CS6501: A2-1

1. Please complete the following Netlab exercises:

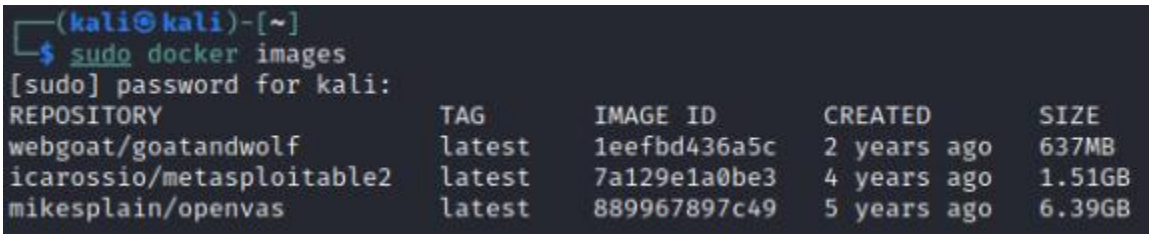
    a. **Lab 06: Vulnerability Checks with OpenVAS from the NDG Security+ V4 series**
    b. **Lab 07: Host Hardening from the NDG CySA+ series**
    c. **Lab 07: Performing Active Reconnaissance from the NDG Security+ v4 series**

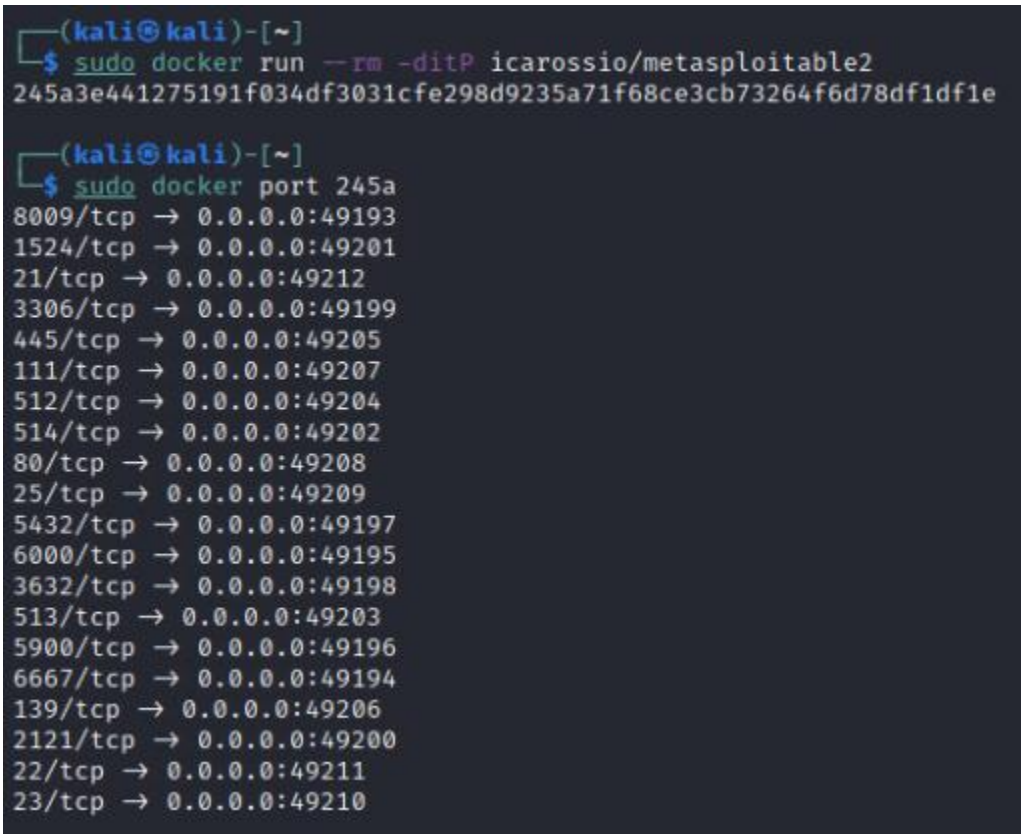
2. The deliverable is a separate document for each lab. Each NetLab exercise should be a separate document showing show the occasional screenshot (which includes your student ID and name) and a brief narrative describing what you are observing. This indicates to me that you have attempted the lab and I can confirm this by viewing the reservation logs on the system. The narrative explaining the screenshot indicates to me whether you understand what it is that is captured in the screenshot.

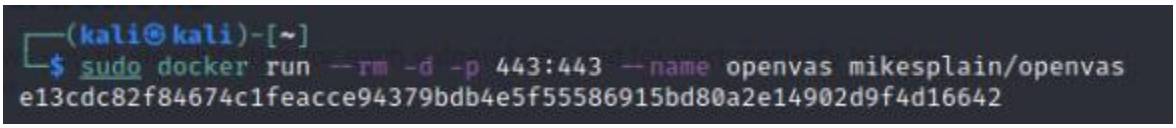
   The due date is 6 May 2024

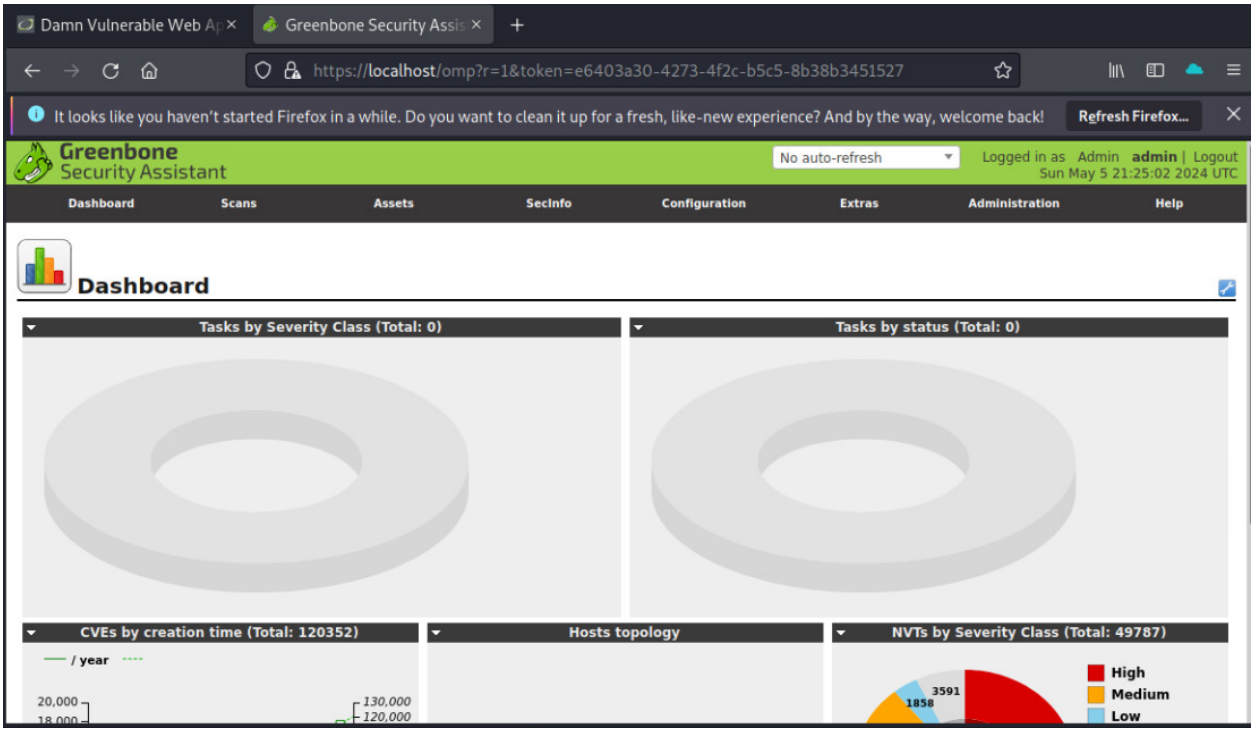
Lab 06: Vulnerability Checks with OpenVAS from the NDG Security+ V4 series

Checking available docker images and can see two files exist









Targets (1 of 1)

1 - 1 of 1

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
metasploitable	127.0.0.1	1	All TCP		

√Apply to page contents

(Applied filter: rows=10 first=1 sort=name)

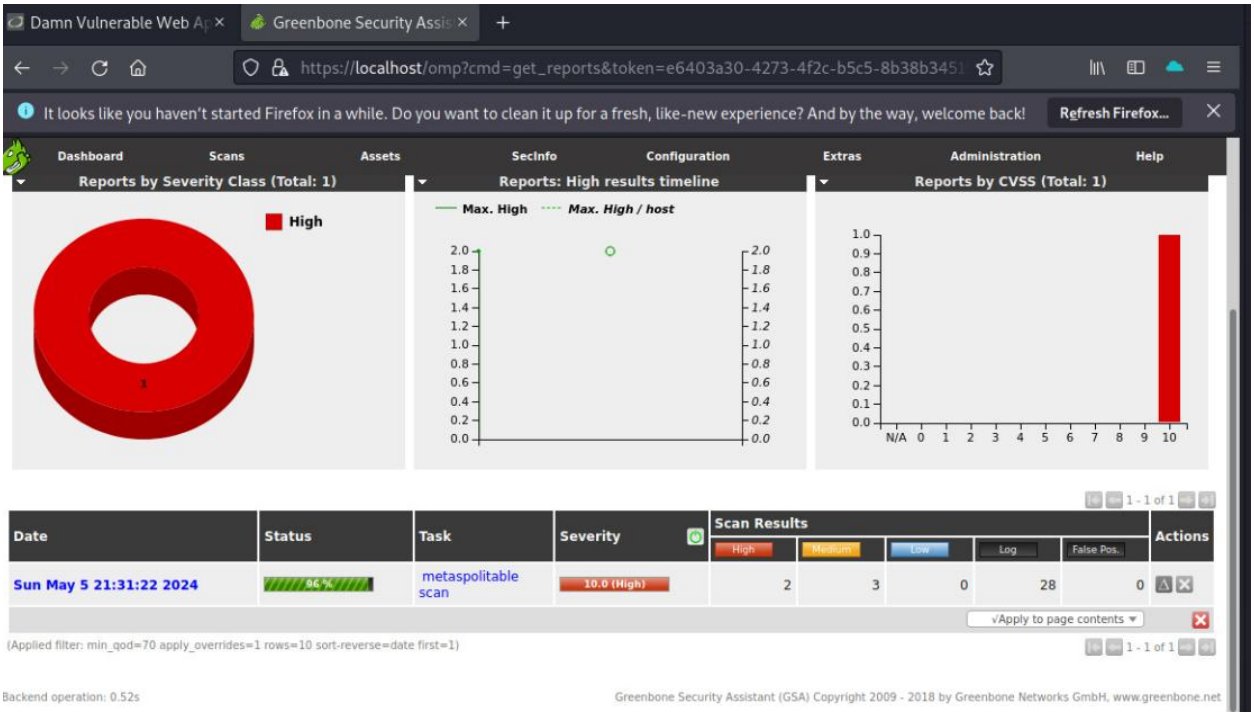
1 - 1 of 1

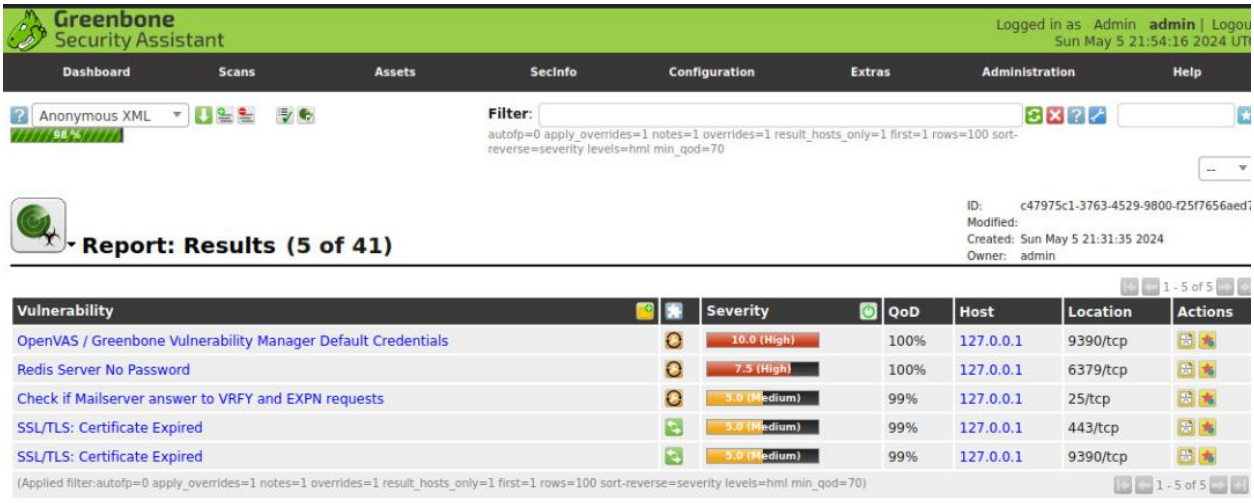
Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Sun May 5 21:31:22 2024	26 %	metaspolitable scan	5.0 (Medium)	0	1	0	16	0	

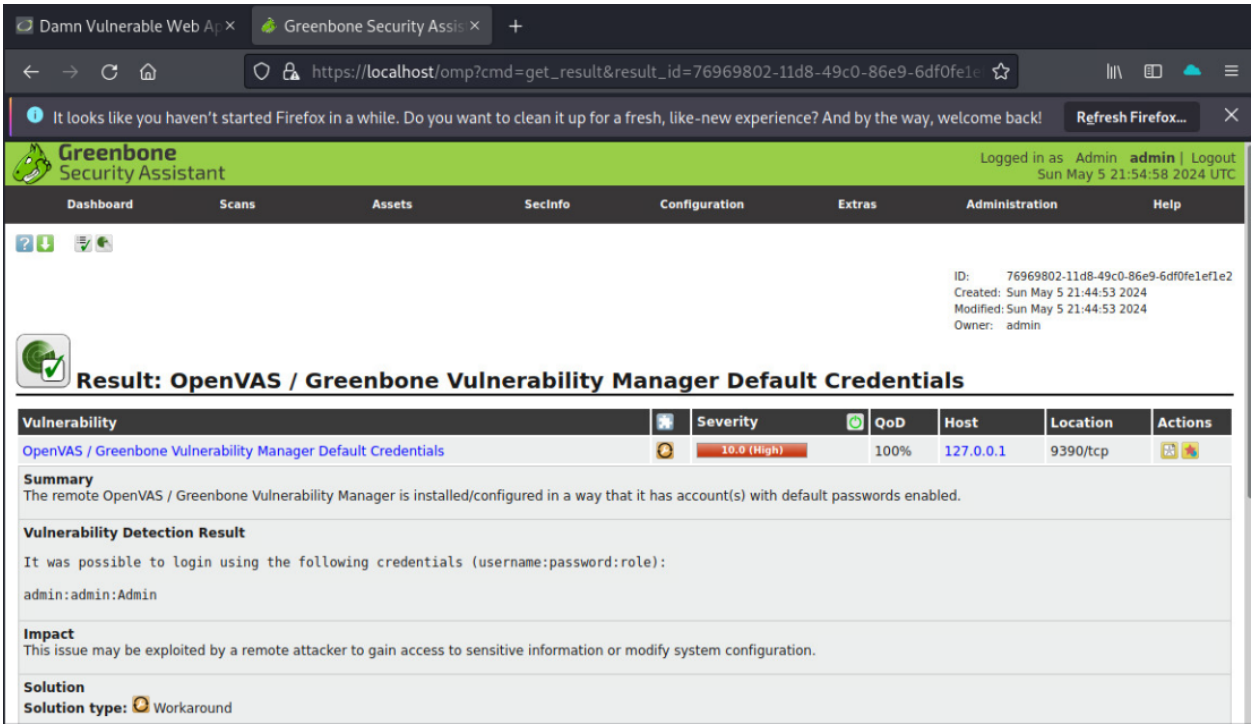
√Apply to page contents

(Applied filter: min_qod=70 apply_overrides=1 rows=10 sort-reverse=date first=1)

1 - 1 of 1


Damn Vulnerable Web Ap
Greenbone Security Assis
https://localhost/omp?cmd=get_reports&token=e6403a30-4273-4f2c-b5c5-8b38b345
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Reports by Severity Class (Total: 1)
High
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
Date
Status
Task
Severity
Scan Results
High
Medium
Low
Log
False Pos.
Actions
Sun May 5 21:31:22 2024
96 %
metaspolitable scan
10.0 (High)
2
3
0
28
0
√Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 sort-reverse=date first=1)
1 - 1 of 1
Backend operation: 0.52s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net


Greenbone
Security Assistant
Logged in as Admin admin | Logou
Sun May 5 21:54:16 2024 UT
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Anonymous XML
98 %
Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70
Report: Results (5 of 41)
ID: c47975c1-3763-4529-9800-f25f7656aed
Modified:
Created: Sun May 5 21:31:35 2024
Owner: admin
1 - 5 of 5
Vulnerability
Severity
QoD
Host
Location
Actions
OpenVAS / Greenbone Vulnerability Manager Default Credentials
10.0 (High)
100%
127.0.0.1
9390/tcp
Redis Server No Password
7.5 (High)
100%
127.0.0.1
6379/tcp
Check if Mailserver answer to VRFY and EXPN requests
5.0 (Medium)
99%
127.0.0.1
25/tcp
SSL/TLS: Certificate Expired
5.0 (Medium)
99%
127.0.0.1
443/tcp
SSL/TLS: Certificate Expired
5.0 (Medium)
99%
127.0.0.1
9390/tcp
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)
1 - 5 of 5



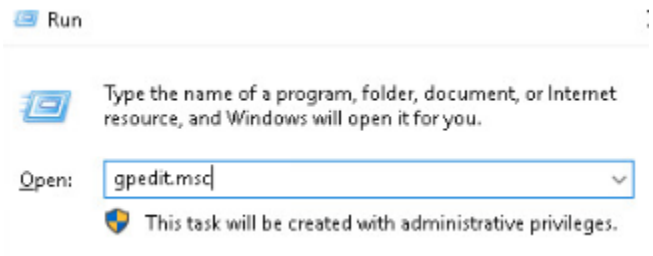
Lab History: Lab 06: Vulnerability Checks with OpenVAS

Summary | PCs

Community	default
Class	CS6501 Information Security 2 2024
Reservation ID	18619
Pod ID	2251
Pod Name	NDG Security+ v4 01
Exercise	Lab 06: Vulnerability Checks with OpenVAS
Attendees	Andrew Gaff
Date/Time	2024-05-06 09:05
Duration (Hrs.)	0.83

Lab 07: Host Hardening from the NDG CySA+ series

In this lab we will see other methods of increasing host security. This is known as hardening. Configure Windows group policies, set up an acceptable use splash screen, close unused ports, installing patches and using windows defender to periodically scan hosts.




```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:35 EDT
Nmap scan report for 192.168.0.50
Host is up (0.00068s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
sysadmin@mintos:~$
```

```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:38 EDT
Nmap scan report for 192.168.0.50
Host is up (0.00031s latency).
Not shown: 98 filtered ports
PORT     STATE SERVICE
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:39 EDT
Nmap scan report for 192.168.0.50
Host is up (0.0004s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
sysadmin@mintos:~$
```

Terminal - sysadmin@mintos: ~

File Edit View Terminal Tabs Help

```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:39 EDT
Nmap scan report for 192.168.0.50
Host is up (0.0004s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
sysadmin@mintos:~$ nmap -F -Pn 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:40 EDT
Nmap scan report for 172.16.1.10
Host is up (0.00047s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
sysadmin@mintos:~$
```

Terminal - sysadmin@mintos: ~

File Edit View Terminal Tabs Help

```
sysadmin@mintos:~$ nmap -F -Pn 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-08 17:58 EDT
Nmap scan report for 172.16.1.10
Host is up (0.00050s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
sysadmin@mintos:~$
```

```
PS C:\Users\Administrator> get-hotfix -Id KB5012170

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
WIN-E3AIDI... Security Update  KB5012170     WIN-E3AIDIHECNG\A... 11/10/2022 12:00:00 AM
```

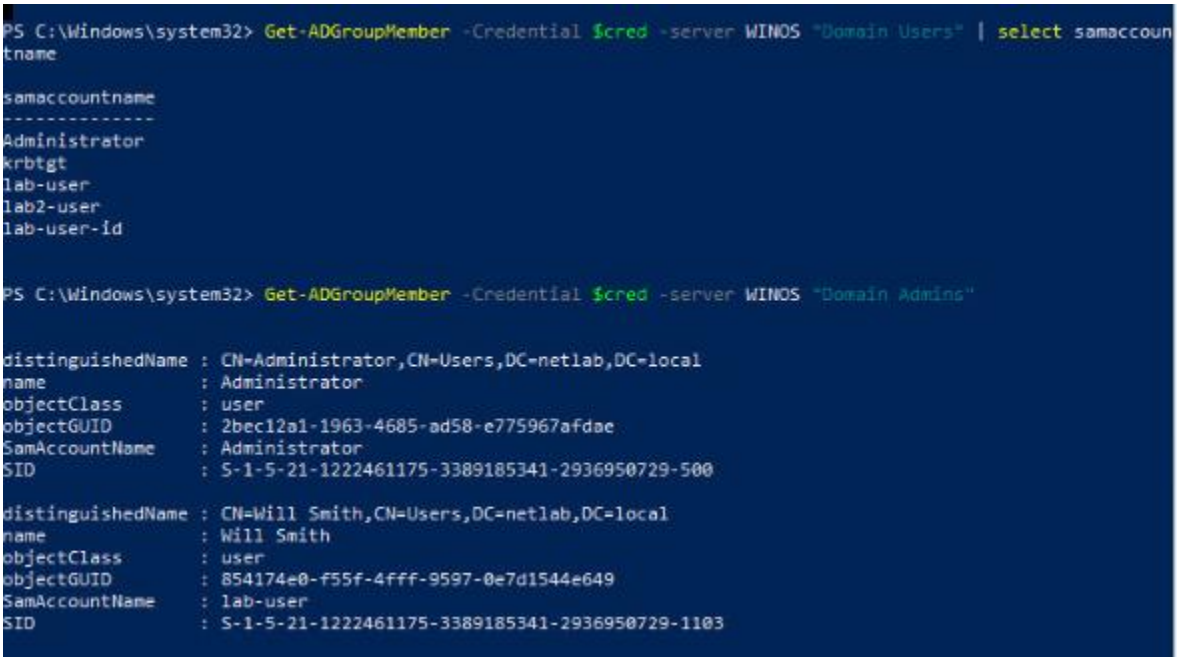
Lab History: Lab 07: Host Hardening

Summary | PCs

Community	default
Class	CS6501 Information Security 2 2024
Reservation ID	18656
Pod ID	2283
Pod Name	NDG CySA+ 03
Exercise	Lab 07: Host Hardening
Attendees	Andrew Gaff
Date/Time	2024-05-09 09:08
Duration (Hrs.)	1.00

Lab 07: Performing Active Reconnaissance from the NDG Security+ v4 series

In this lab, you will use PowerShell for active reconnaissance on a Windows server. Also, you will use a variety of tools to finish the same types of tasks on Linux. Objective In this lab, you will perform the following tasks: Experience active reconnaissance in Windows and in Linux Scan the network for vulnerable systems



```
PS C:\Windows\system32> Get-ADDomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=netlab,DC=local
DeletedObjectsContainer           : CN=Deleted Objects,DC=netlab,DC=local
DistinguishedName                 : DC=netlab,DC=local
DNSRoot                           : netlab.local
DomainControllersContainer        : OU=Domain Controllers,DC=netlab,DC=local
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-1222461175-3389185341-2936950729
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=netlab,DC=local
Forest                            : netlab.local
InfrastructureMaster              : WinOS.netlab.local
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=n
                                    etlab,DC=local}
LostAndFoundContainer             : CN=LostAndFound,DC=netlab,DC=local
ManagedBy                         :
Name                              : netlab
NetBIOSName                       : NETLAB
ObjectClass                       : domainDNS
ObjectGUID                        : e2cc52cb-e710-42a9-80b6-2c451a5e7e94
ParentDomain                      :
PDCEmulator                       : WinOS.netlab.local
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=netlab,DC=local
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {WinOS.netlab.local}
RIDMaster                         : WinOS.netlab.local
SubordinateReferences             : {DC=ForestDnsZones,DC=netlab,DC=local,
                                    DC=DomainDnsZones,DC=netlab,DC=local,
                                    CN=Configuration,DC=netlab,DC=local}
SystemsContainer                  : CN=System,DC=netlab,DC=local
UsersContainer                    : CN=Users,DC=netlab,DC=local



PS C:\Windows\system32> Get-ADUser -filter 'samaccountname -eq "lab2-user"'


DistinguishedName : CN=John Deere,CN=Users,DC=netlab,DC=local
Enabled           : True
GivenName         : John
Name              : John Deere
ObjectClass       : user
ObjectGUID        : fe6836b4-f6fd-4c5b-b817-311c1b4703d1
SamAccountName    : lab2-user
SID               : S-1-5-21-1222461175-3389185341-2936950729-1104
```

```
PS C:\Windows\system32> [system.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()


Forest                  : netlab.local
DomainControllers       : {WinOS.netlab.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : WinOS.netlab.local
RidRoleOwner            : WinOS.netlab.local
InfrastructureRoleOwner : WinOS.netlab.local
Name                    : netlab.local



PS C:\Windows\system32>
```

Part 3: Scanning the network for vulnerable systems

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.*
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:37 CDT
Nmap scan report for 172.16.1.1
Host is up (0.012s latency).
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00043s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.11 seconds
```

```
Spoofing MAC address 2B:A8:DD:7B:56:AA (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored without the necessary privileges.
Initiating Ping Scan at 17:38
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 17:38, 2.91s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:38
Completed Parallel DNS resolution of 1 host. at 17:38, 13.00s elapsed
Nmap scan report for 172.16.1.0 [host down]
Nmap scan report for 172.16.1.1
Host is up (0.00063s latency).
Nmap scan report for 172.16.1.2 [host down]
Nmap scan report for 172.16.1.3 [host down]
Nmap scan report for 172.16.1.4 [host down]
Nmap scan report for 172.16.1.5 [host down]
Nmap scan report for 172.16.1.6 [host down]
Nmap scan report for 172.16.1.7 [host down]
Nmap scan report for 172.16.1.8 [host down]
Nmap scan report for 172.16.1.9 [host down]
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00050s latency).
Nmap scan report for 172.16.1.11 [host down]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -P0 172.16.1.10
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:40 CDT
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00041s latency).
Not shown: 991 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.0.6
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:41 CDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -0 192.168.0.1
nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:42 CDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.59 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.0.0/24 172.16.1.0/28
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:44 CDT
Nmap scan report for 172.16.1.1
Host is up (0.00027s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00057s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 272 IP addresses (2 hosts up) scanned in 16.19 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.16.1.10
Starting Nmap 7.91 ( https://nmap.org ) at 2024-05-08 17:46 CDT
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00045s latency).
Not shown: 991 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
80/tcp  open  http     nginx
110/tcp open  pop3     Dovecot pop3d
143/tcp open  imap     Dovecot imapd (Ubuntu)
443/tcp open  ssl/http nginx
587/tcp open  smtp     Postfix smtpd
993/tcp open  ssl/imap Dovecot imapd (Ubuntu)
995/tcp open  ssl/pop3 Dovecot pop3d
Service Info: Hosts: -ubuntusrv.netlab.local,  ubuntusrv.netlab.local; OS: Linux; CPE: cpe:/o:li
nux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds
```