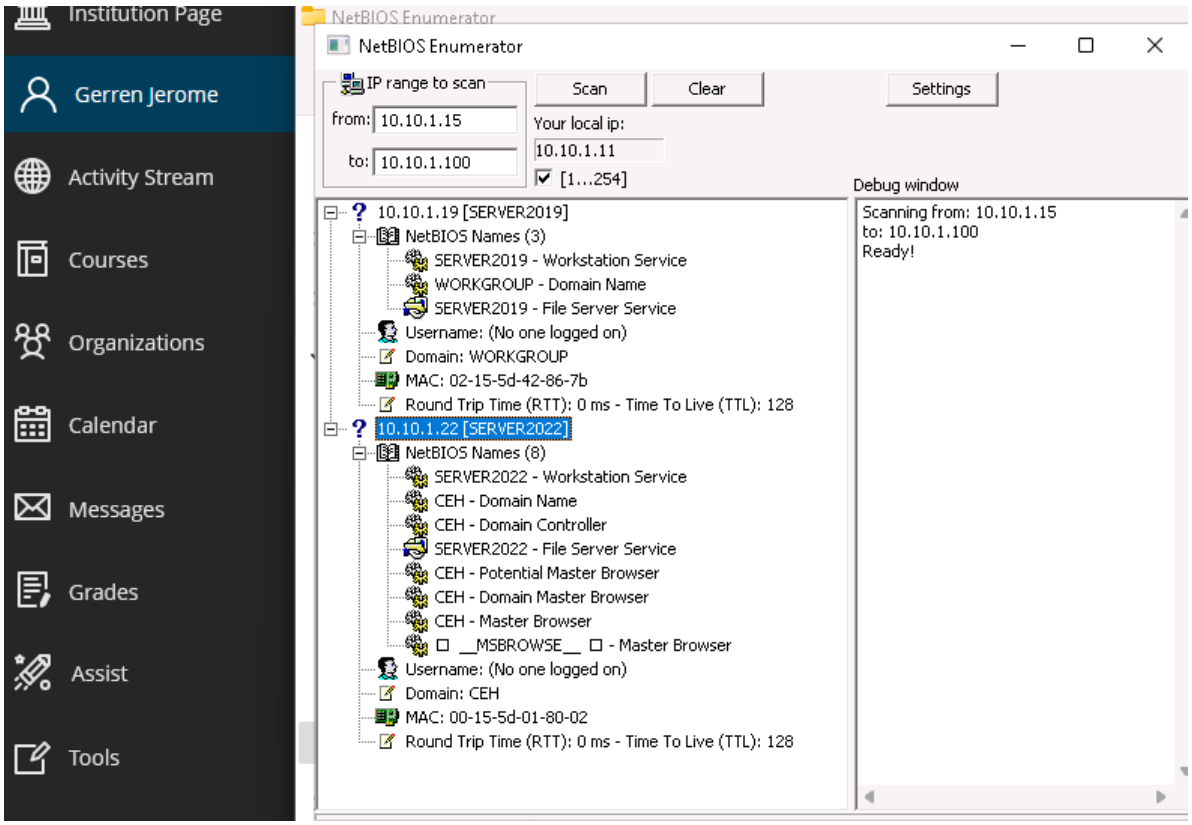
NetBIOS enumeration via NetBIOS enumerator

NBE result (Debug)



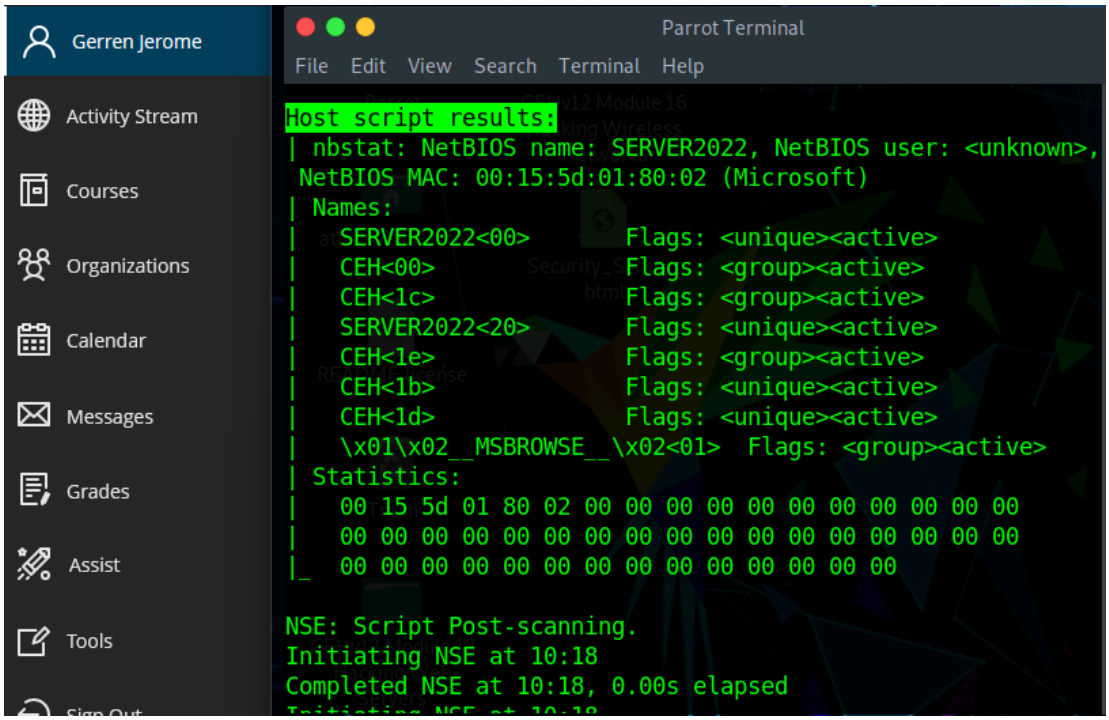
Gerren Jerome - Enumeration

Expanded result



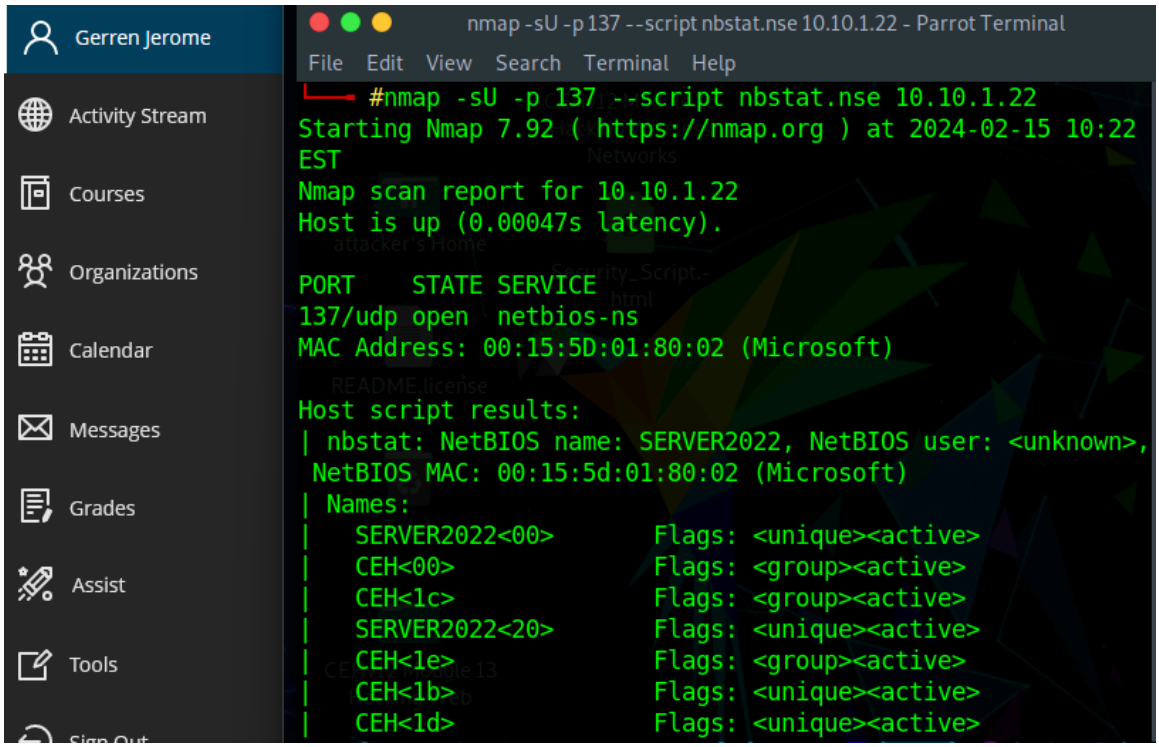
NetBIOS enumeration via NSE Script

Nmap scan (-sV)



Gerren Jerome - Enumeration

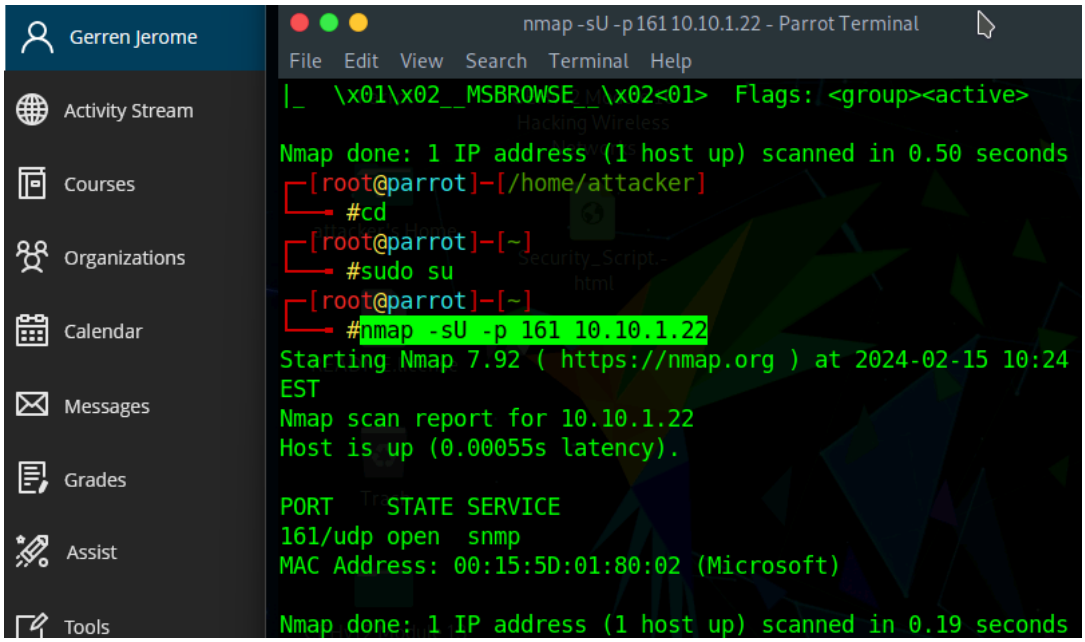
Nmap scan (-sU)



Perform enumeration (SNMP)

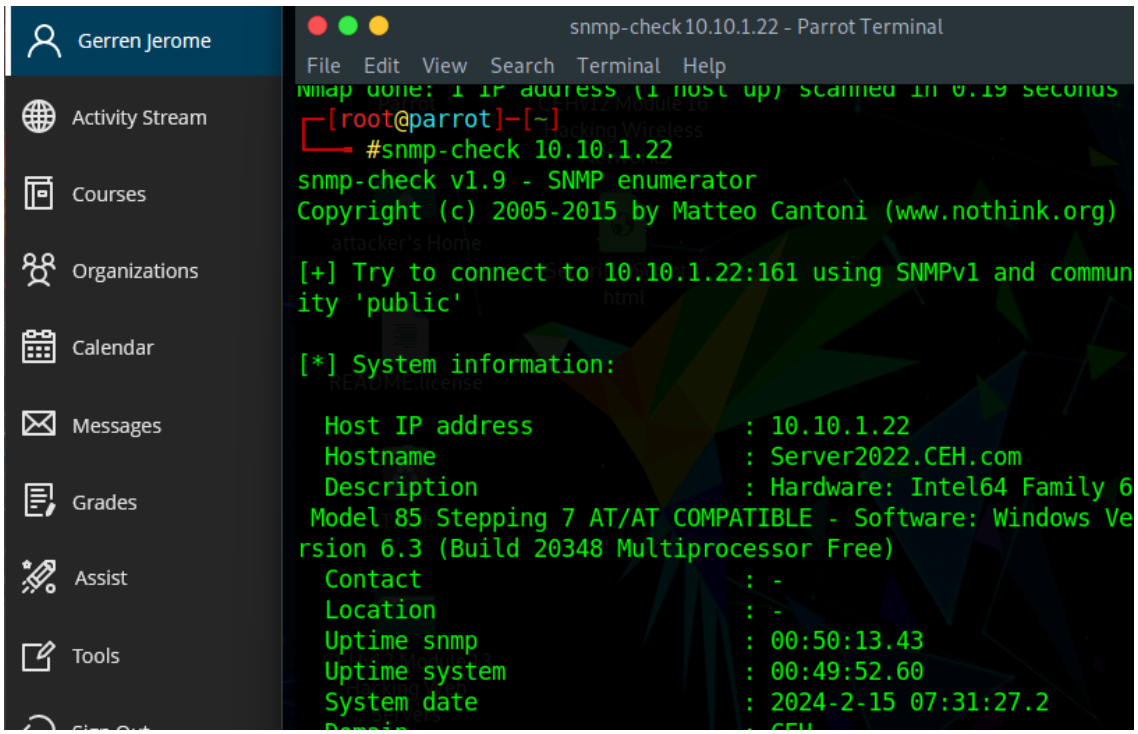
SNMP enumeration via snmp-check

Nmap scan (-sU)

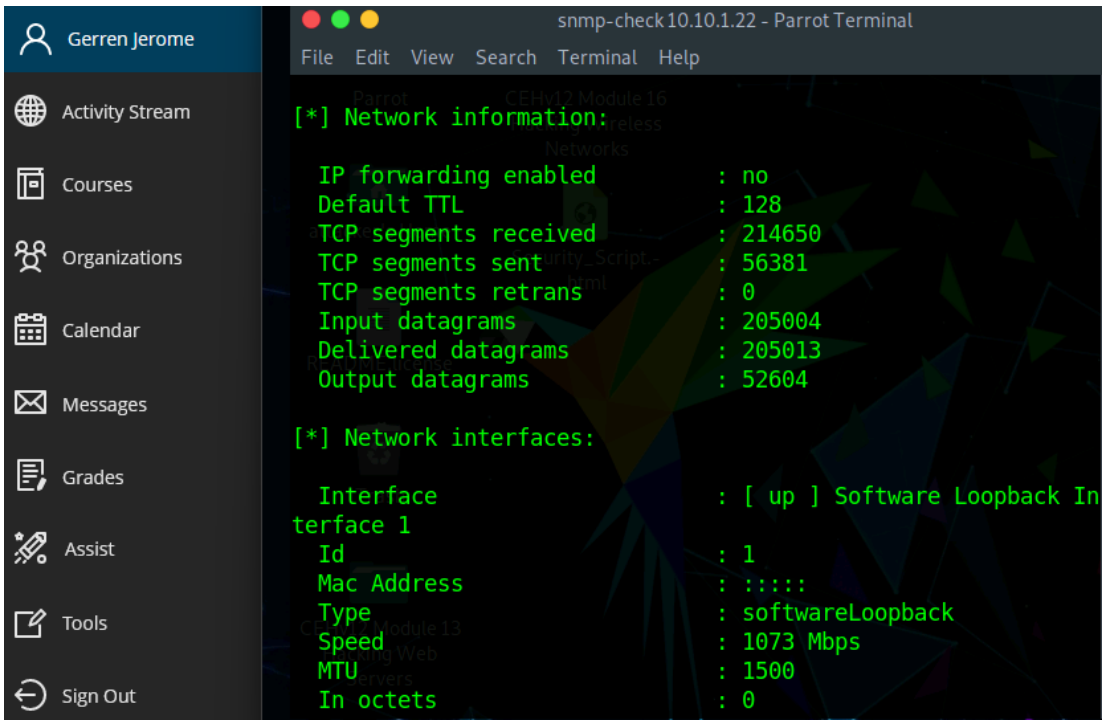


Gerren Jerome - Enumeration

snmp-check results (1 of 3)

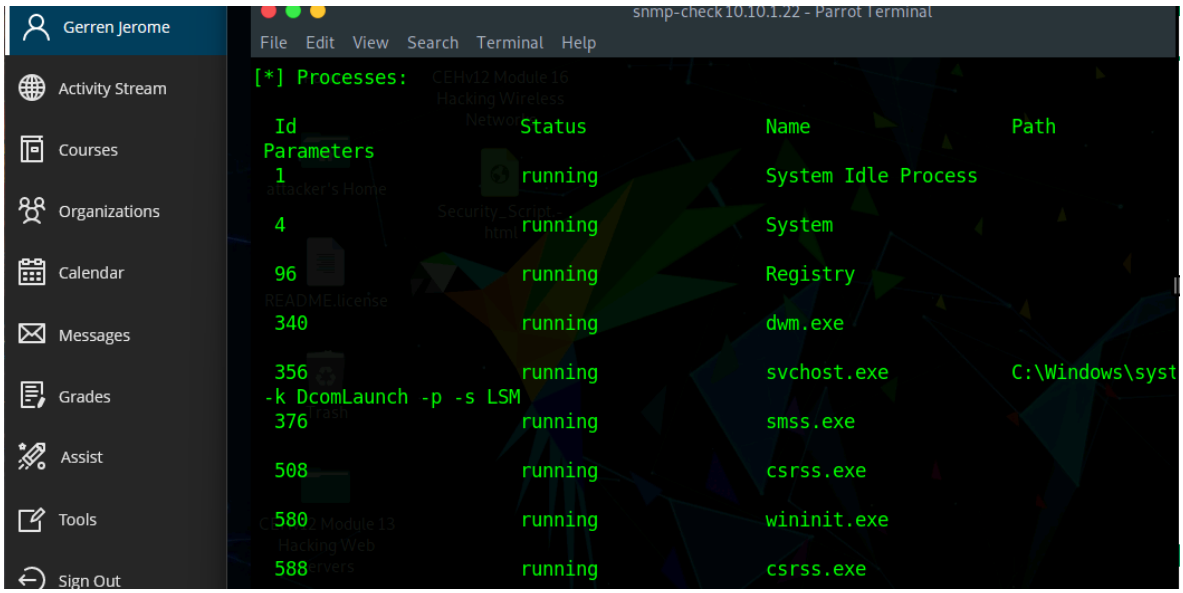


snmp-check results (2 of 3)



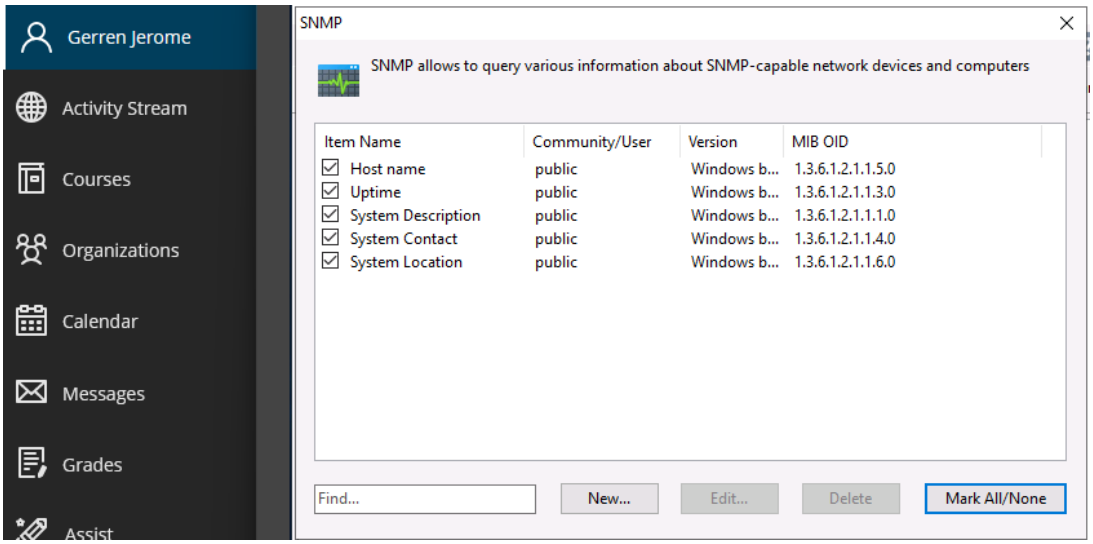
Gerren Jerome - Enumeration

snmp-check results (3 of 3)



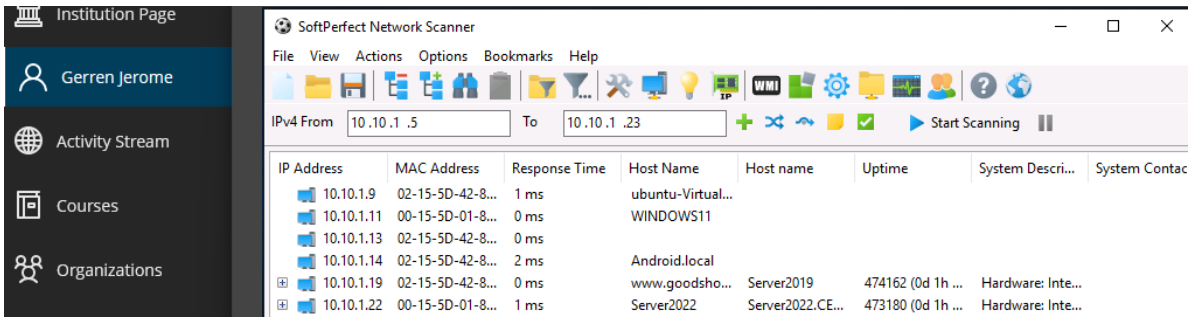
SNMP enumeration via SoftPerfect Network Scanner

prescan config

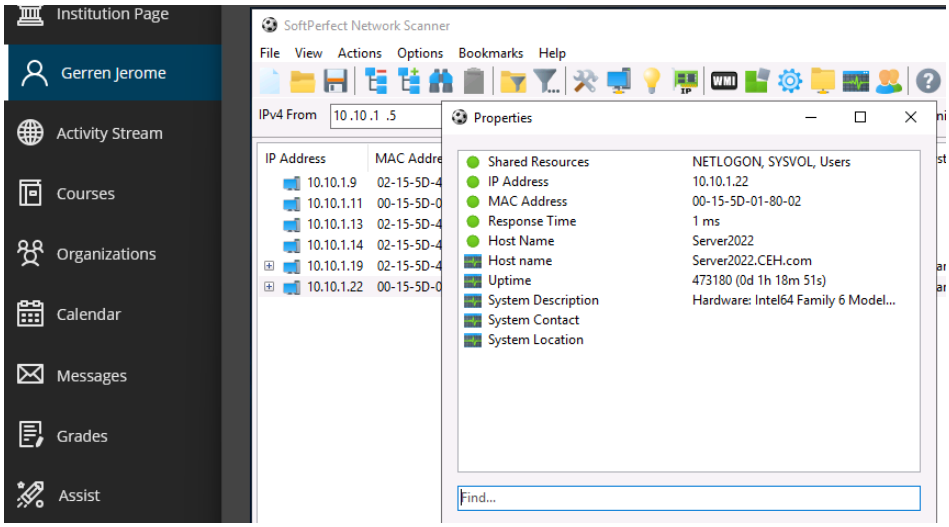


Gerren Jerome - Enumeration

SPNS scan results

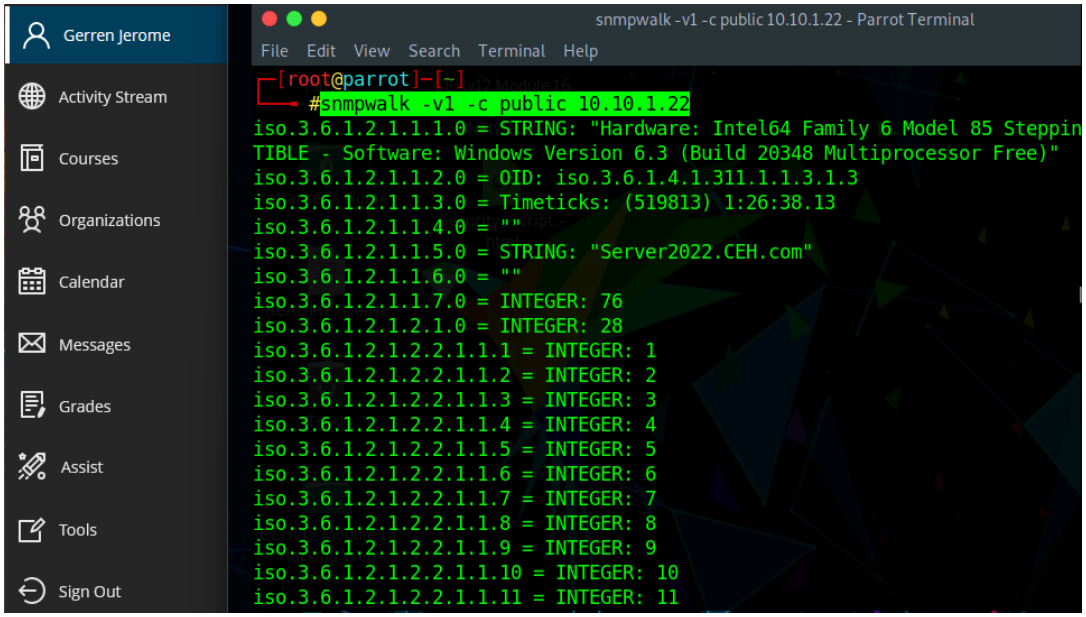


properties of target machine (10.10.1.22)



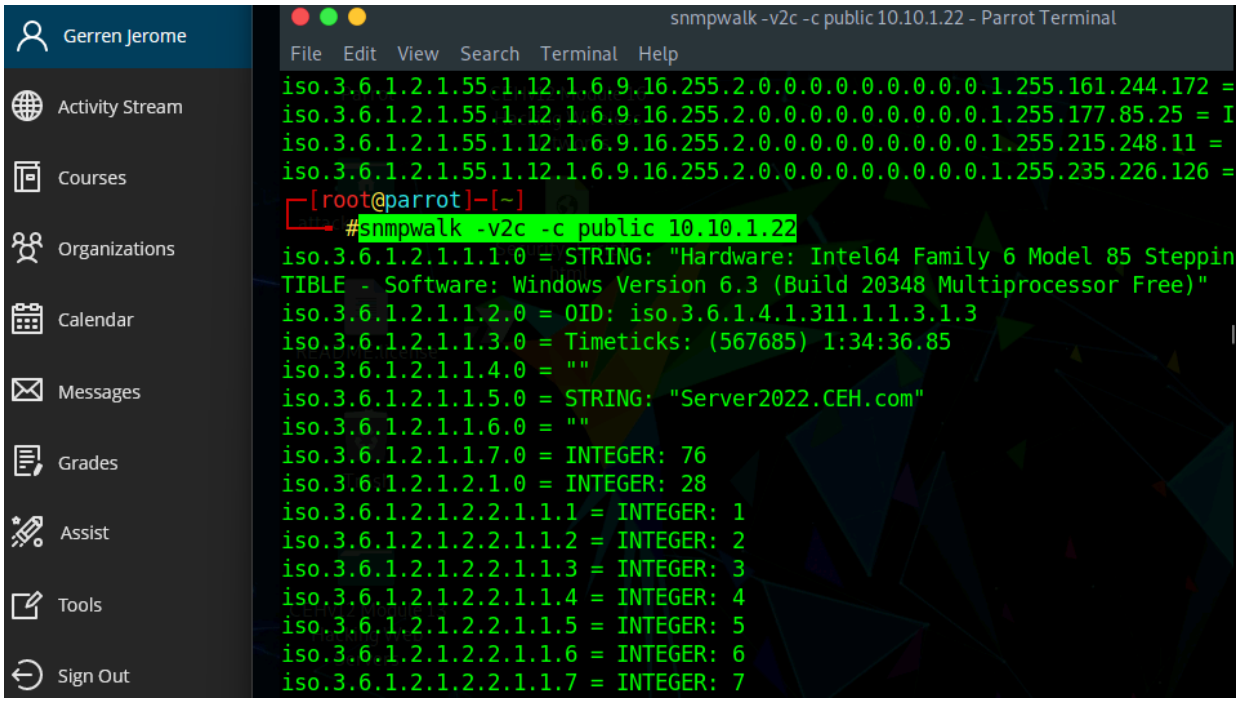
SNMP enumeration via SnmpWalk

scan result (snmpwalk -v1)



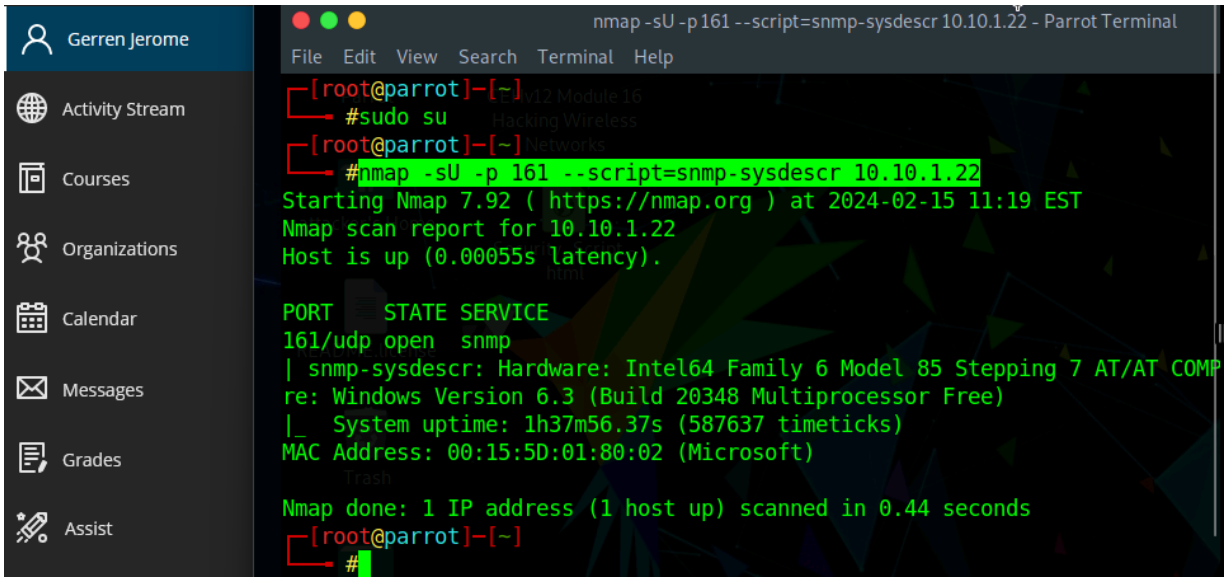
Gerren Jerome - Enumeration

scan result (snmpwalk -v2c)



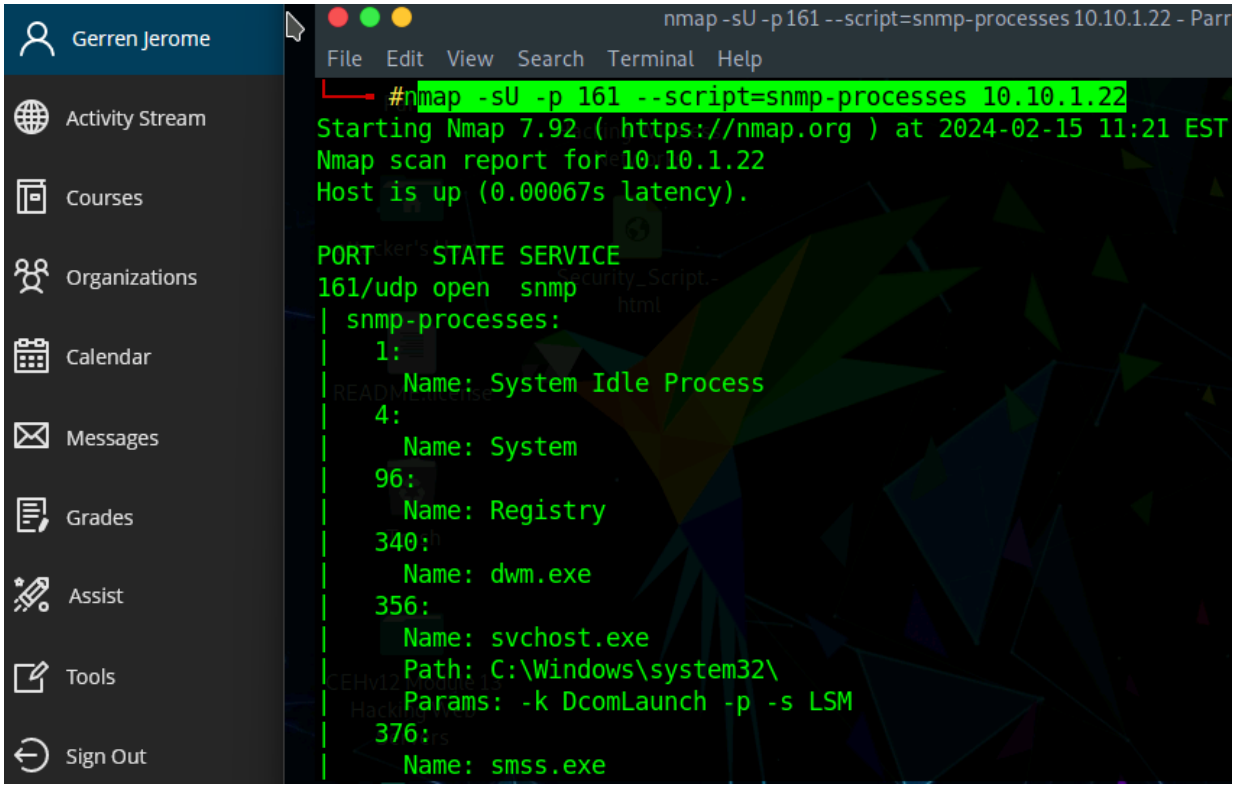
SNMP enumeration via Nmap (4 tasks)

scan result (type and description)

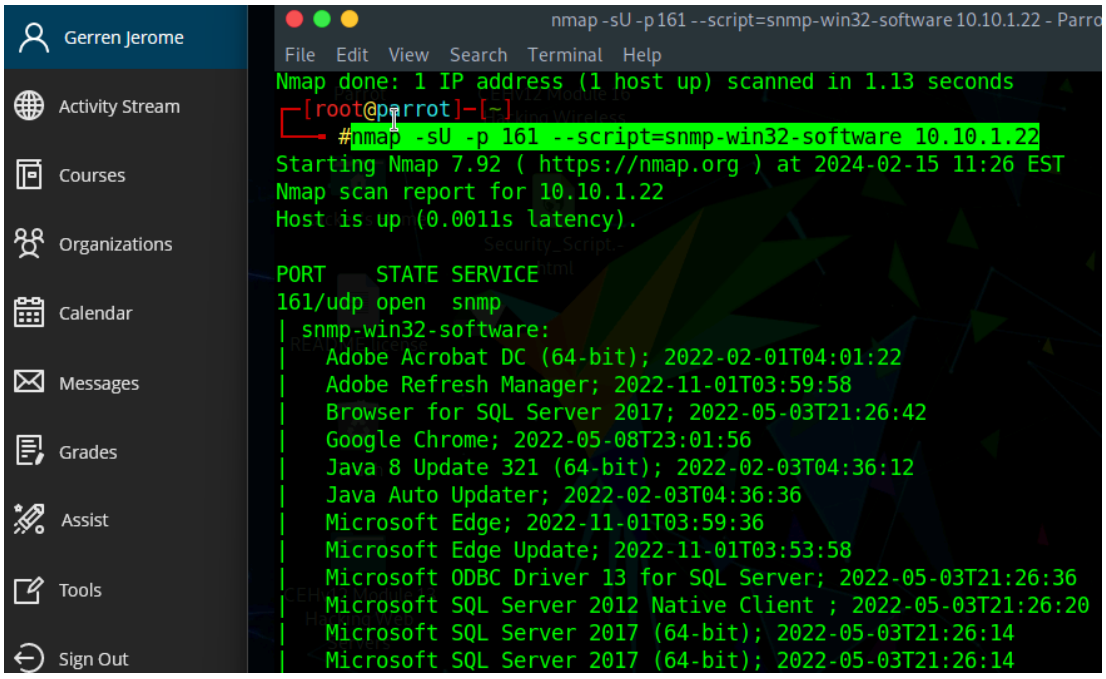


Gerren Jerome - Enumeration

scan result (ports and processes)

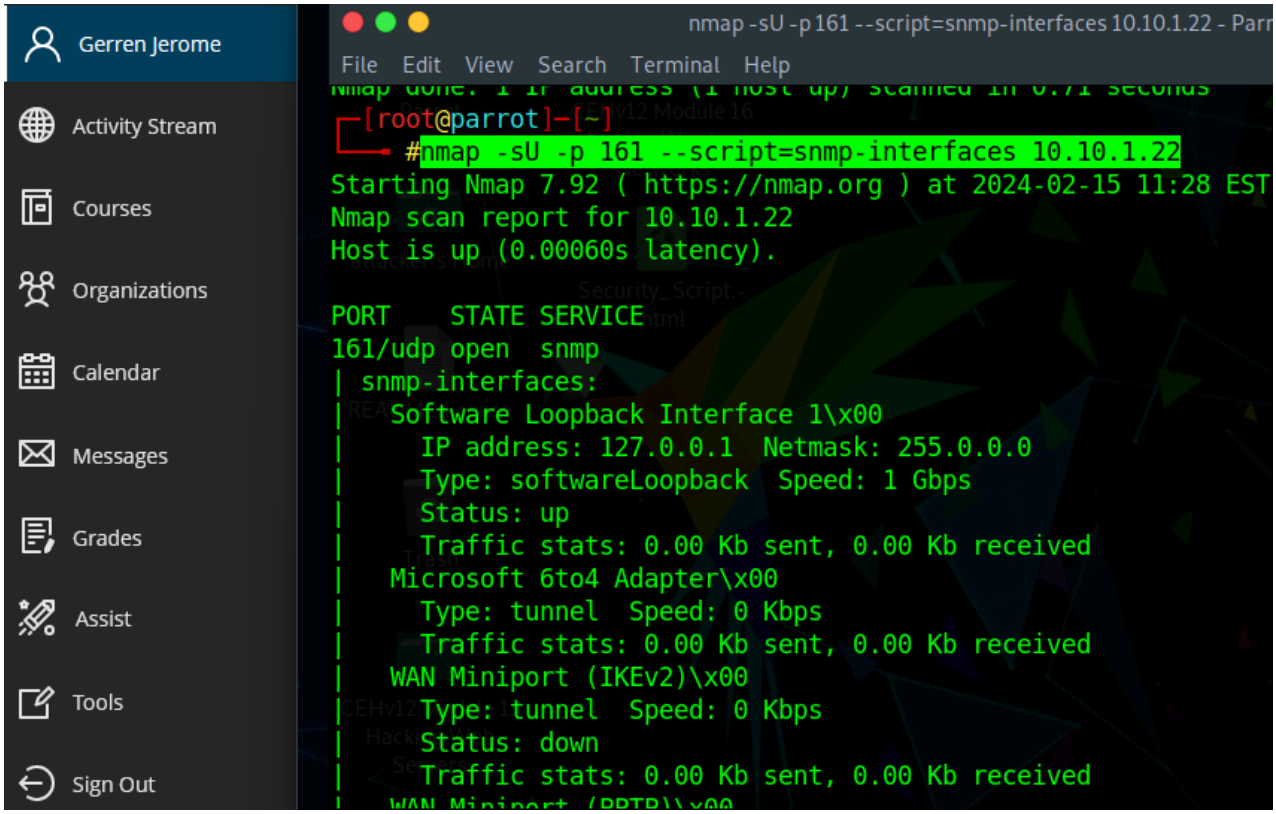


scan result (applications)



Gerren Jerome - Enumeration

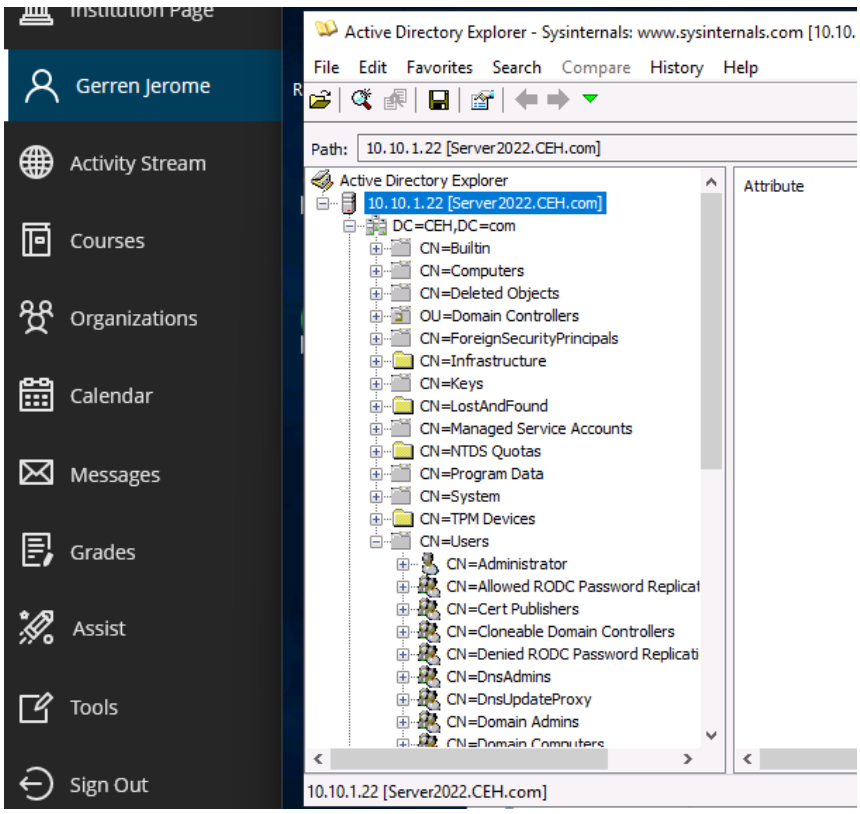
scan result (interfaces)



Perform enumeration (LDAP)

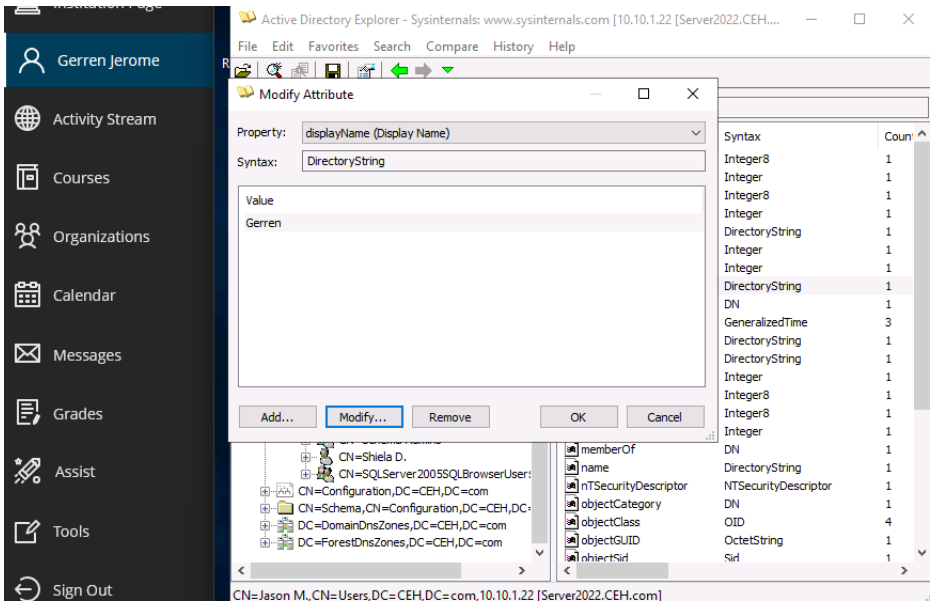
Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Navigating ADExplorer



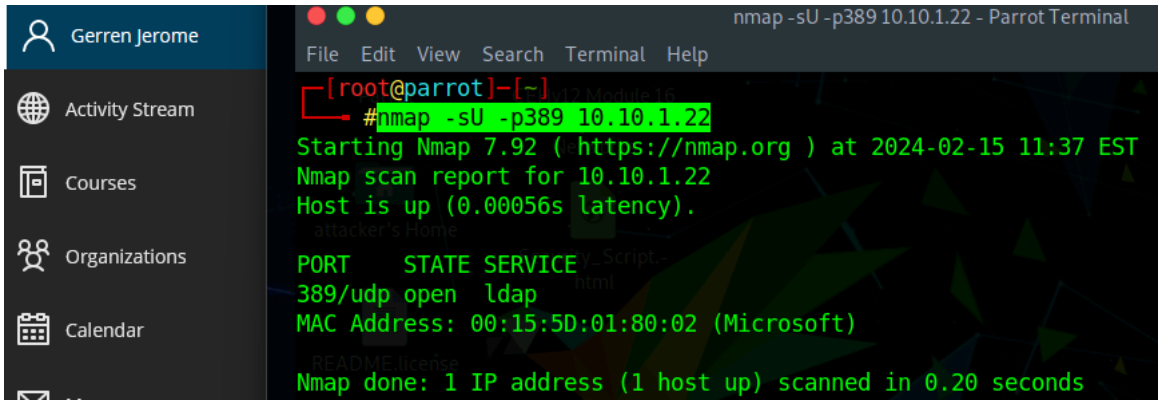
Gerren Jerome - Enumeration

user attribute modification



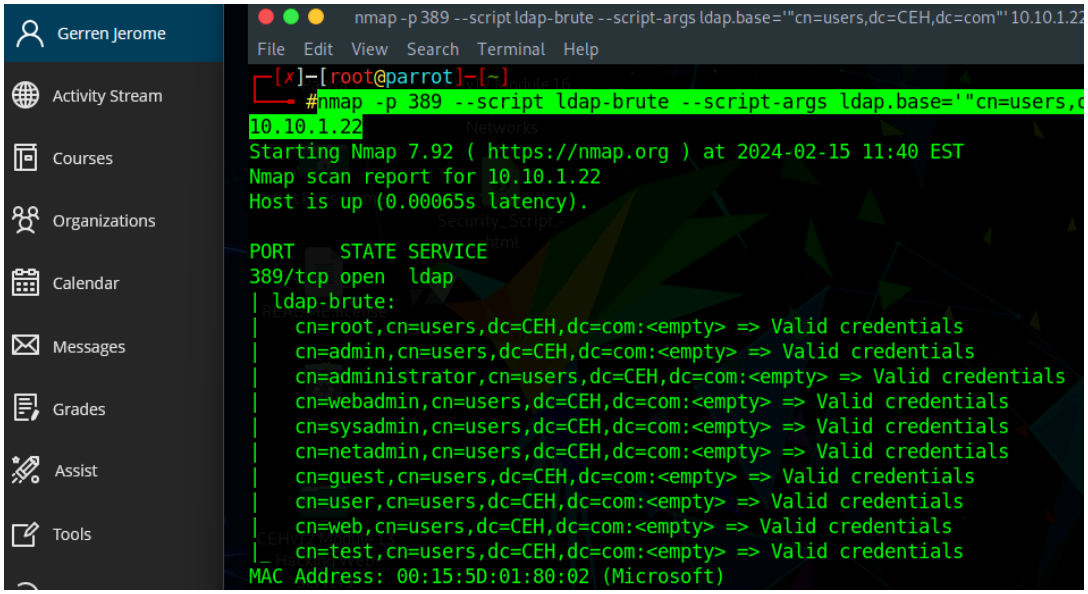
Perform LDAP enumeration using Python and Nmap

scan result (Nmap -sU)

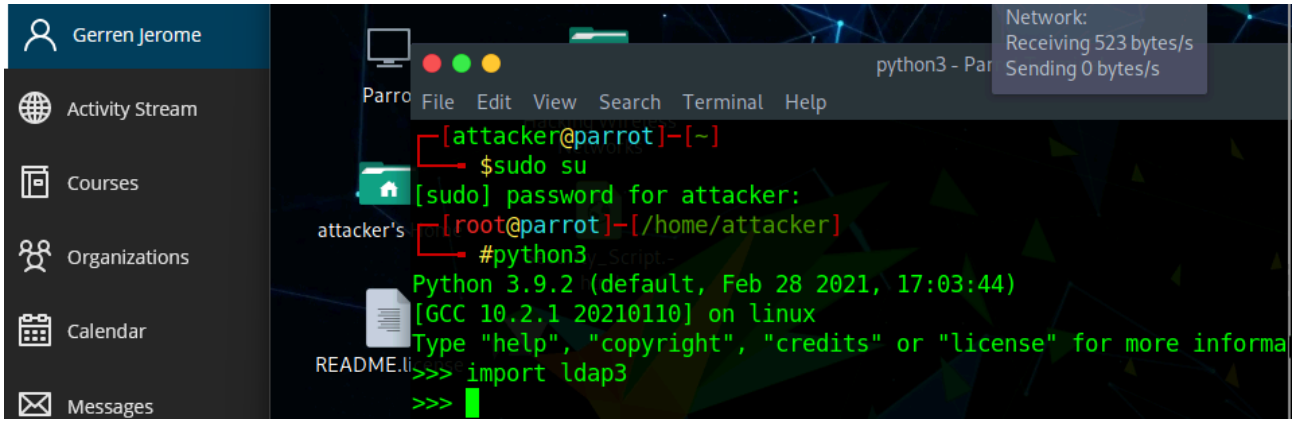


Gerren Jerome - Enumeration

result (Nmap LDAP bruteforce)

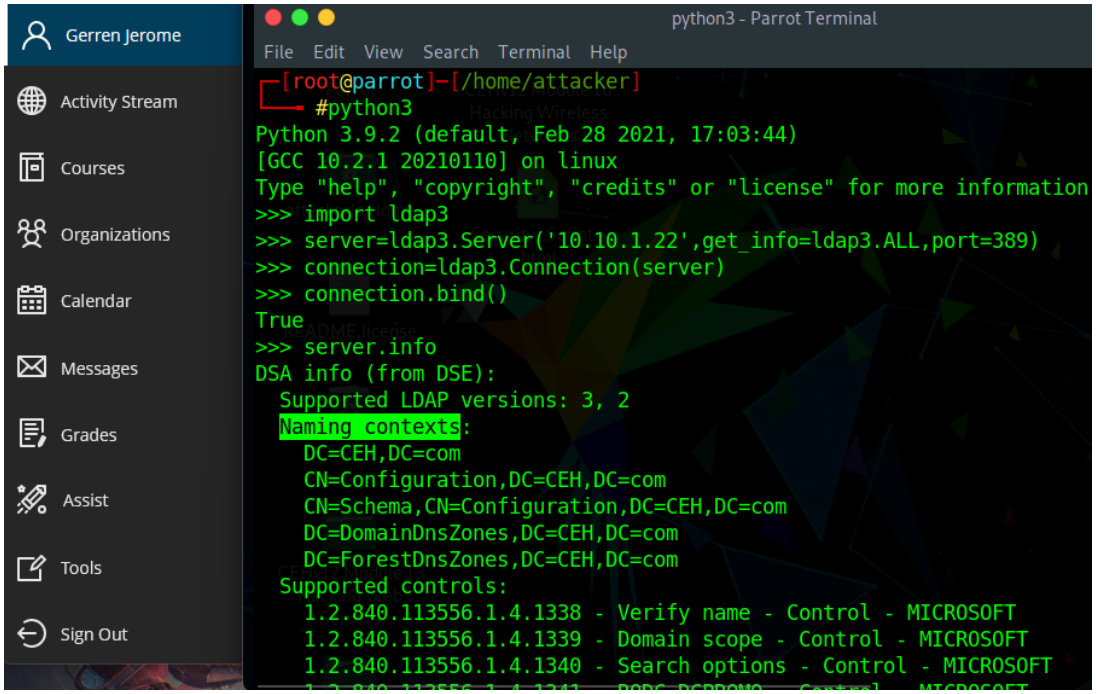


import ldap3 into Python

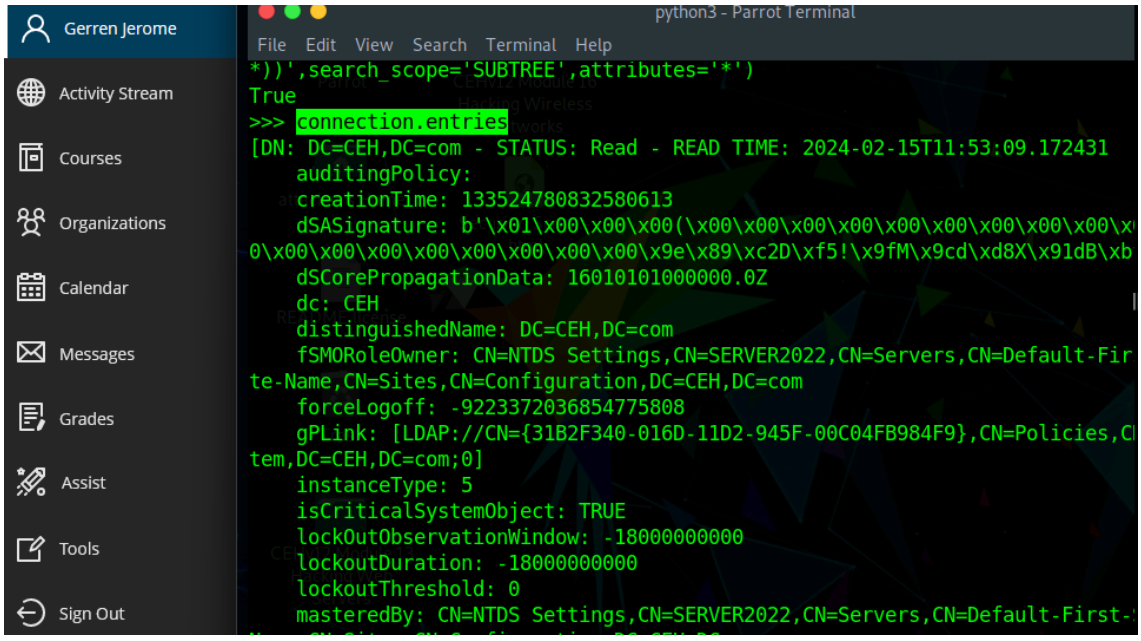


Gerren Jerome - Enumeration

gain naming context

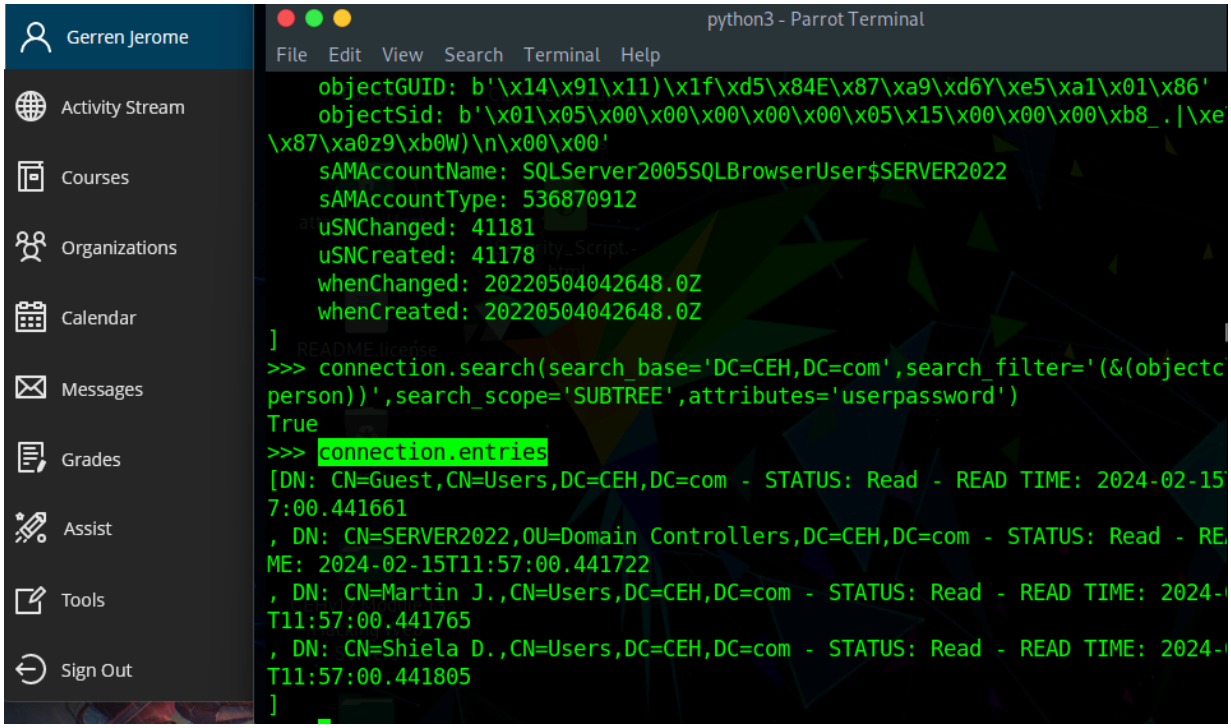


retrieve directory objects



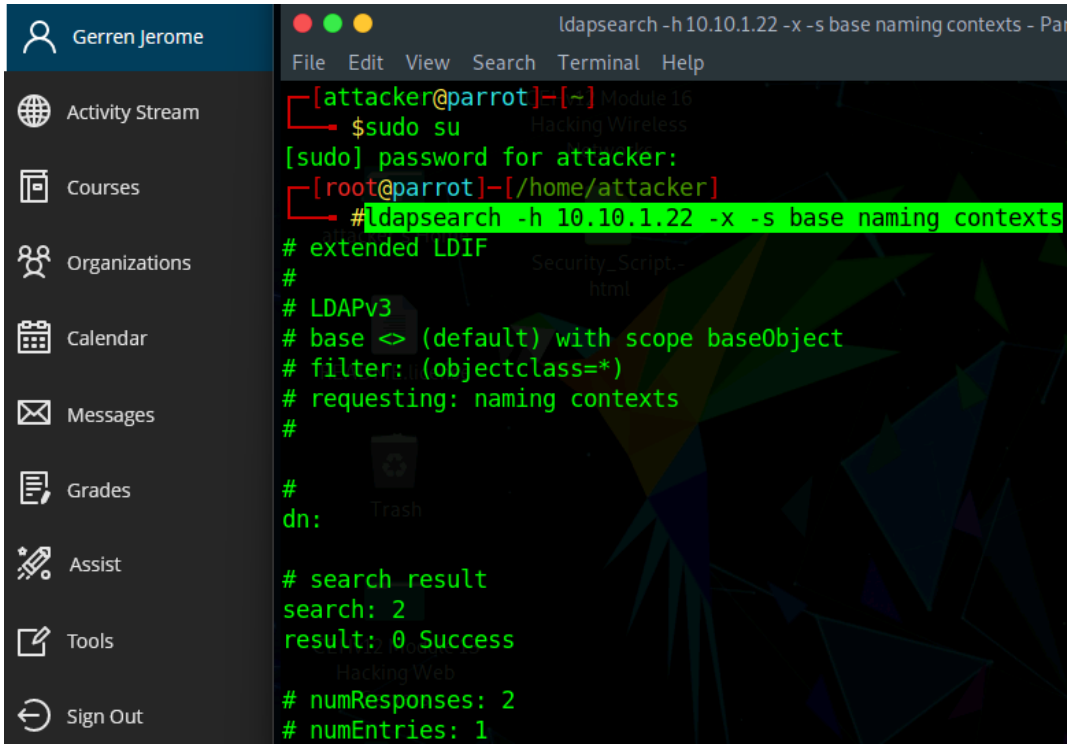
Gerren Jerome - Enumeration

result (LDAP dump)



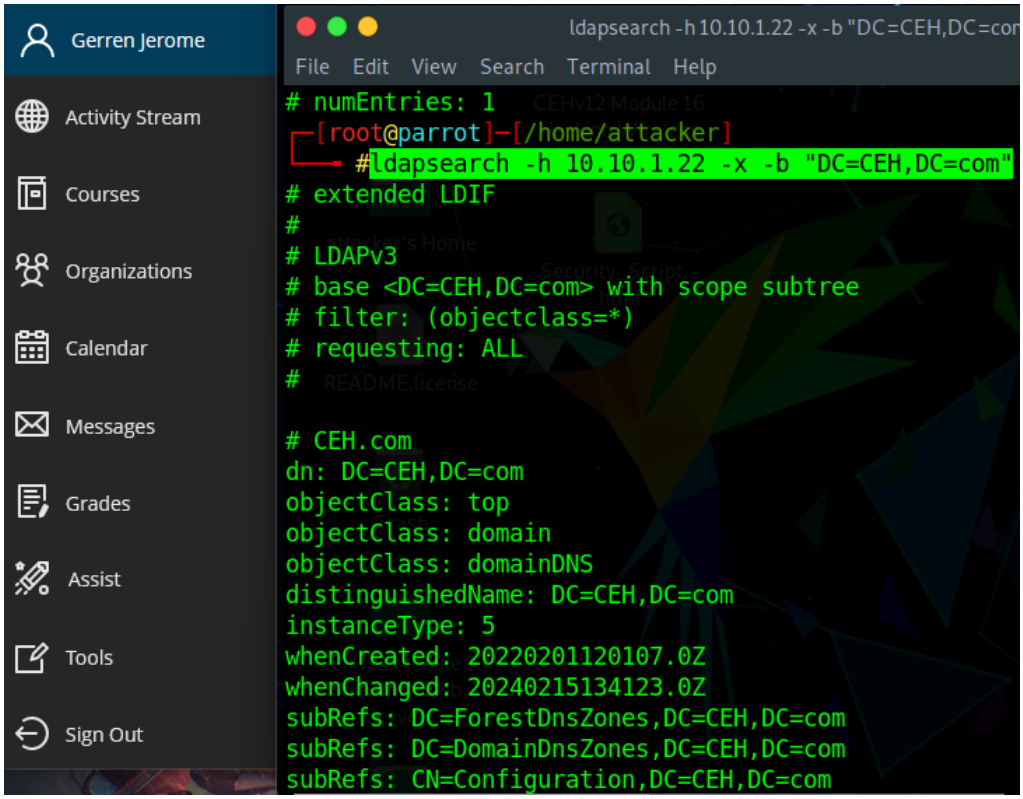
Perform LDAP enumeration using ldapsearch

gain naming context via ldapsearch

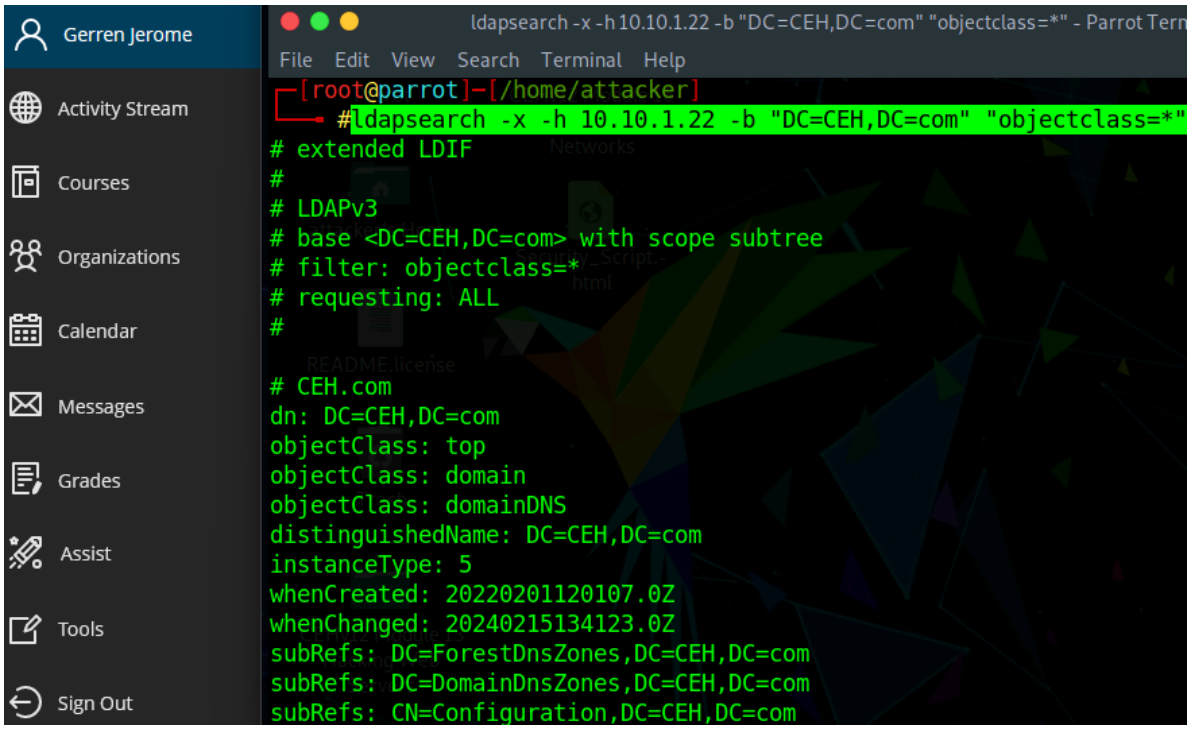


Gerren Jerome - Enumeration

more information about primary domain



retrieve info about objects in directory tree

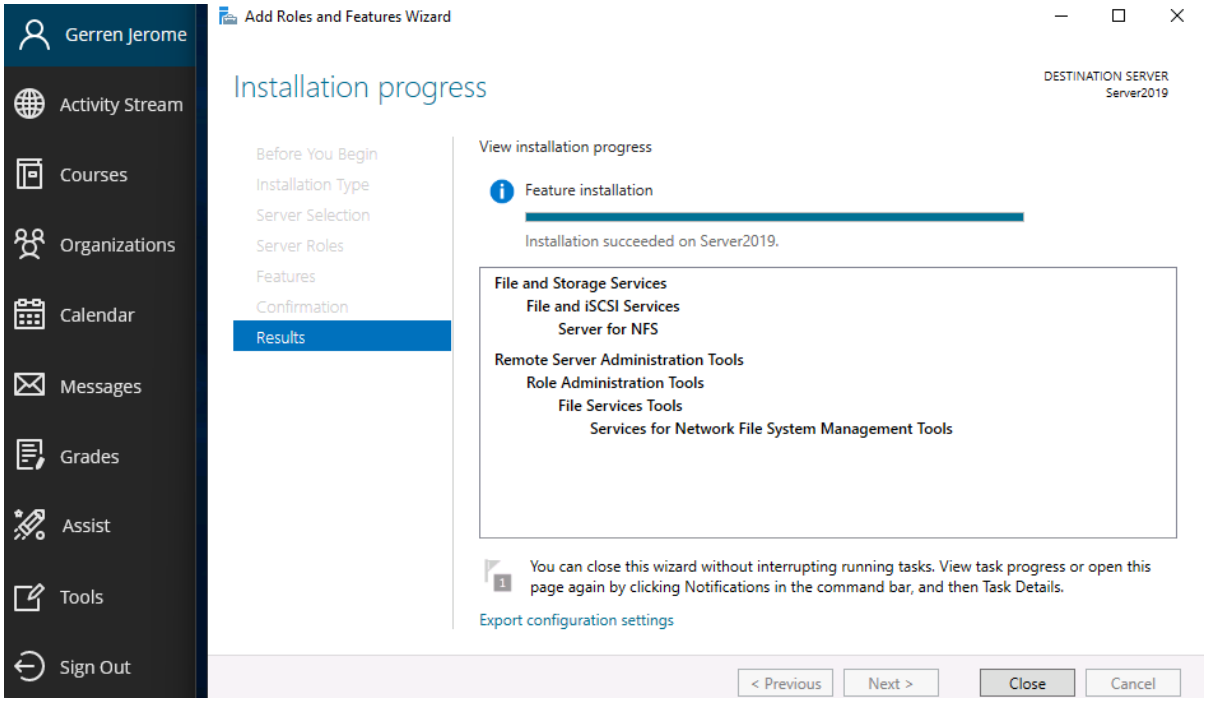


Gerren Jerome - Enumeration

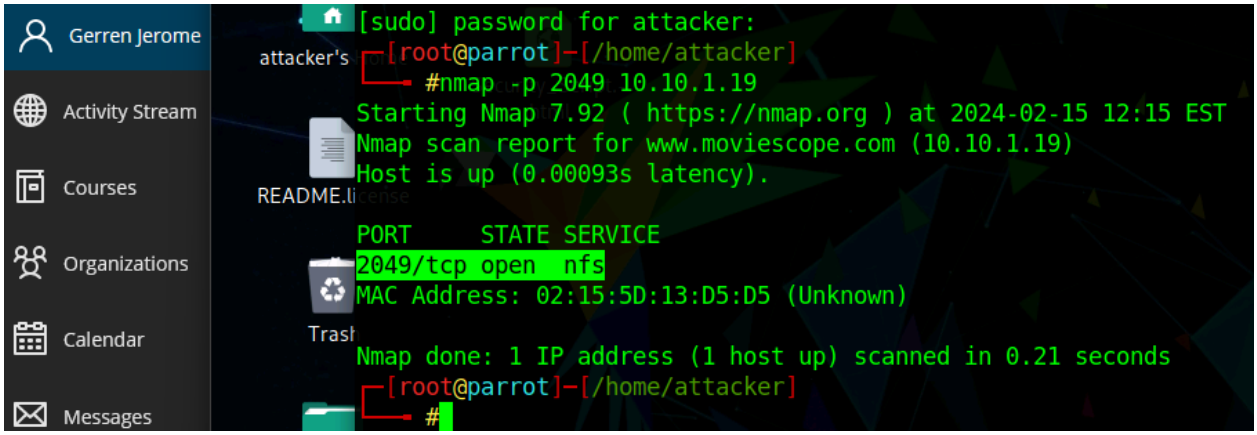
Perform enumeration (NFS)

Perform NFS enumeration using RPCScan and SuperEnum

confirm install/enable of NFS service in Windows

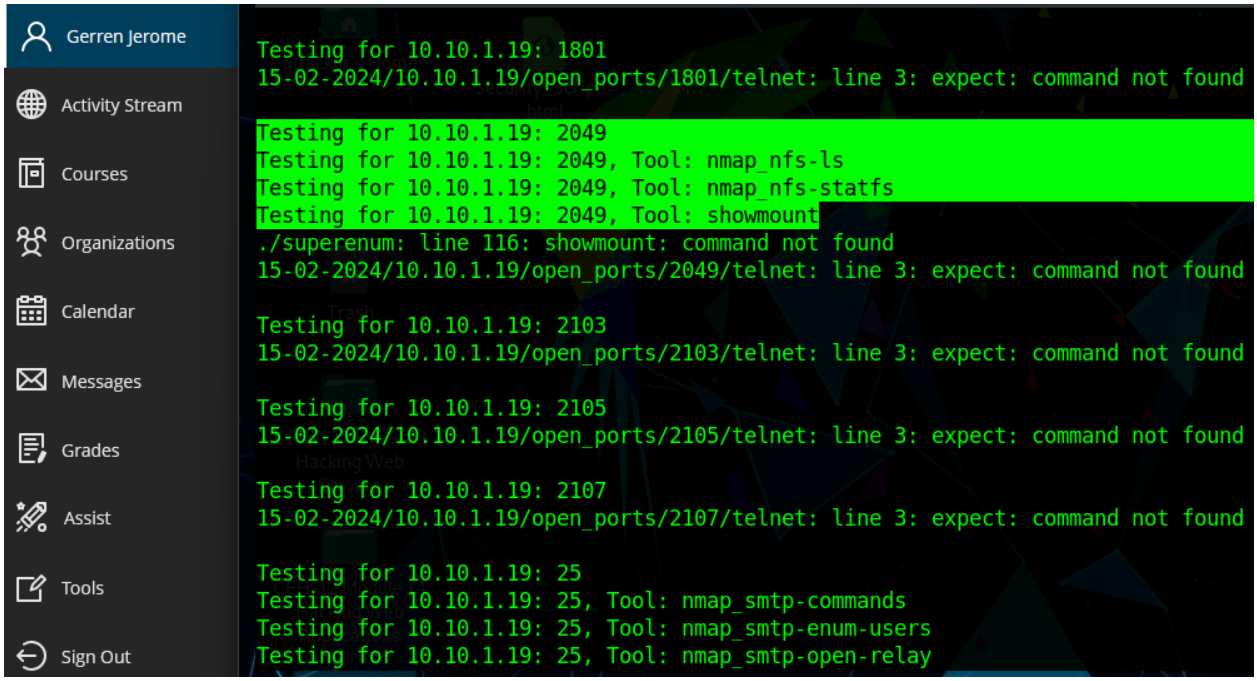


scan result (NFS running?)

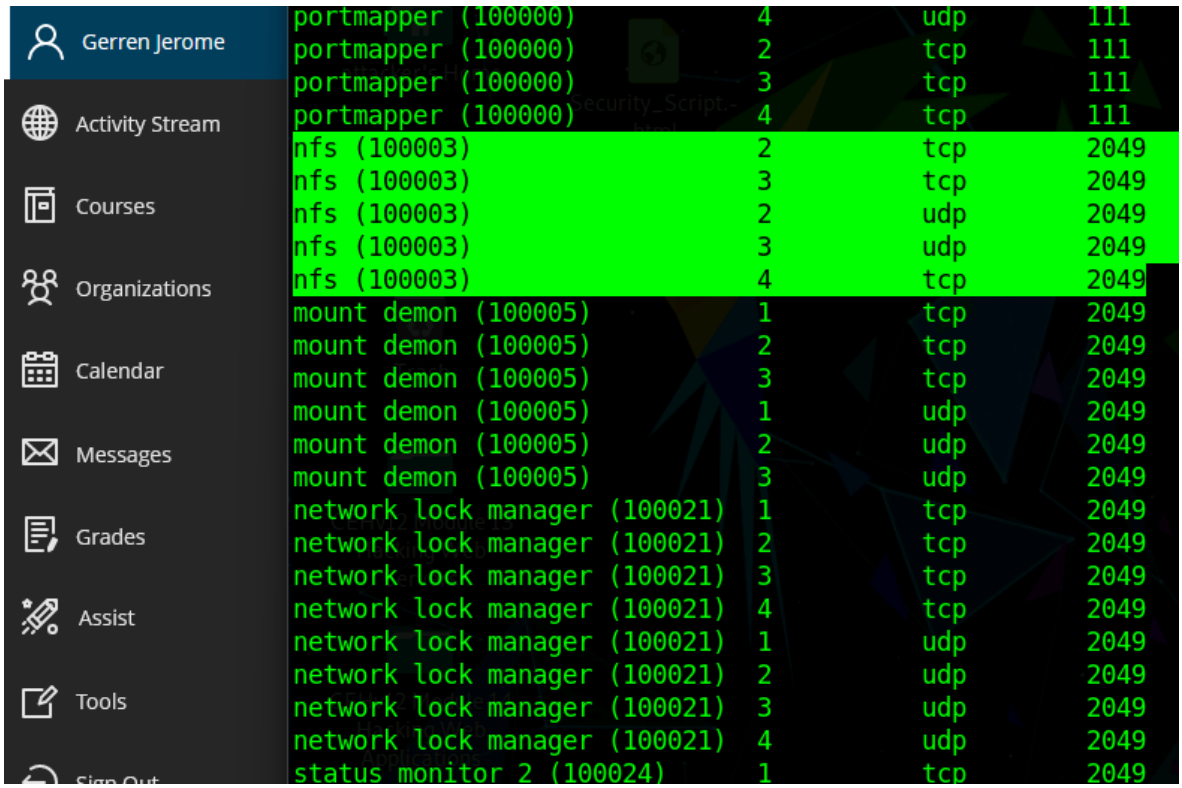


Gerren Jerome - Enumeration

scan result (SuperEnum)



scan result (RPCScan)

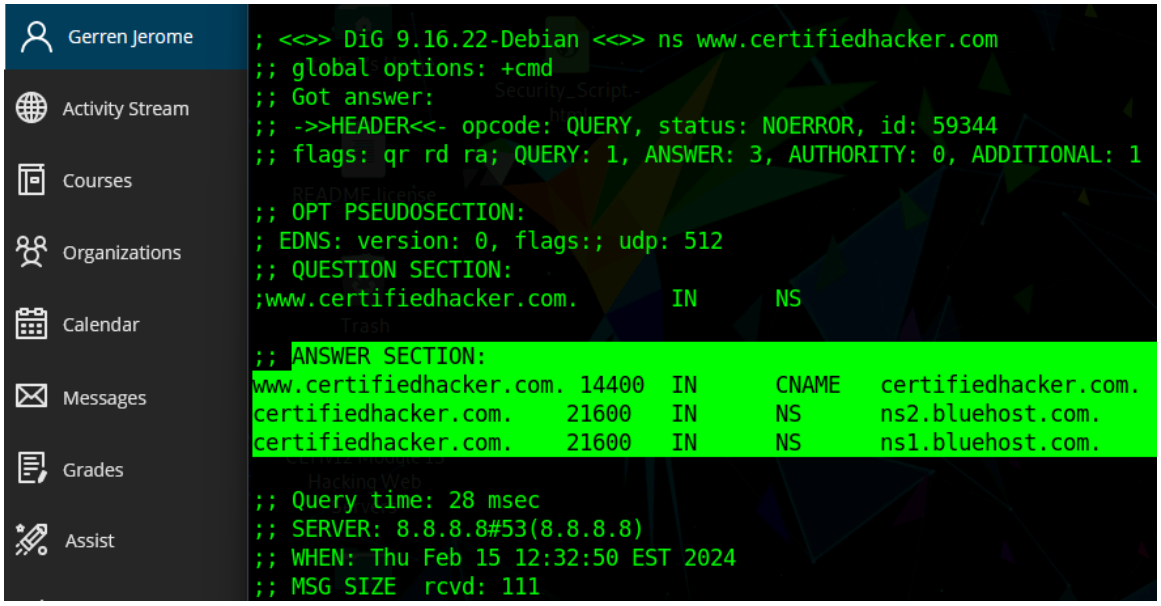


Gerren Jerome - Enumeration

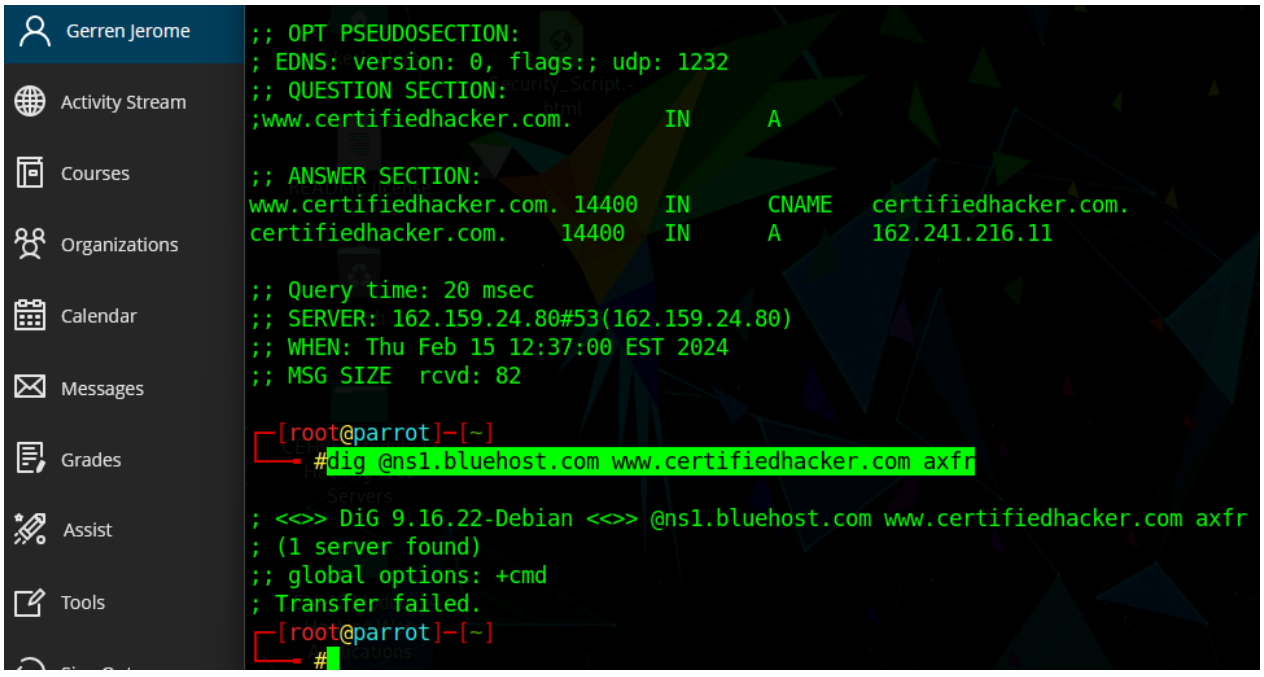
Perform enumeration (DNS)

Perform DNS enumeration using zone transfer.

scan result (dig ns www.certifiedhacker.com)

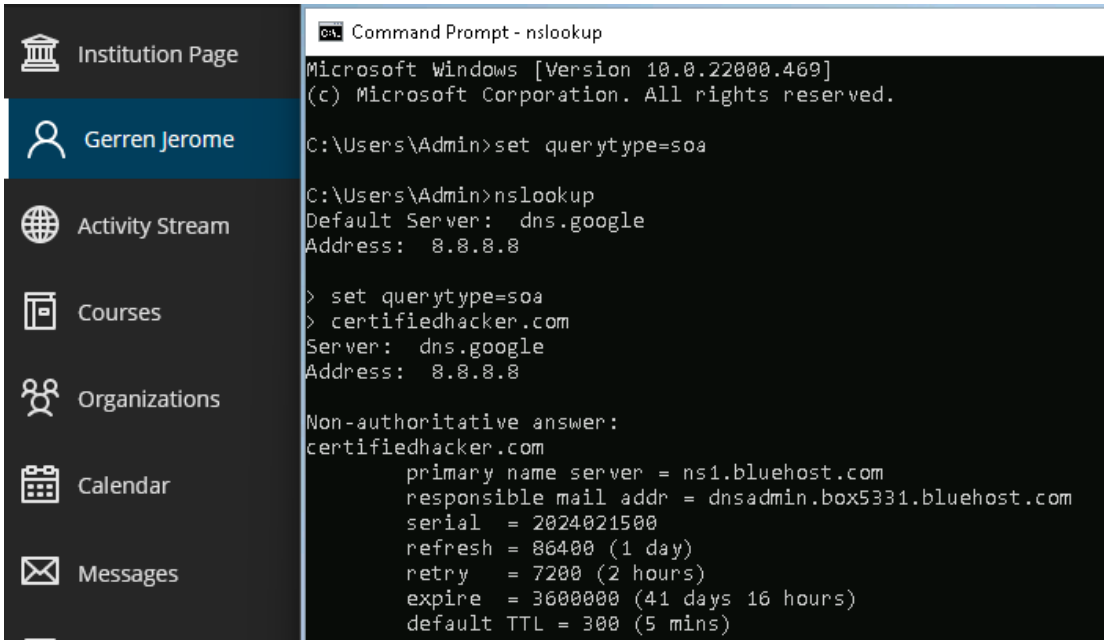


scan result (dig transfer failed?)

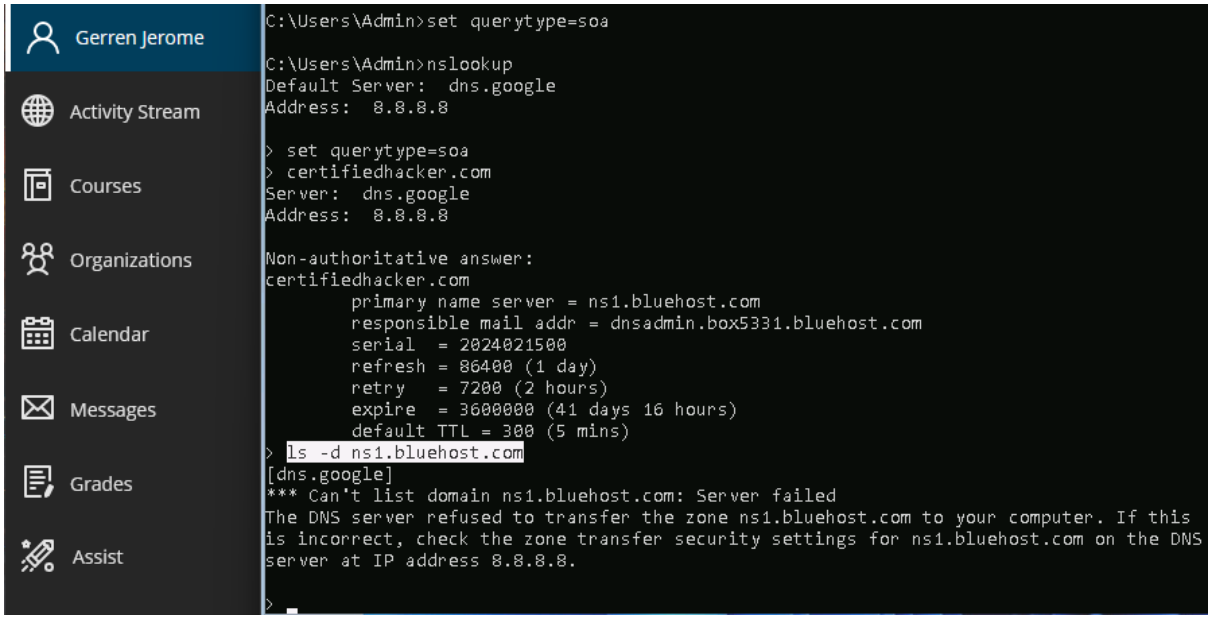


Gerren Jerome - Enumeration

scan result (nslookup (interactive mode) – certifiedhacker)



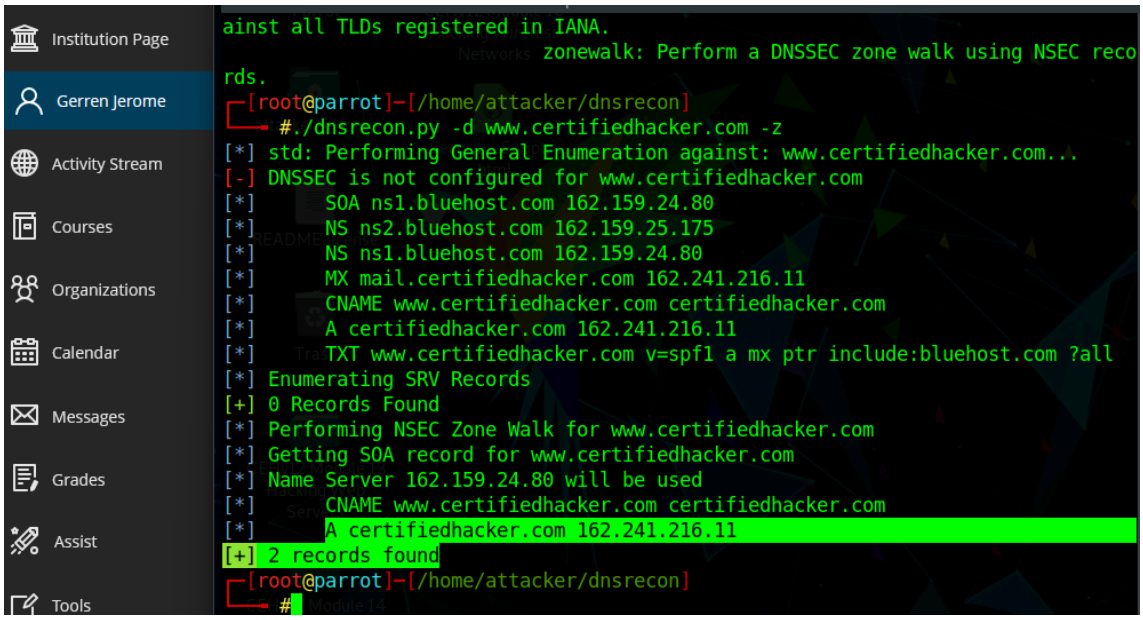
scan result (nslookup (interactive mode) – bluehost)



Gerren Jerome - Enumeration

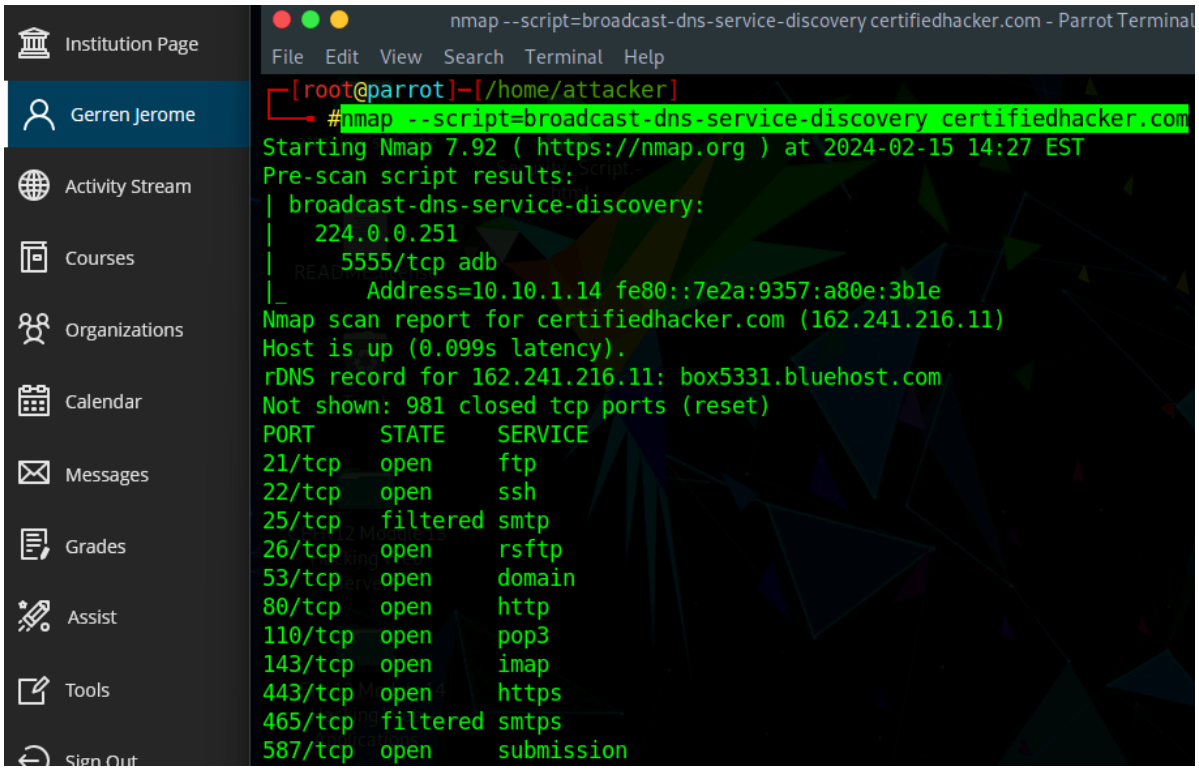
Perform DNS enumeration using DNSSEC zone walking

result (dnsrecon – certifiedhacker)



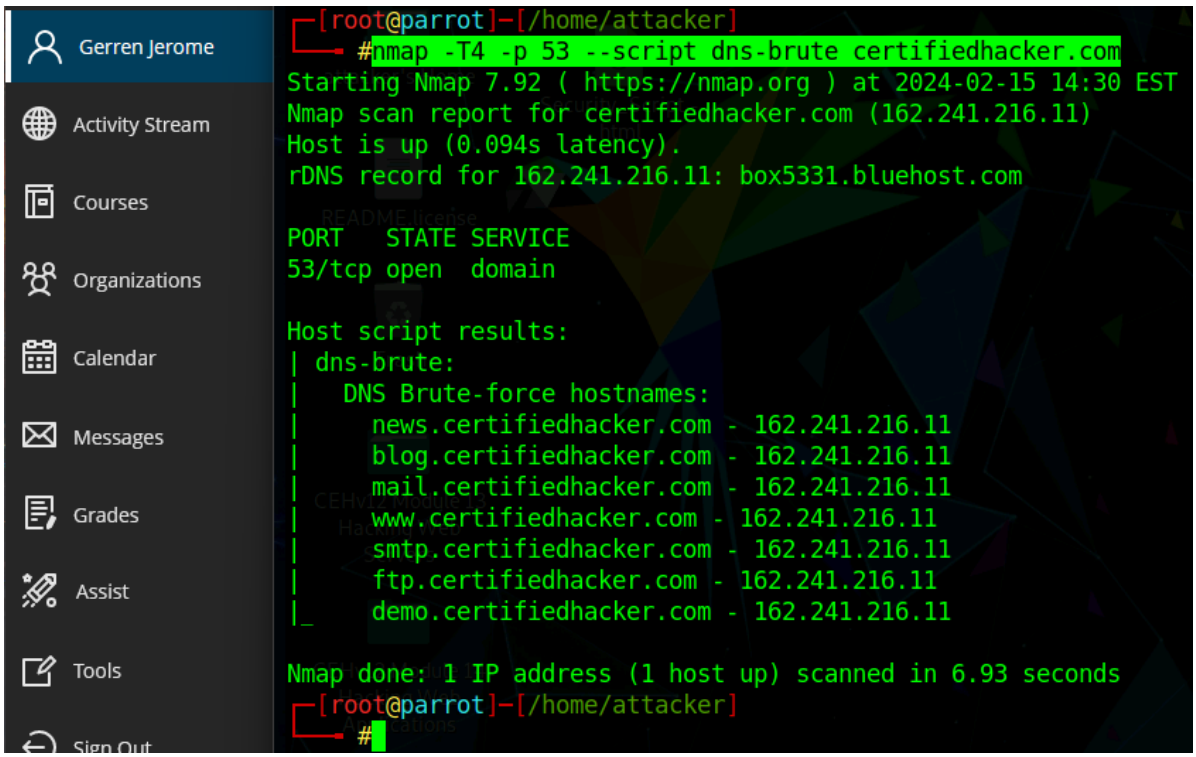
Perform DNS enumeration using Nmap

scan result (nmap service discovery)

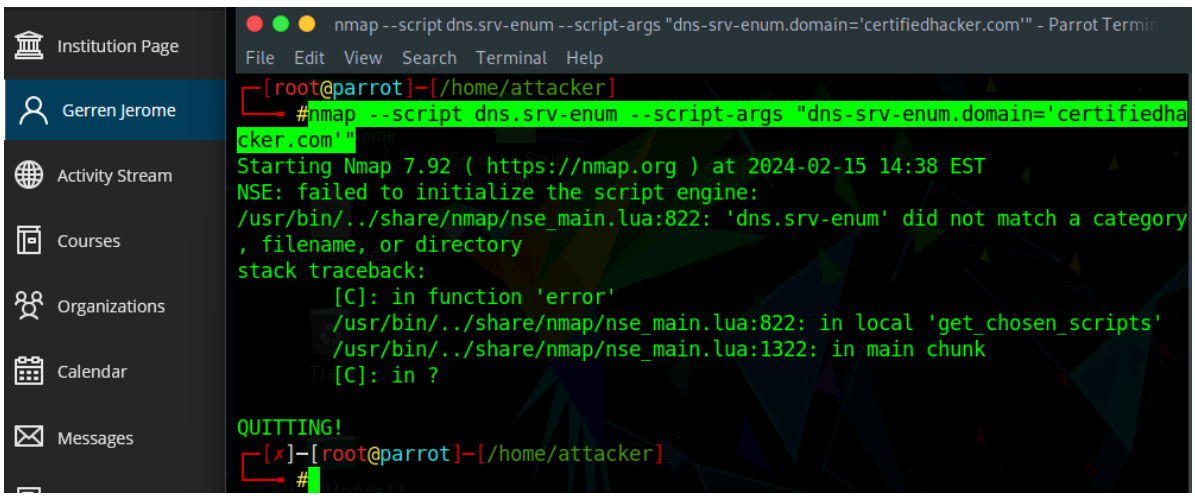


Gerren Jerome - Enumeration

scan result (associated subdomains)



scan result (SRV records)

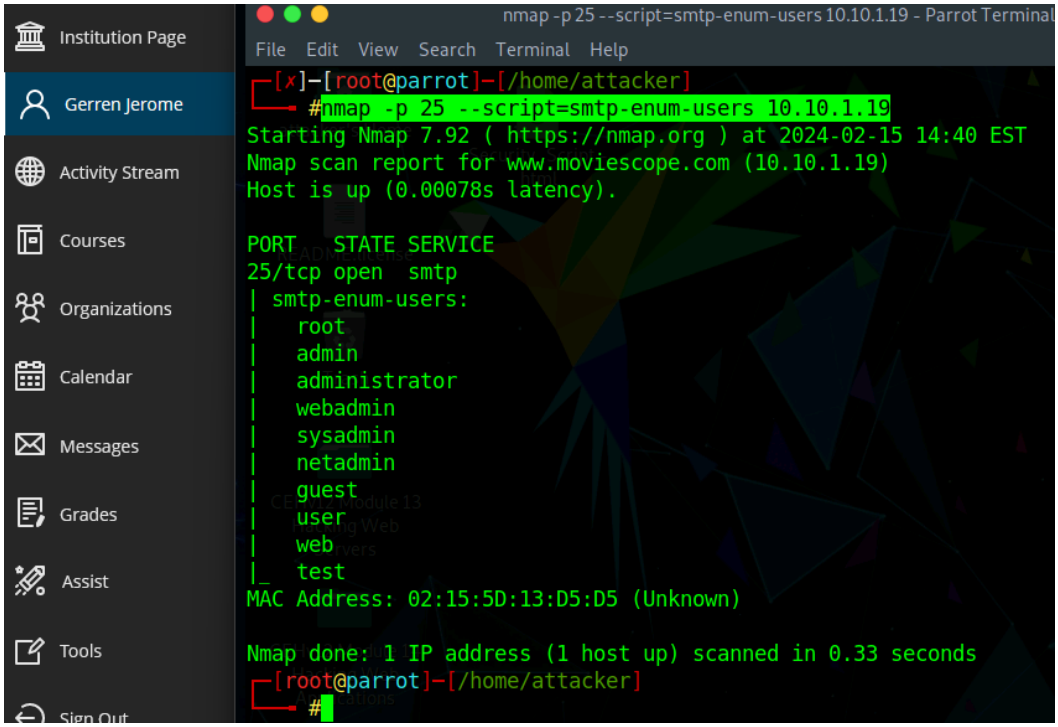


Gerren Jerome - Enumeration

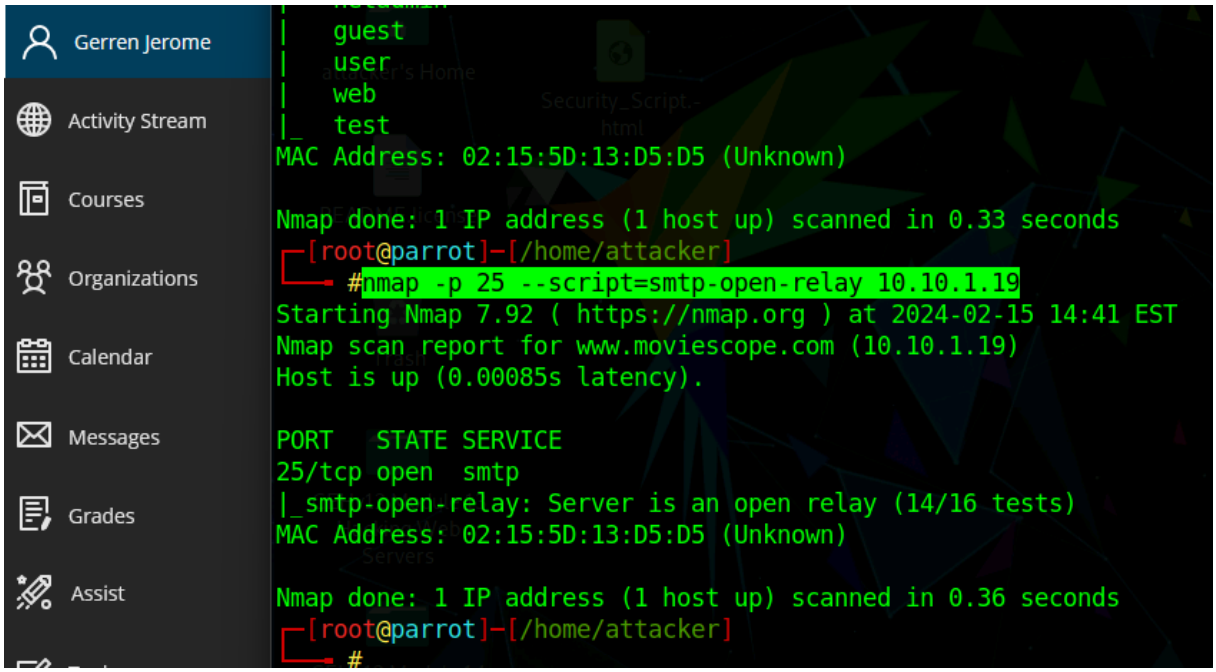
Perform enumeration (SMTP)

Perform SMTP enumeration using Nmap

list all mail users



list open SMTP relays

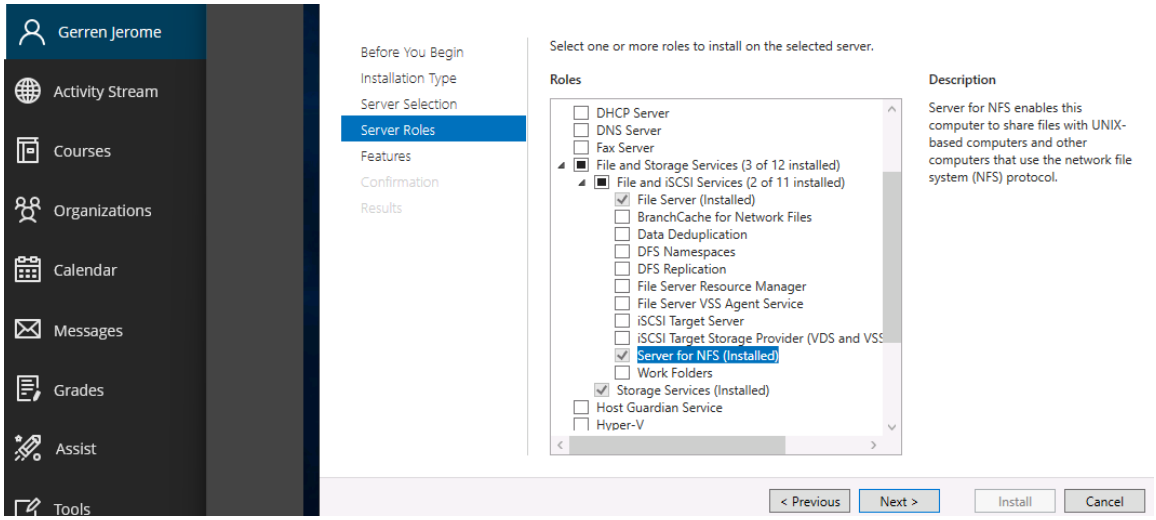


Gerren Jerome - Enumeration

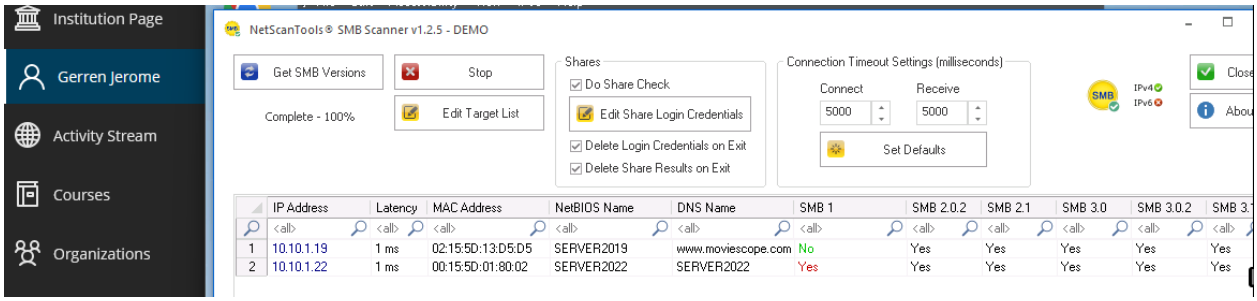
Perform enumeration (RPC, SMB, and FTP)

Perform SMB and RPC enumeration using NetScanTools Pro

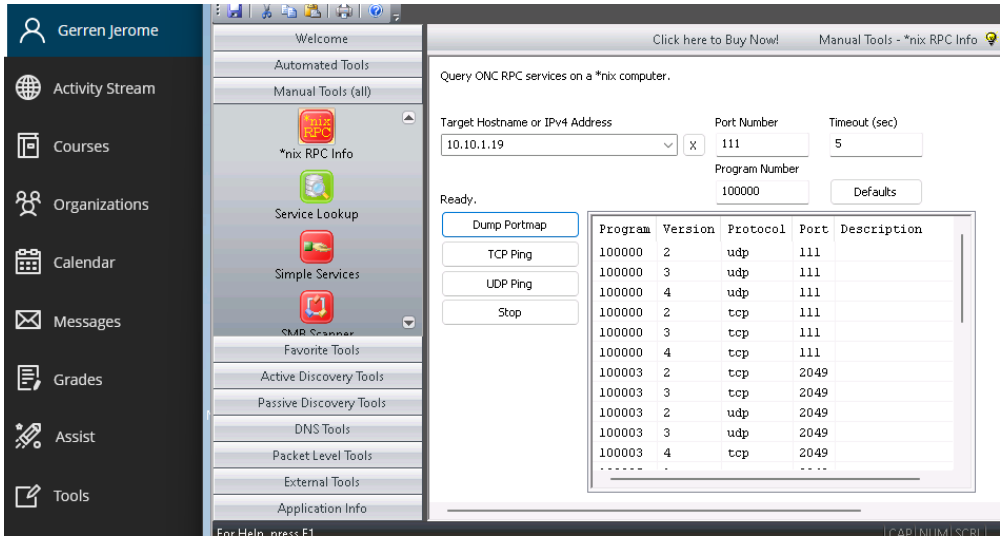
confirm install/enable NFS services.



SMB scanner results



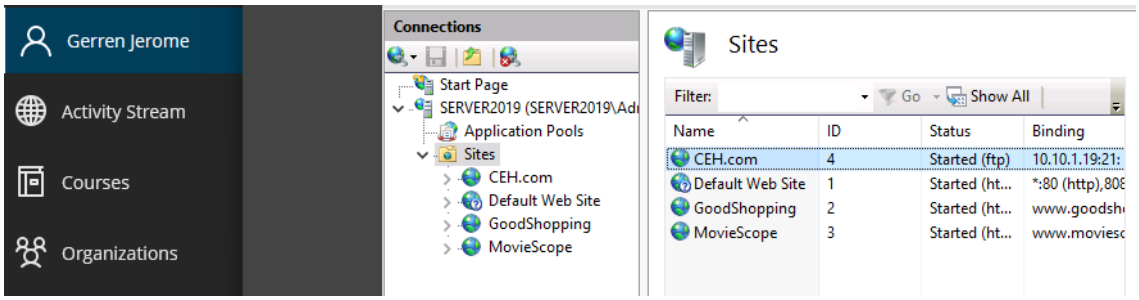
portmap dump (WIN_SVR_19)



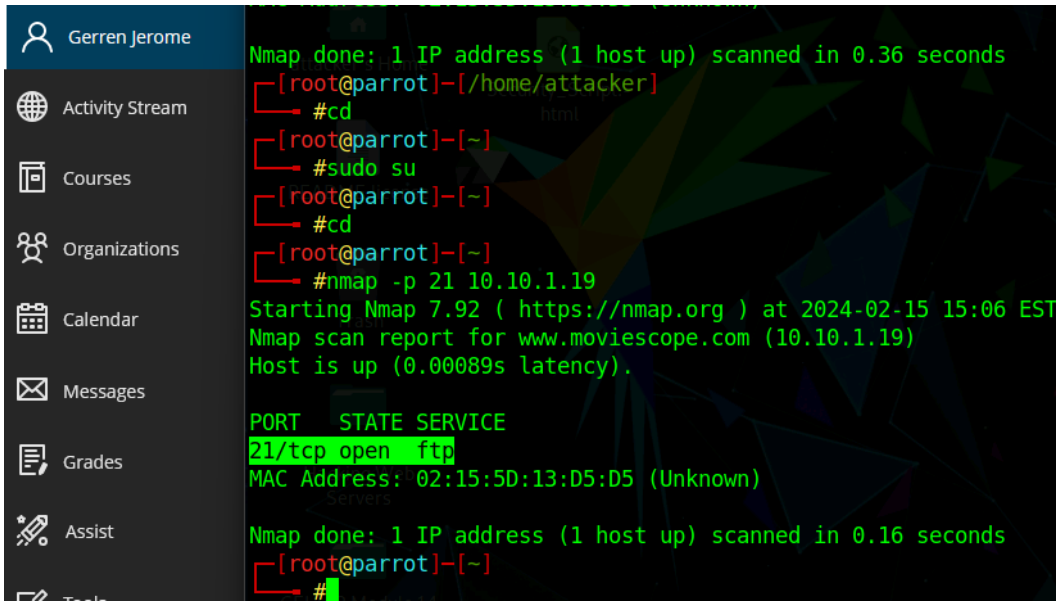
Gerren Jerome - Enumeration

Perform RPC, SMB, and FTP enumeration using Nmap.

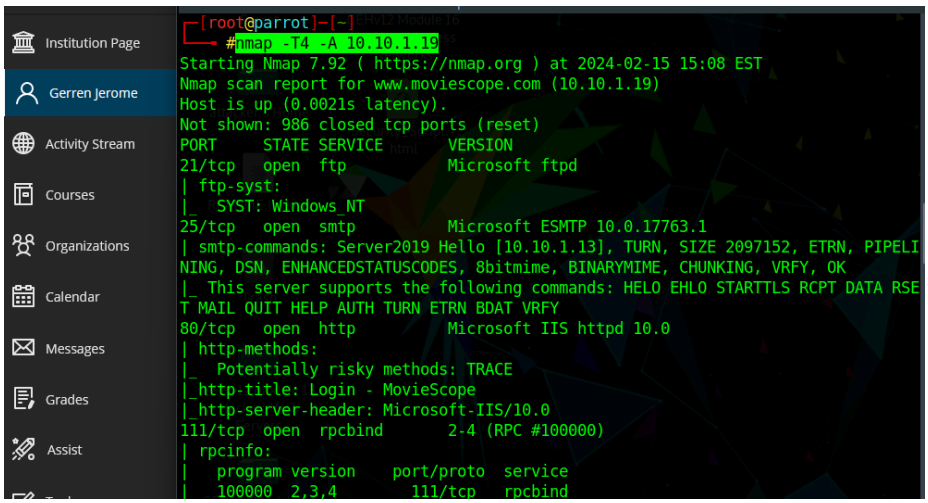
confirm addition of CEH.com FTP site to IIS



nmap scan (Port 21 - FTP)

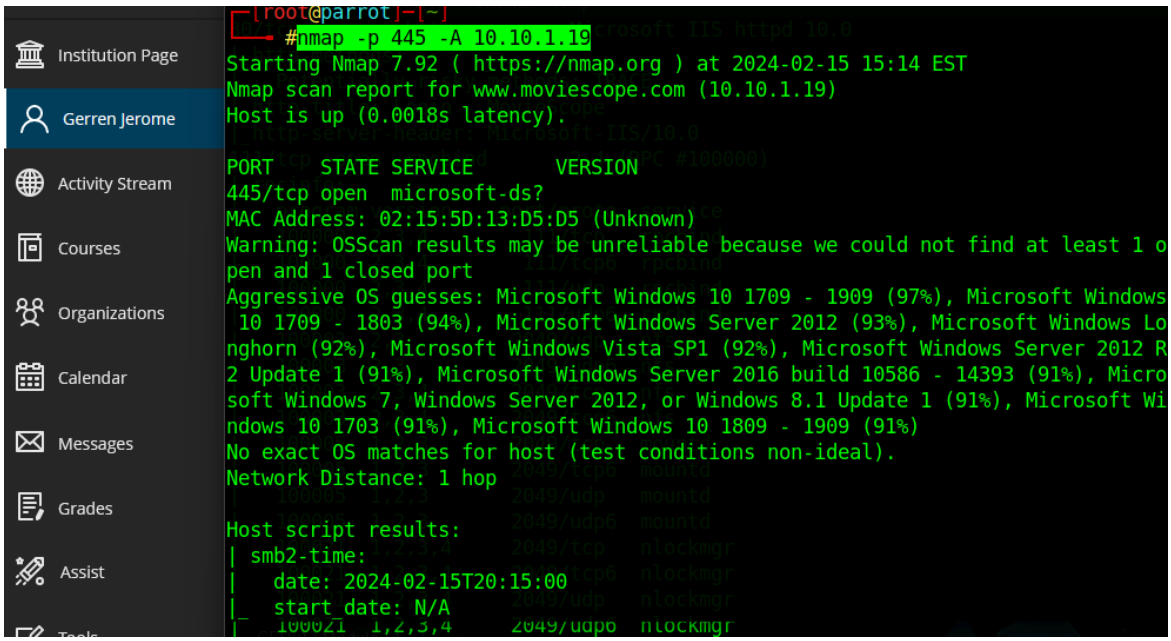


nmap scan (other services and ports)

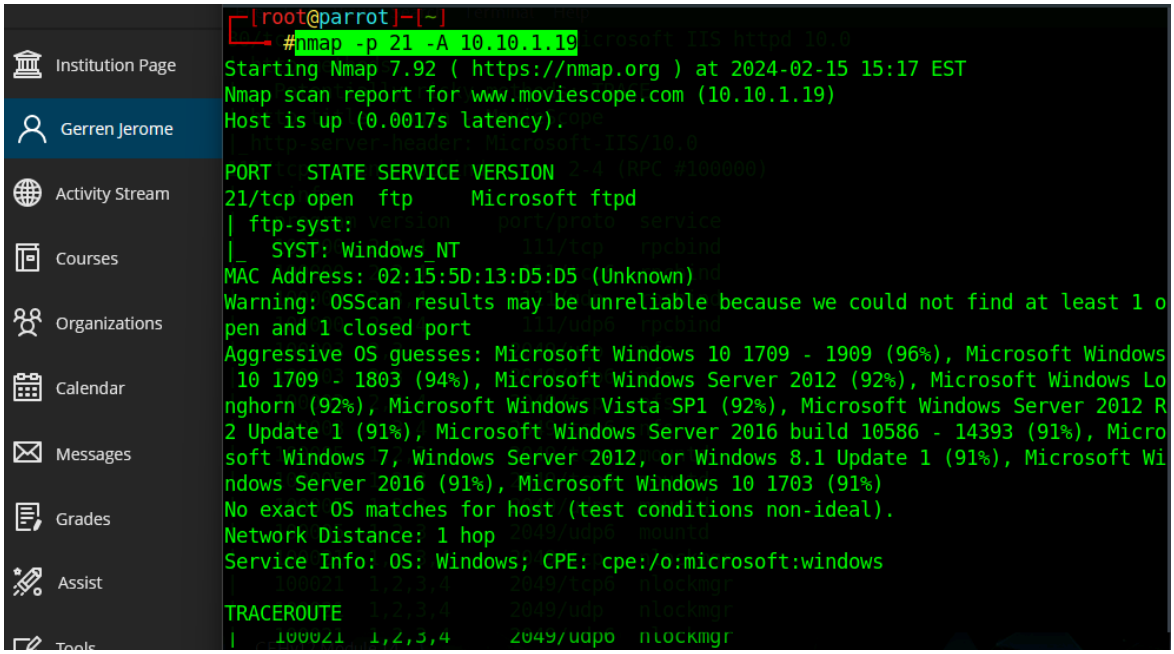


Gerren Jerome - [Enumeration]

nmap scan (Port 445 – SMB)



nmap scan (Port 21 + traceroute)

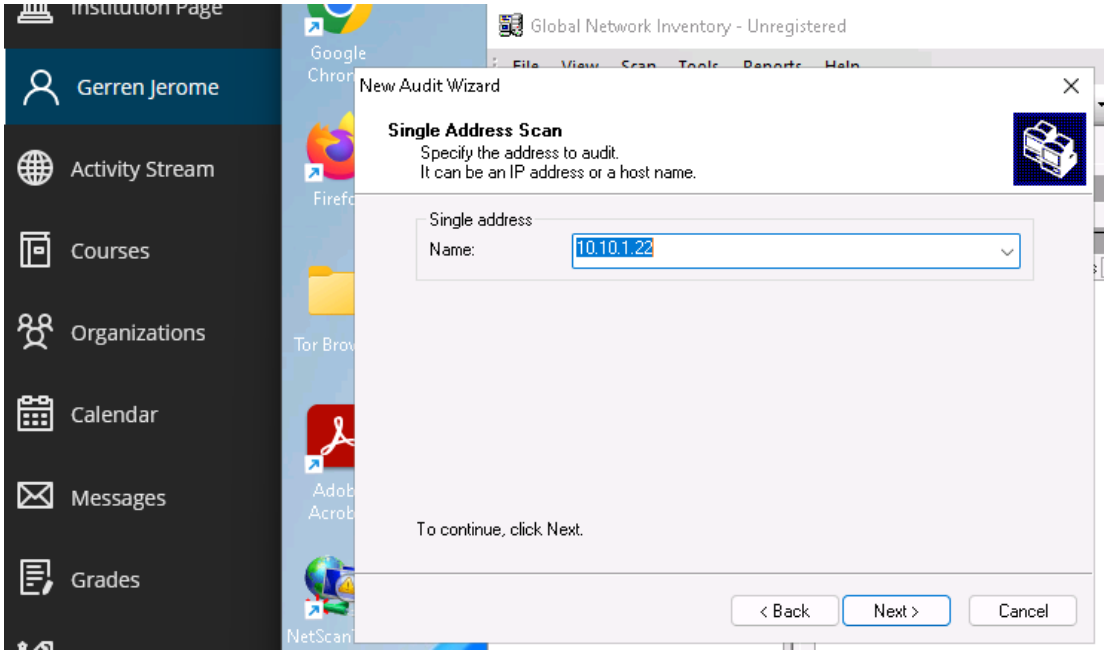


Gerren Jerome - Enumeration

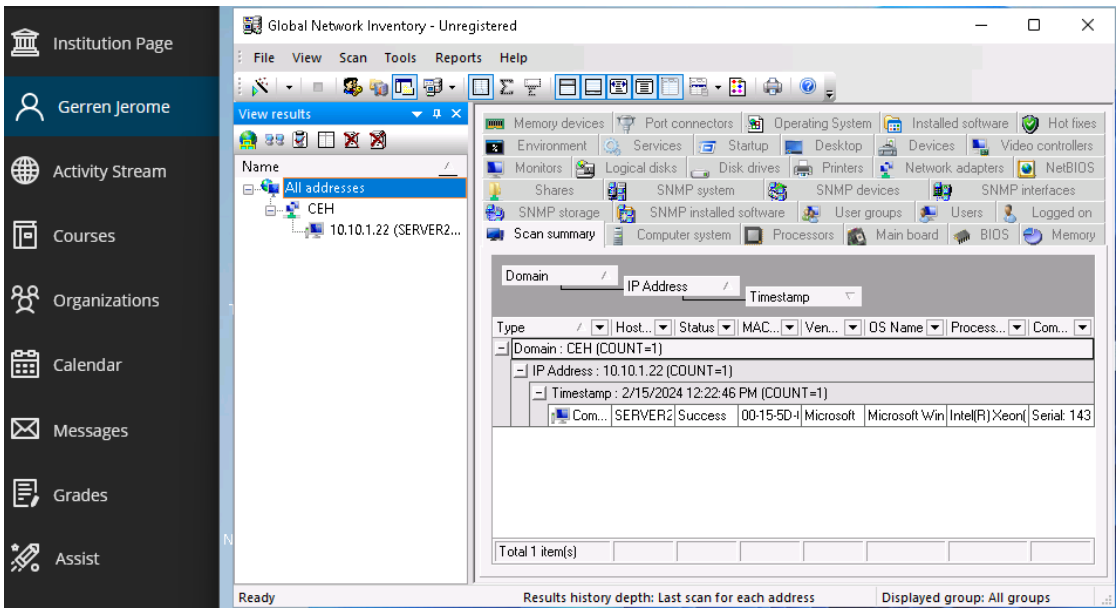
Perform enumeration using various enumeration tools.

Enumerate information using Global Network Inventory

confirm settings (GNI single address scan)

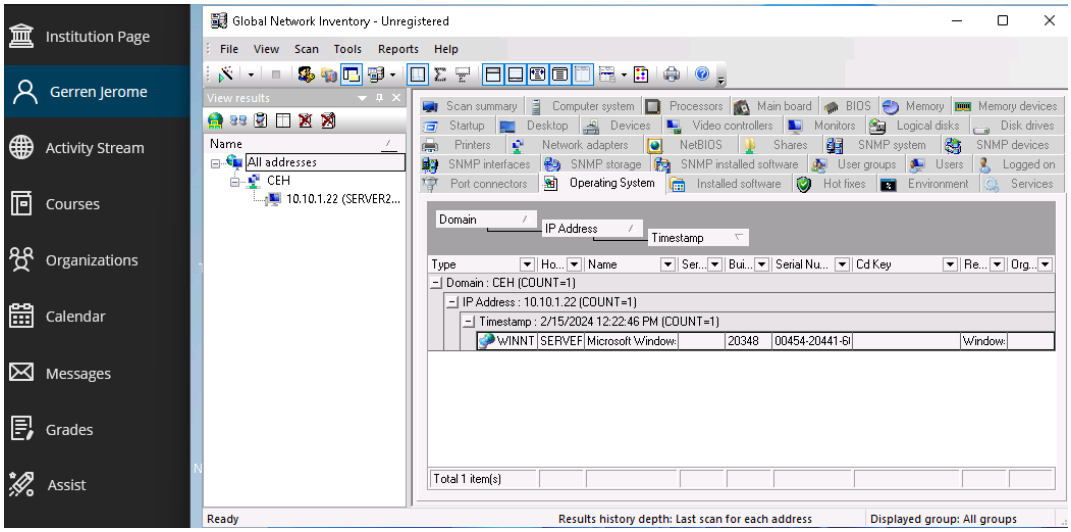


Scan summary (GNI)

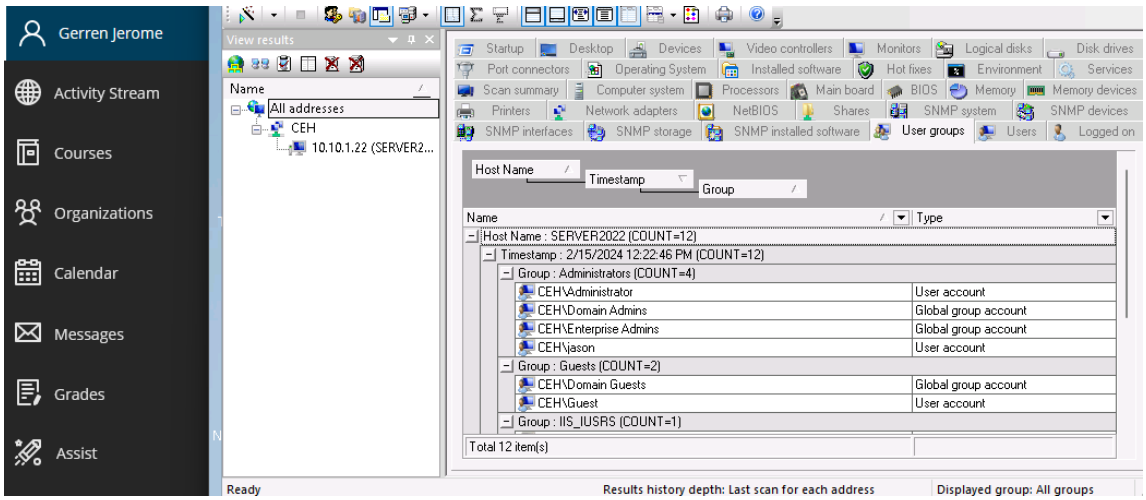


Gerren Jerome - Enumeration

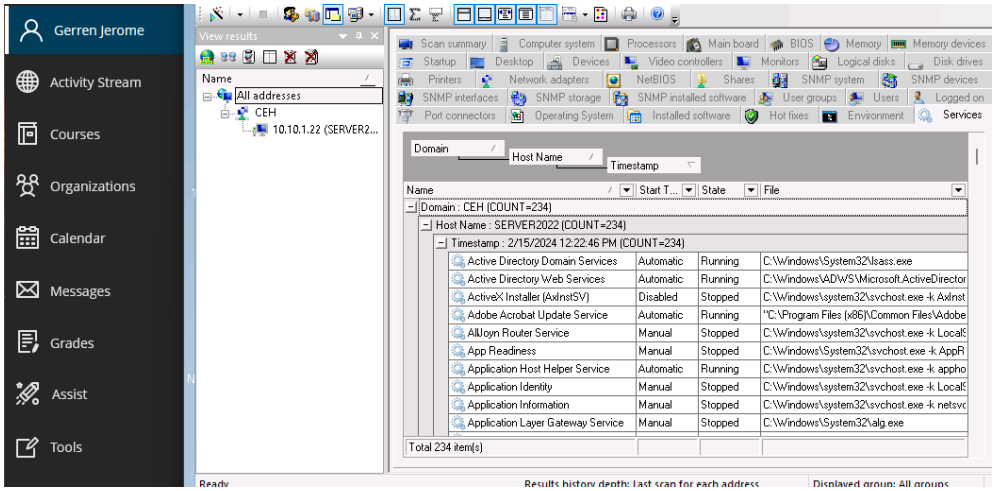
GNI Scan Result (Operating System)



GNI Scan Result (User Groups)

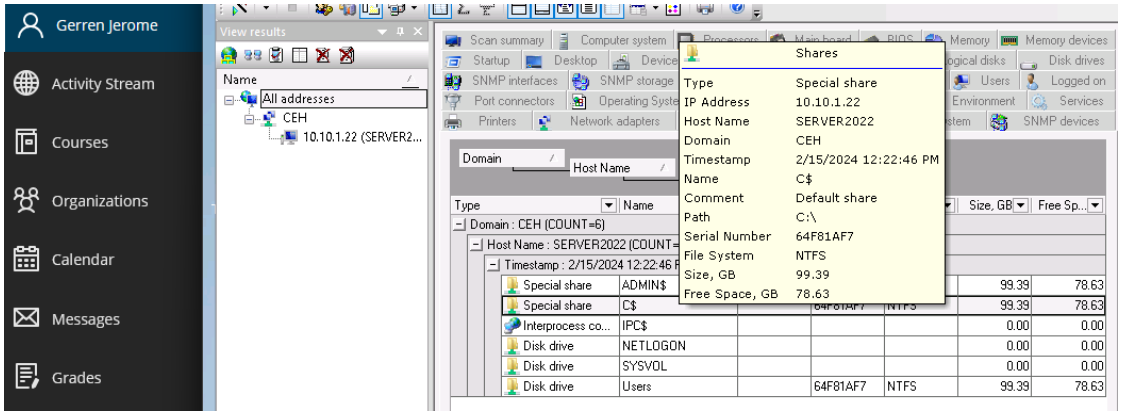


GNI Scan Result (Services)



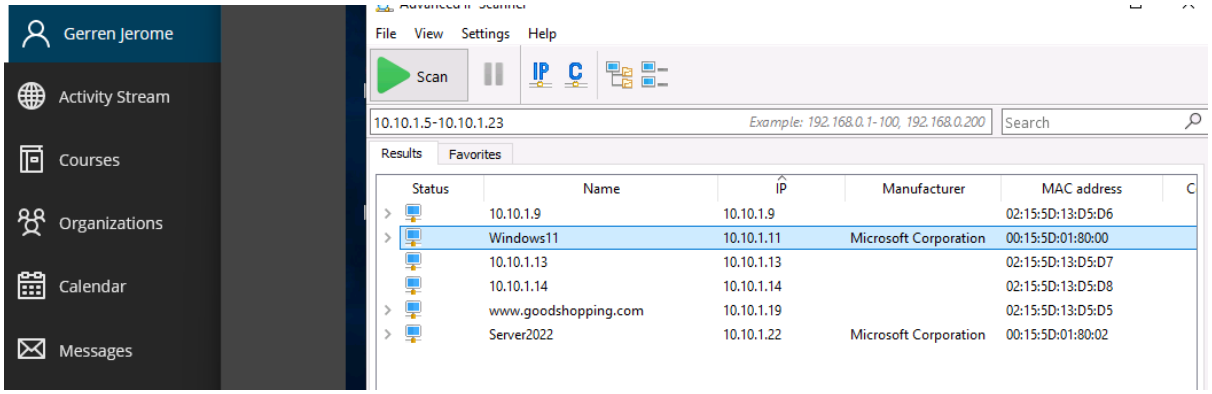
Gerren Jerome - Enumeration

GNI Scan Result (Shares)



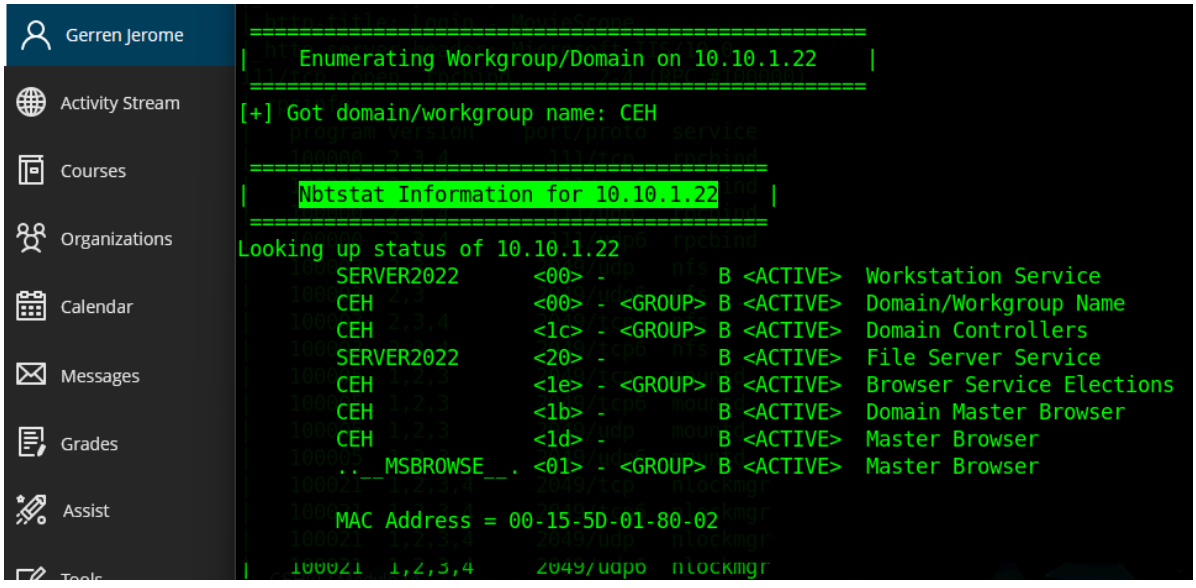
Enumerate network resources using Advanced IP Scanner

Advanced IP Scanner results



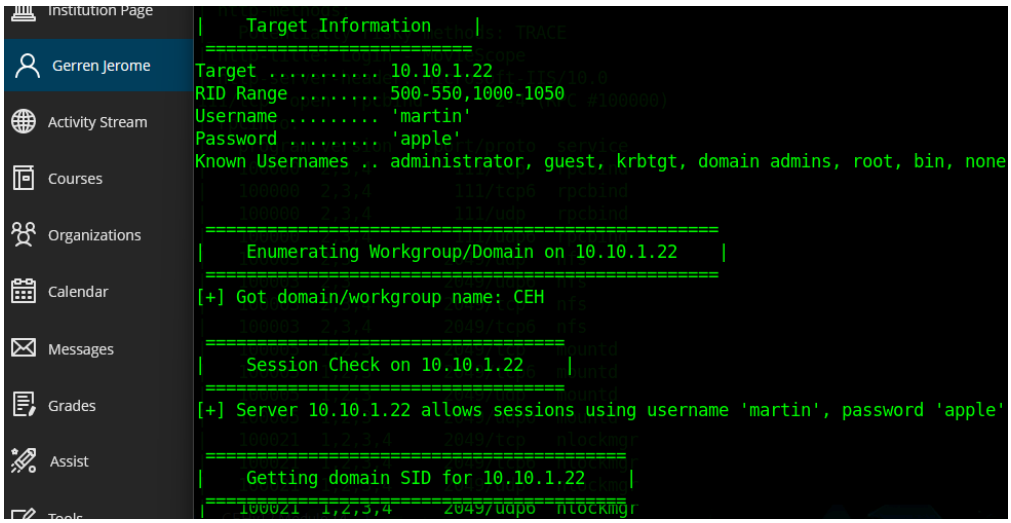
Enumerate information from Windows and Samba hosts using Enum4linux.

NetBIOS scan (10.10.1.22)

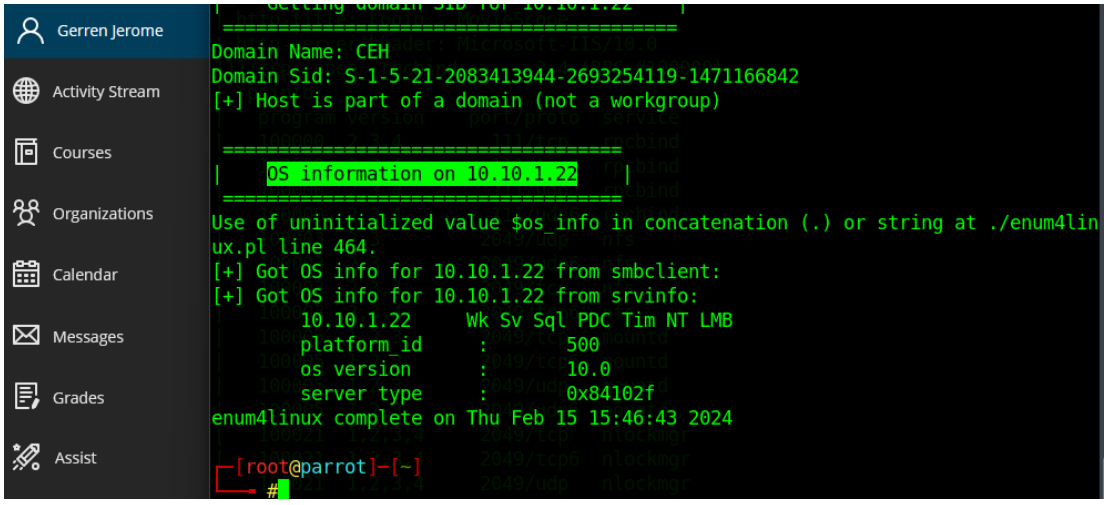


Gerren Jerome - Enumeration

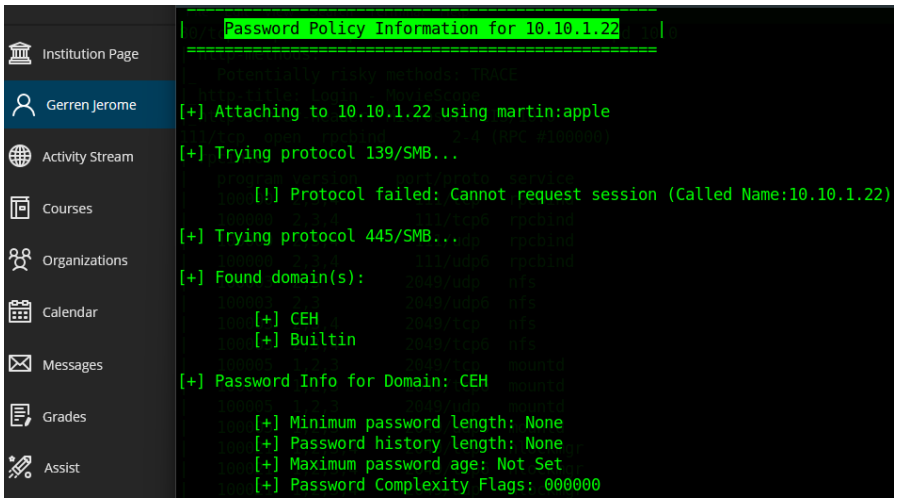
SID/RID info (10.10.1.22)



OS Details (10.10.1.22)

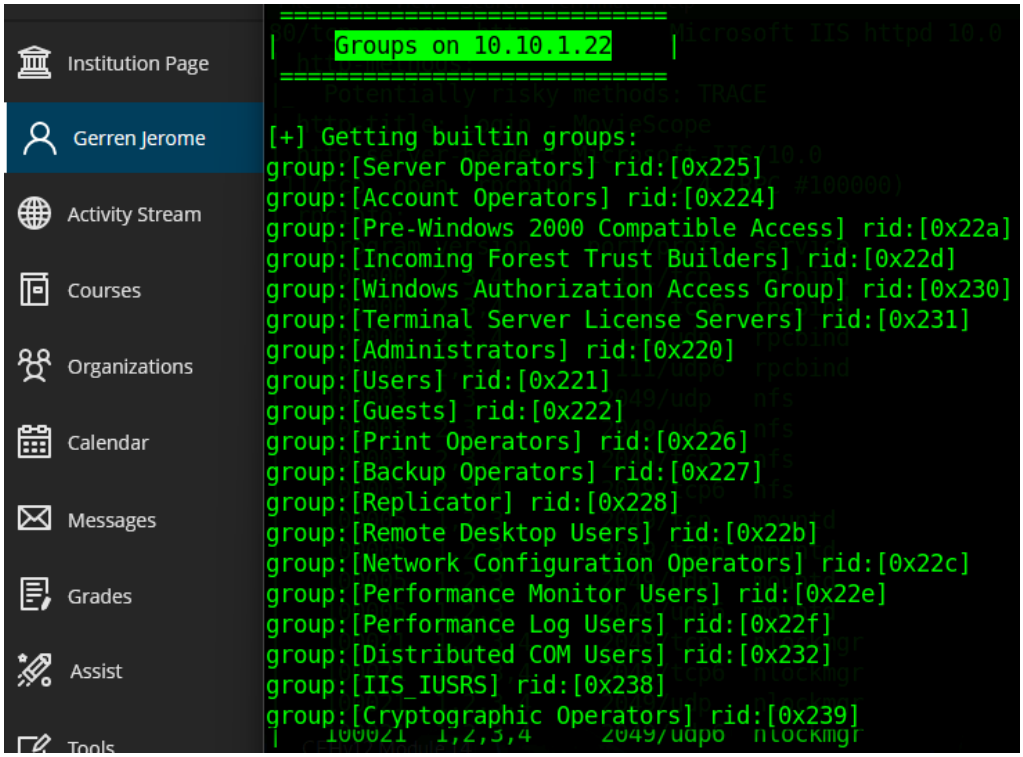


Password policy (10.10.1.22)

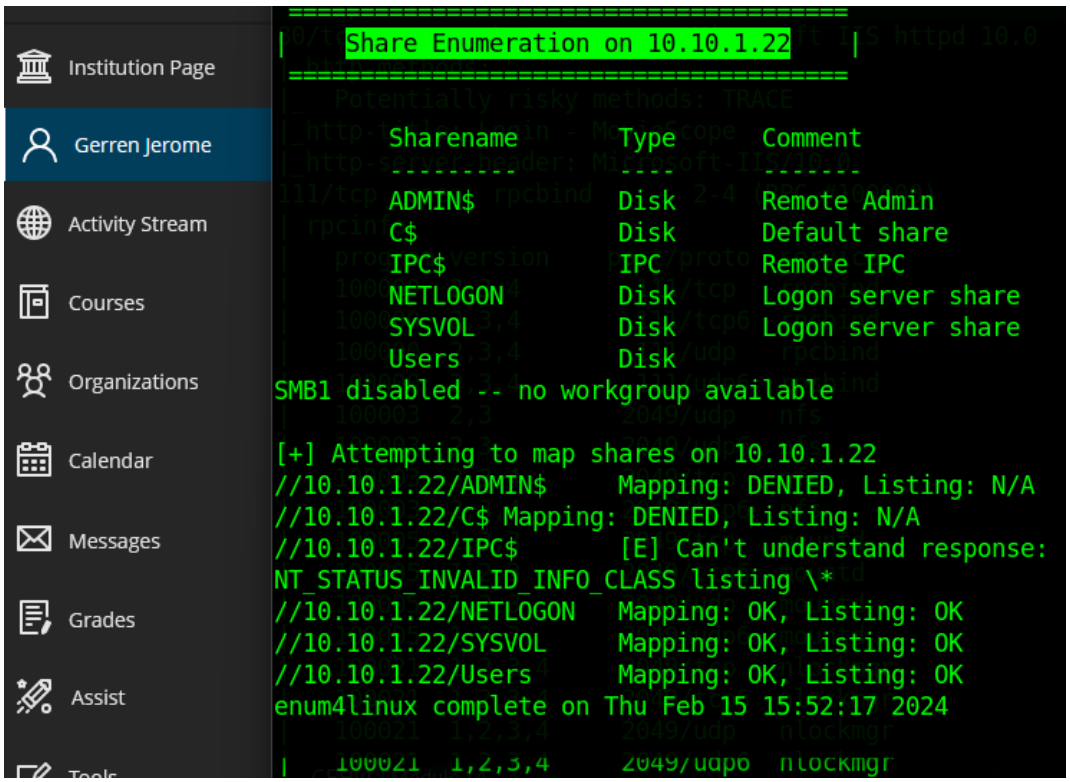


Gerren Jerome - Enumeration

Group Policy (10.10.1.22)



Shares (10.10.1.22)



Reflection

This project provided valuable hands-on experience with various enumeration techniques essential for ethical hacking and penetration testing. I developed a deeper understanding of how to effectively gather and analyze information from a target network, which is crucial for identifying potential security weaknesses.