CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

Task A: Sword - Network Scanning (20+ 20 = 40 points)

Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

Make sure you didn't add/delete any firewall policy before continuing.

1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.
2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

   The traffic pattern is very erractic coming from the IP address 192.168.217.3. Nmap is doing its job by probing around to see what ports on the victim, Ubuntu or 192.168.10.10, are open. Wireshark on Ubuntu displays this behavior, which appears to be very strange if you are in the position of the victim. A host probing around and trying every port is very troublesome news for the victim. Extra attention is drawn to the communications from the External Kali Attack Machine by the usage of the bright red color that immediately draws one's eyes to it. The communication with External Kali Attack Machine is very aggressive. The observed pattern of highly aggressive and invasive communication by the External Kali Attack Machine is indicative of the dangers one may face with nmap (or Zenmap). Such activites showcase the importance of structurally sound firewalls and the need for constant traffic monitoring as a way to ensure the protection of vital information, data, and other assets. Nmap's actions were intense and seemingly unrelenting. The observed traffic pattern was incredibly unique and provides an incredibly clear view of the impact of network traffic, much is at stake in securing traffic against bad actors worldwide.

Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	**LAN**	**BLOCK**	**192.168.217.3**	**192.168.10.10**	**ICMP**

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)

2	**WAN**	**BLOCK**	**192.168.217.3**	**LAN Net**	**ICMP**

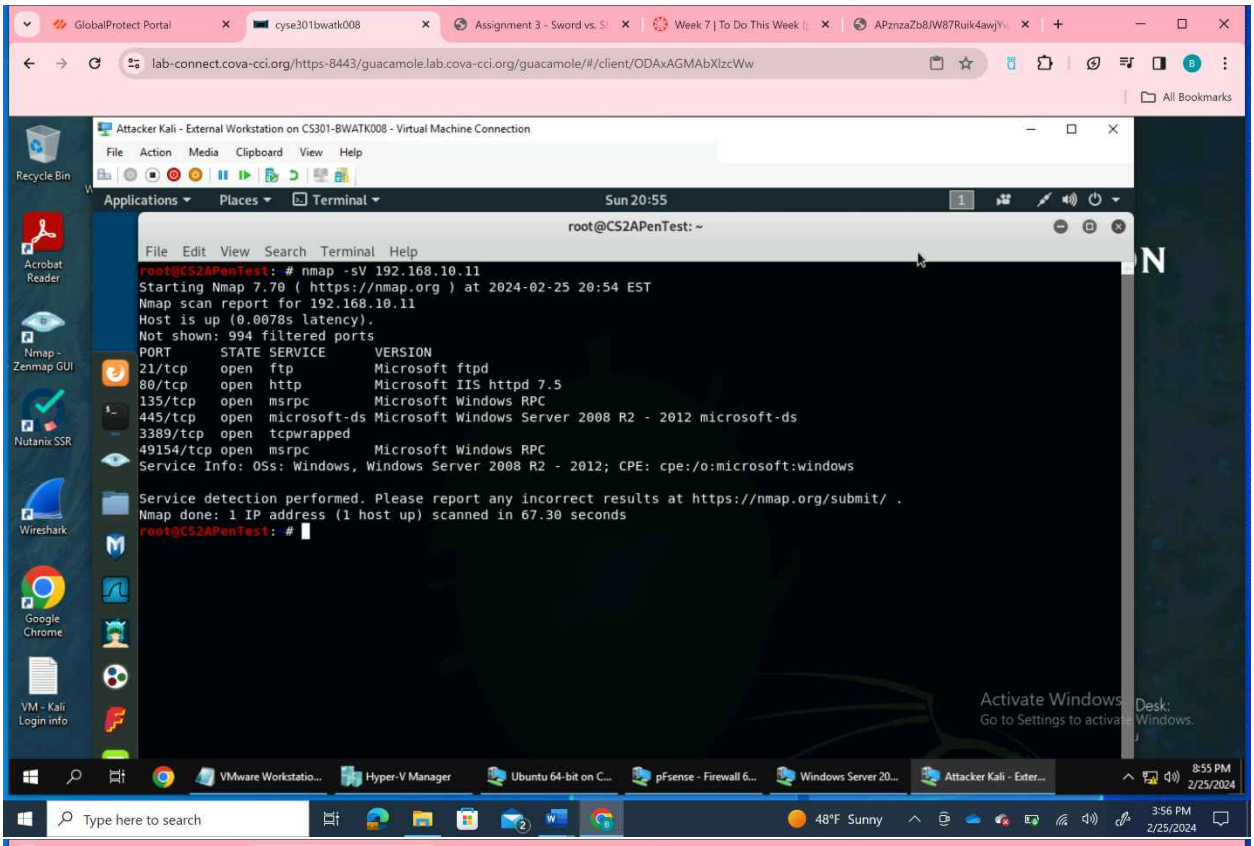
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

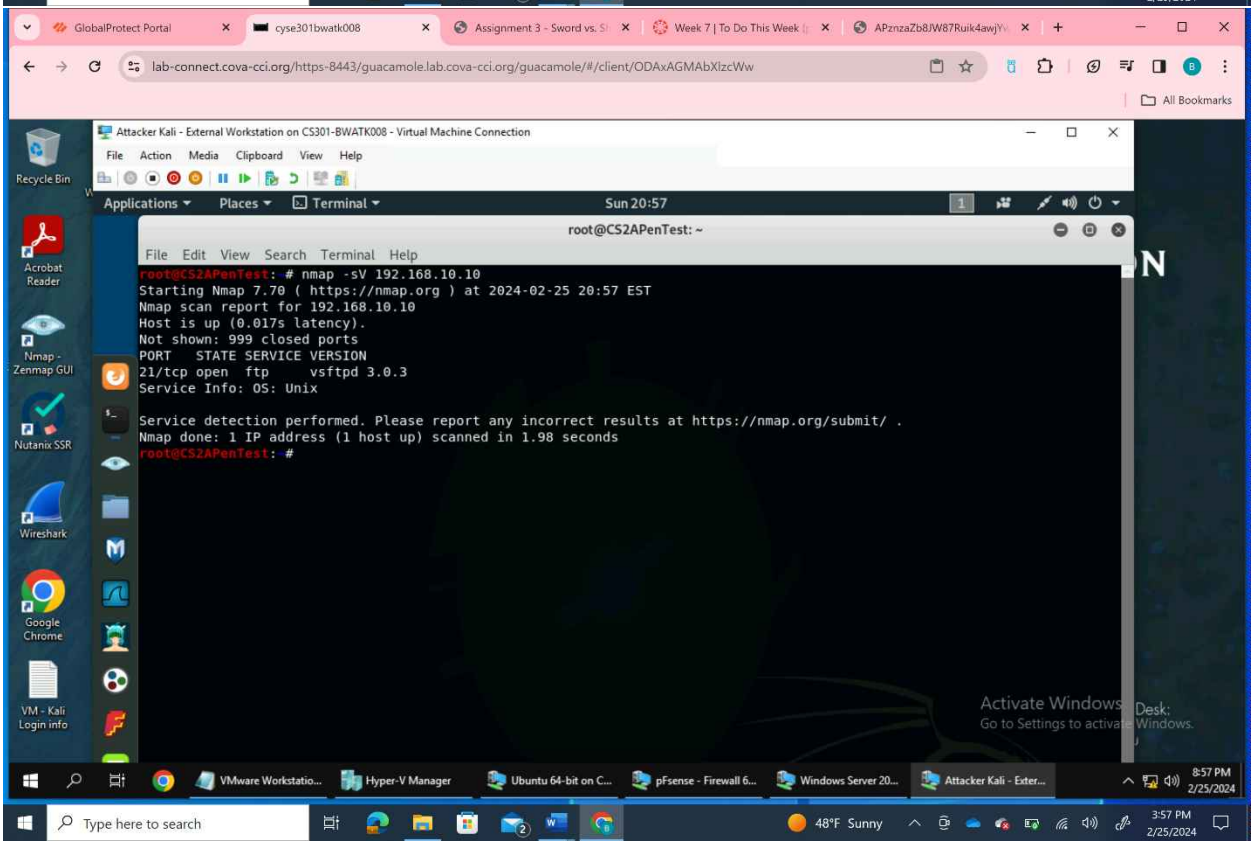
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
3	**WAN**	**ALLOW**	**192.168.217.3**	**192.168.10.11**	**FTP**
4	**WAN**	**BLOCK**	**192.168.217.3**	**LAN Net**	**ANY**

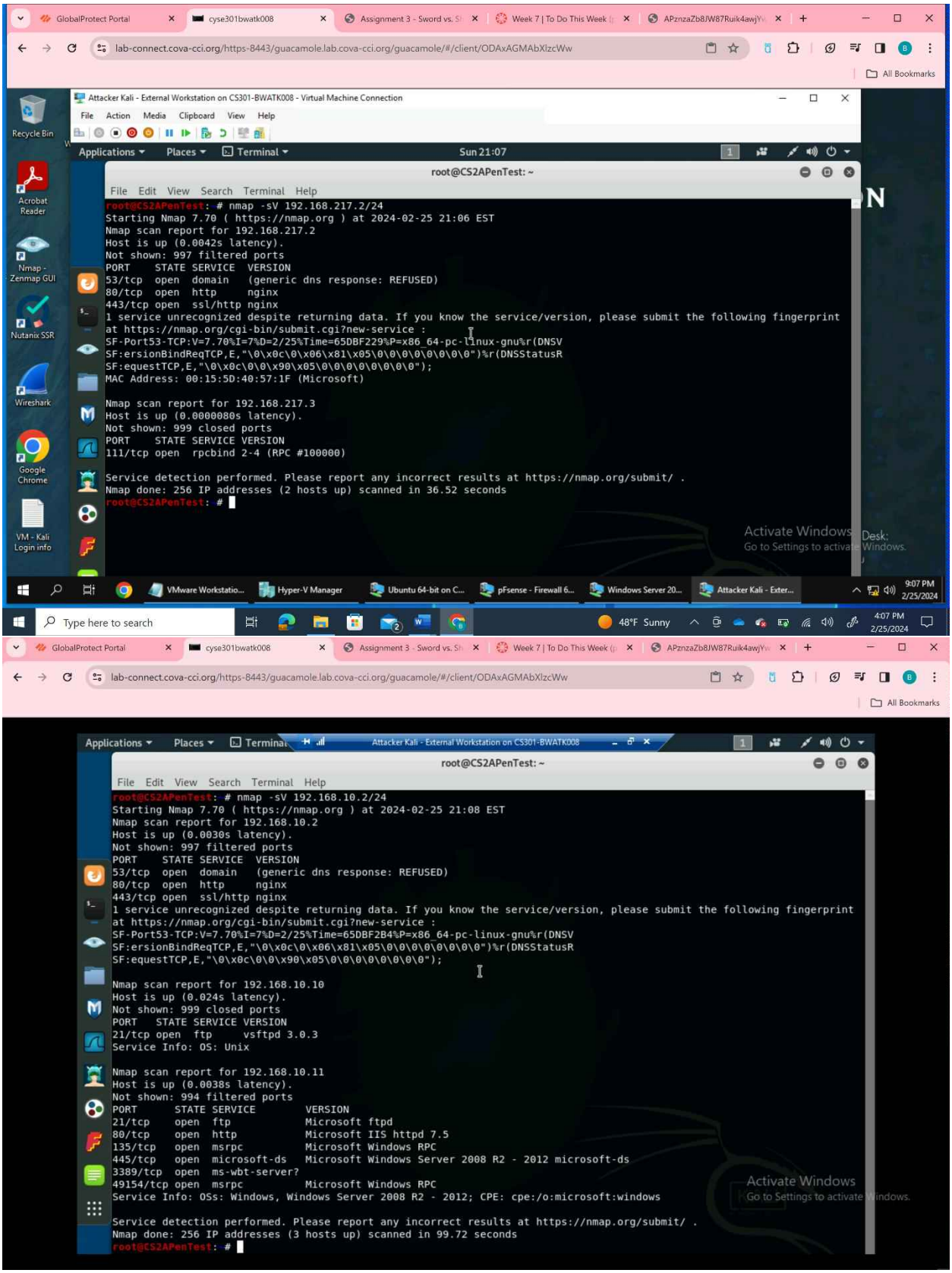
4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

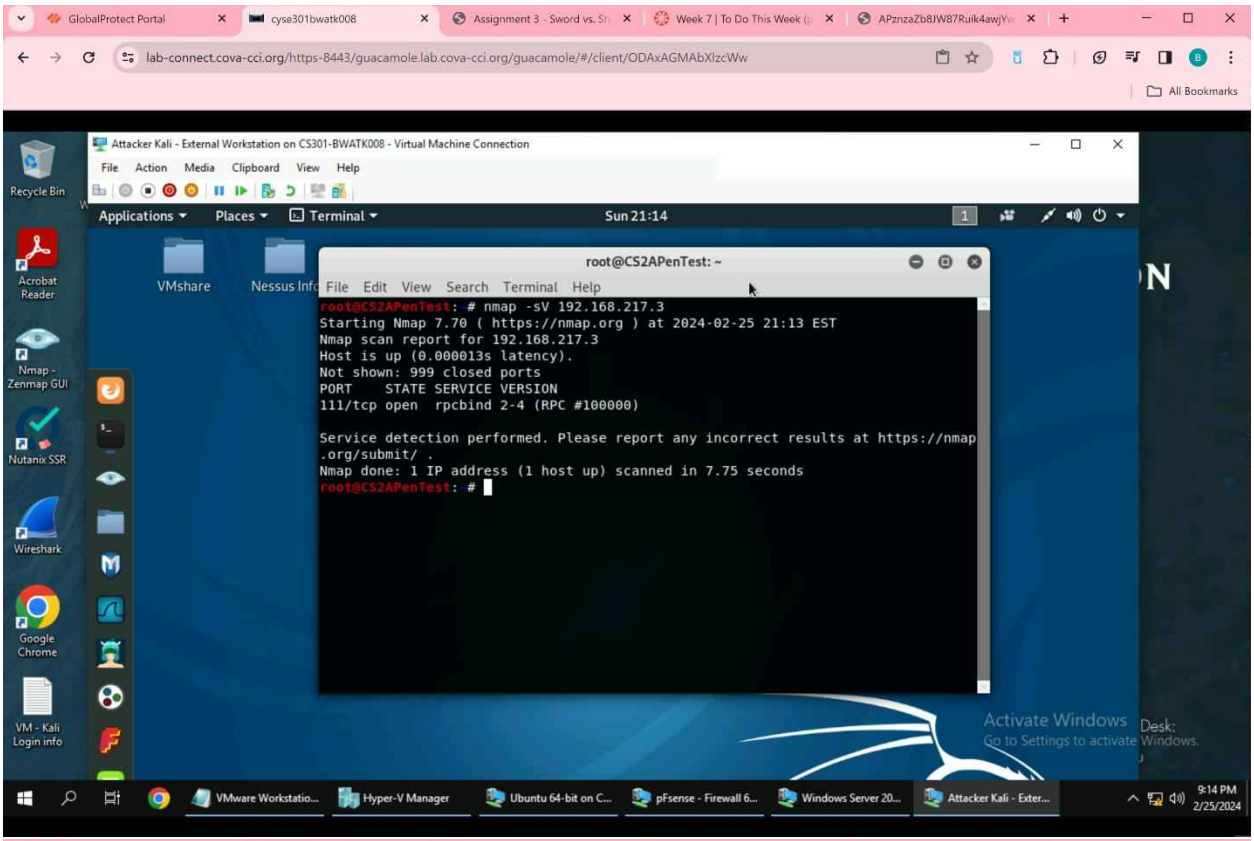
   There is a message that says "Host seems down" and that ping probes are being blocked.

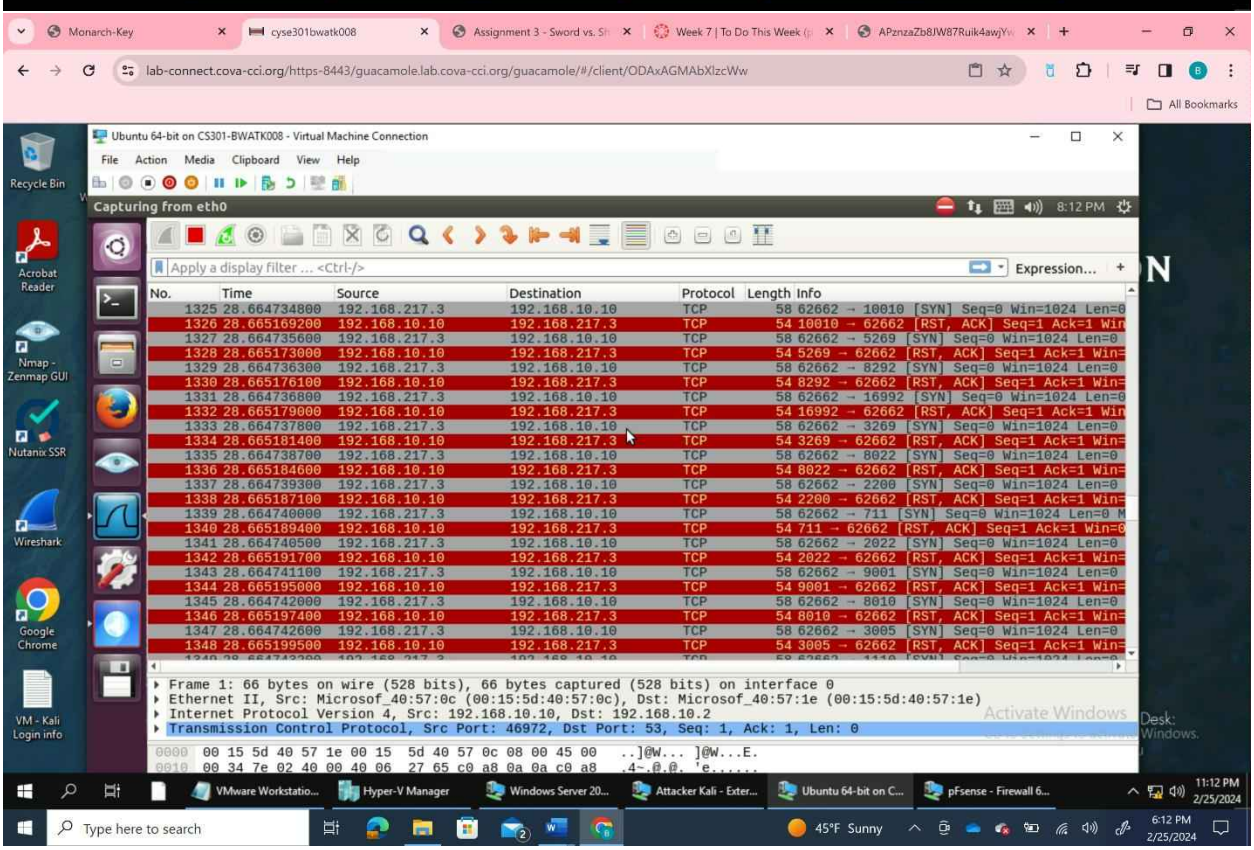
Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.

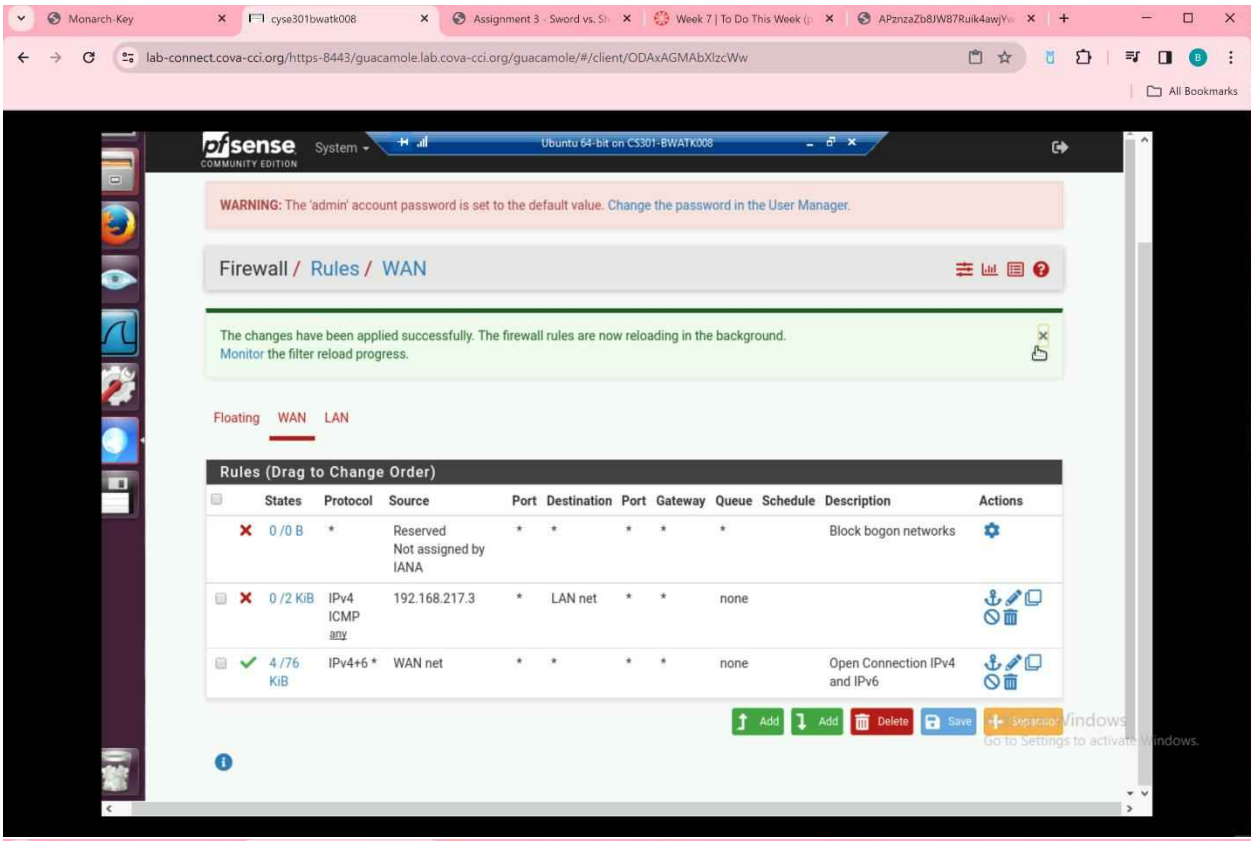

GlobalProtect Portal
cyse301bwatk008
Assignment 3 - Sword vs. S
Week 7 | To Do This Week
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Attacker Kali - External Workstation on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sun 20:55
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap -sV 192.168.10.11
Starting Nmap 7.70 (https://nmap.org) at 2024-02-25 20:54 EST
Nmap scan report for 192.168.10.11
Host is up (0.0078s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 7.5
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open tcpwrapped
49154/tcp open msrpc Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.30 seconds
root@CS2APenTest: #
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
Activate Windows
Go to Settings to activate Windows.
VMware Workstatio...
Hyper-V Manager
Ubuntu 64-bit on C...
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
8:55 PM 2/25/2024
Type here to search
48°F Sunny
3:56 PM 2/25/2024

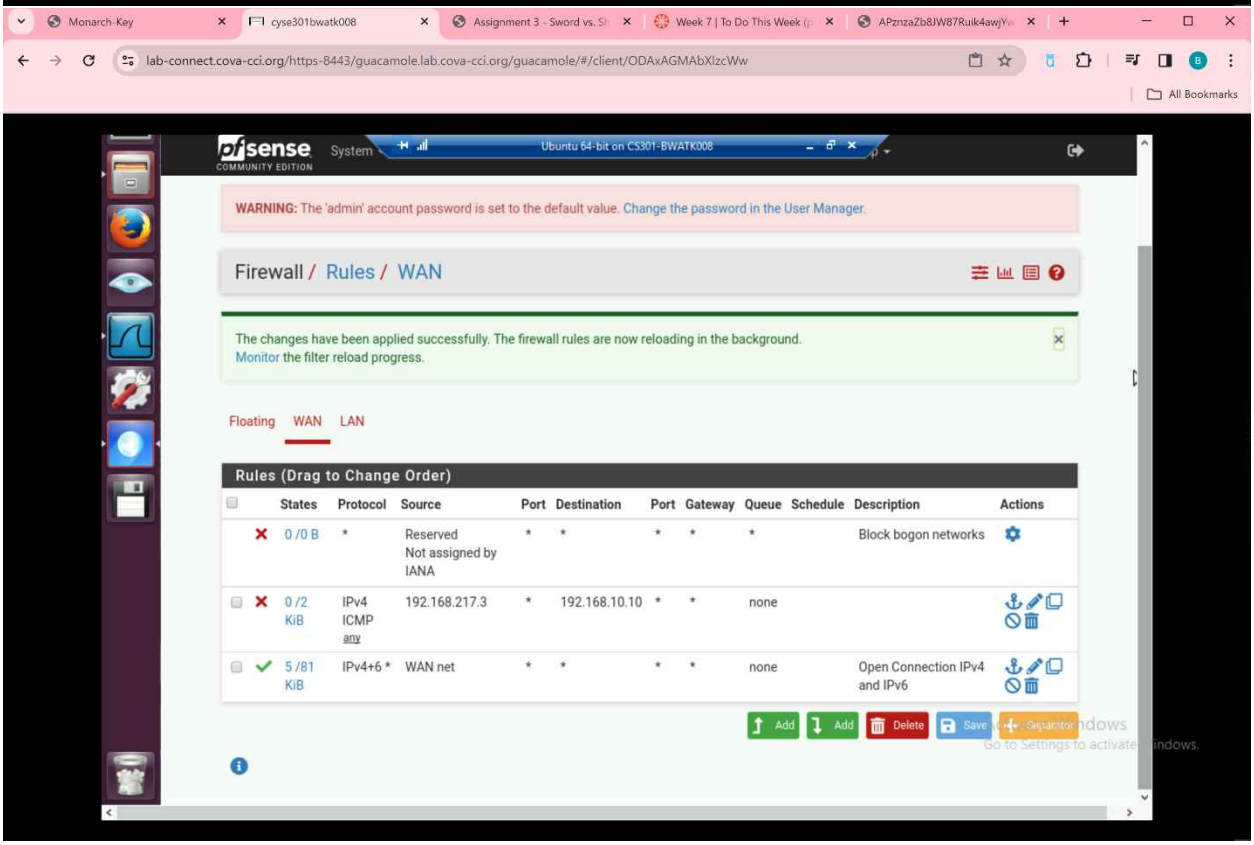

GlobalProtect Portal
cyse301bwatk008
Assignment 3 - Sword vs. S
Week 7 | To Do This Week
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Attacker Kali - External Workstation on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sun 20:57
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap -sV 192.168.10.10
Starting Nmap 7.70 (https://nmap.org) at 2024-02-25 20:57 EST
Nmap scan report for 192.168.10.10
Host is up (0.017s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
root@CS2APenTest: #
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
Activate Windows
Go to Settings to activate Windows.
VMware Workstatio...
Hyper-V Manager
Ubuntu 64-bit on C...
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
8:57 PM 2/25/2024
Type here to search
48°F Sunny
3:57 PM 2/25/2024

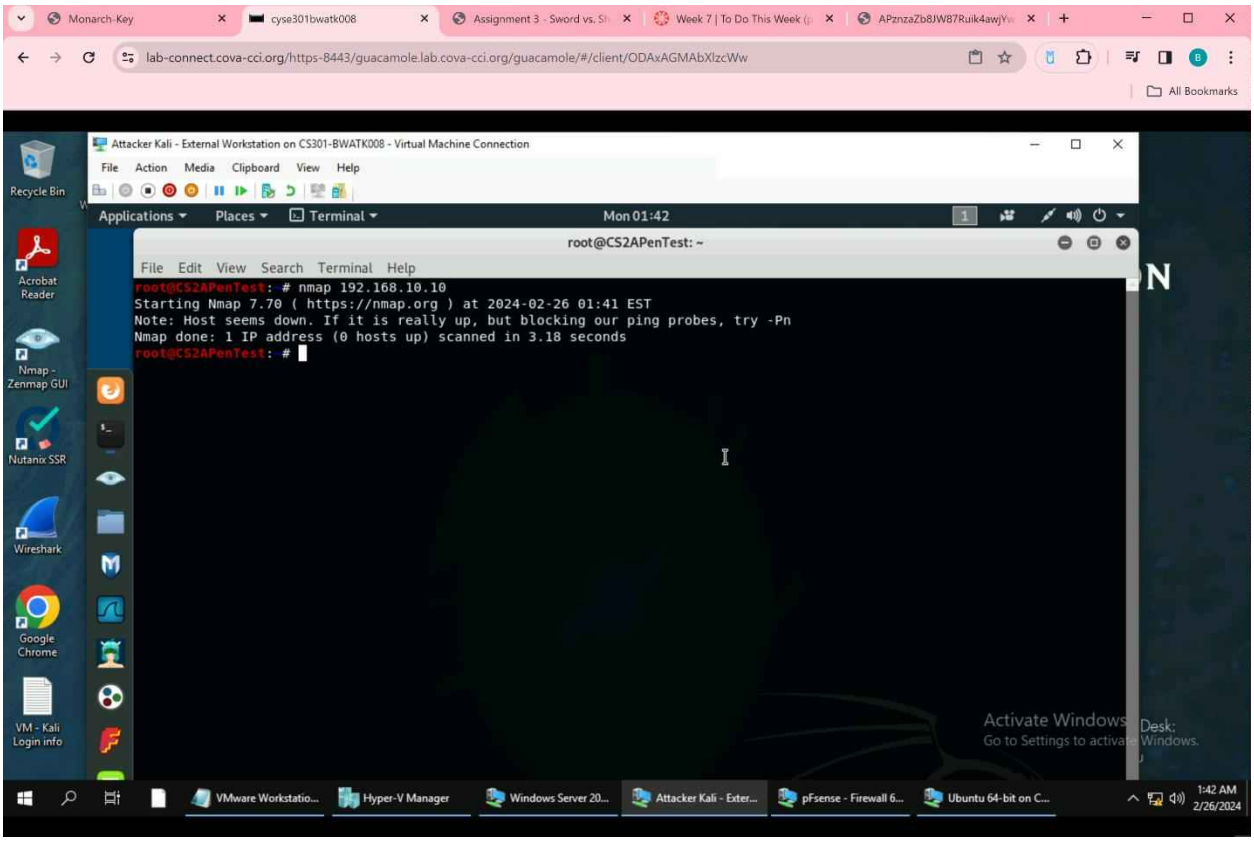

GlobalProtect Portal
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Attacker Kali - External Workstation on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sun 21:07
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap -sV 192.168.217.2/24
Starting Nmap 7.70 (https://nmap.org) at 2024-02-25 21:06 EST
Nmap scan report for 192.168.217.2
Host is up (0.0042s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
80/tcp open http nginx
443/tcp open ssl/http nginx
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=2/25%Time=65DBF229%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0")%r(DNSStatusR
SF:equestTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0");
MAC Address: 00:15:5D:40:57:1F (Microsoft)
Nmap scan report for 192.168.217.3
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
111/tcp open rpcbind 2-4 (RPC #100000)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 36.52 seconds
root@CS2APenTest: #
Activate Windows
Go to Settings to activate Windows.
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
VMware Workstatio...
Hyper-V Manager
Ubuntu 64-bit on C...
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
9:07 PM
2/25/2024
Type here to search
48°F Sunny
4:07 PM
2/25/2024
GlobalProtect Portal
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Applications Places Terminal
Attacker Kali - External Workstation on CS301-BWATK008
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap -sV 192.168.10.2/24
Starting Nmap 7.70 (https://nmap.org) at 2024-02-25 21:08 EST
Nmap scan report for 192.168.10.2
Host is up (0.0030s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
80/tcp open http nginx
443/tcp open ssl/http nginx
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=2/25%Time=65DBF2B4%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0")%r(DNSStatusR
SF:equestTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0");
Nmap scan report for 192.168.10.10
Host is up (0.024s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
Service Info: OS: Unix
Nmap scan report for 192.168.10.11
Host is up (0.0038s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 7.5
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server?
49154/tcp open msrpc Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 99.72 seconds
root@CS2APenTest: #
Activate Windows
Go to Settings to activate Windows.


GlobalProtect Portal
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week (p
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Attacker Kali - External Workstation on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sun 21:14
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap -sV 192.168.217.3
Starting Nmap 7.70 (https://nmap.org) at 2024-02-25 21:13 EST
Nmap scan report for 192.168.217.3
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
111/tcp open rpcbind 2-4 (RPC #100000)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.75 seconds
root@CS2APenTest: #
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
VMshare
Nessus Info
Activate Windows
Go to Settings to activate Windows.
VMware Workstatio...
Hyper-V Manager
Ubuntu 64-bit on C...
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
9:14 PM
2/25/2024


Monarch-Key
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week (p
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Ubuntu 64-bit on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Capturing from eth0
8:12 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1325 28.664734800 192.168.217.3 192.168.10.10 TCP 58 62662 → 10010 [SYN] Seq=0 Win=1024 Len=0
1326 28.665169200 192.168.10.10 192.168.217.3 TCP 54 10010 → 62662 [RST, ACK] Seq=1 Ack=1 Win
1327 28.664735600 192.168.217.3 192.168.10.10 TCP 58 62662 → 5269 [SYN] Seq=0 Win=1024 Len=0
1328 28.665173000 192.168.10.10 192.168.217.3 TCP 54 5269 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1329 28.664736300 192.168.217.3 192.168.10.10 TCP 58 62662 → 8292 [SYN] Seq=0 Win=1024 Len=0
1330 28.665176100 192.168.10.10 192.168.217.3 TCP 54 8292 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1331 28.664736800 192.168.217.3 192.168.10.10 TCP 58 62662 → 16992 [SYN] Seq=0 Win=1024 Len=0
1332 28.665179000 192.168.10.10 192.168.217.3 TCP 54 16992 → 62662 [RST, ACK] Seq=1 Ack=1 Win
1333 28.664737800 192.168.217.3 192.168.10.10 TCP 58 62662 → 3269 [SYN] Seq=0 Win=1024 Len=0
1334 28.665181400 192.168.10.10 192.168.217.3 TCP 54 3269 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1335 28.664738700 192.168.217.3 192.168.10.10 TCP 58 62662 → 8022 [SYN] Seq=0 Win=1024 Len=0
1336 28.665184600 192.168.10.10 192.168.217.3 TCP 54 8022 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1337 28.664739300 192.168.217.3 192.168.10.10 TCP 58 62662 → 2200 [SYN] Seq=0 Win=1024 Len=0
1338 28.665187100 192.168.10.10 192.168.217.3 TCP 54 2200 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1339 28.664740000 192.168.217.3 192.168.10.10 TCP 58 62662 → 711 [SYN] Seq=0 Win=1024 Len=0 M
1340 28.665189400 192.168.10.10 192.168.217.3 TCP 54 711 → 62662 [RST, ACK] Seq=1 Ack=1 Win=0
1341 28.664740500 192.168.217.3 192.168.10.10 TCP 58 62662 → 2022 [SYN] Seq=0 Win=1024 Len=0
1342 28.665191700 192.168.10.10 192.168.217.3 TCP 54 2022 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1343 28.664741100 192.168.217.3 192.168.10.10 TCP 58 62662 → 9001 [SYN] Seq=0 Win=1024 Len=0
1344 28.665195000 192.168.10.10 192.168.217.3 TCP 54 9001 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1345 28.664742000 192.168.217.3 192.168.10.10 TCP 58 62662 → 8010 [SYN] Seq=0 Win=1024 Len=0
1346 28.665197400 192.168.10.10 192.168.217.3 TCP 54 8010 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
1347 28.664742600 192.168.217.3 192.168.10.10 TCP 58 62662 → 3005 [SYN] Seq=0 Win=1024 Len=0
1348 28.665199500 192.168.10.10 192.168.217.3 TCP 54 3005 → 62662 [RST, ACK] Seq=1 Ack=1 Win=
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2
Transmission Control Protocol, Src Port: 46972, Dst Port: 53, Seq: 1, Ack: 1, Len: 0
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 ..]@W...]@W...E.
0010 00 34 7e 02 40 00 40 06 27 65 c0 a8 0a 0a c0 a8 .4~.@.@. 'e.....
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
Activate Windows
Go to Settings to activate Windows.
VMware Workstatio...
Hyper-V Manager
Windows Server 20...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
pFsense - Firewall 6...
11:12 PM
2/25/2024
Type here to search
45°F Sunny
6:12 PM
2/25/2024


Monarch-Key
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week (p
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
pfsense
COMMUNITY EDITION
System
Ubuntu 64-bit on CS301-BWATK008
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0 /0 B
*
Reserved
Not assigned by
IANA
Block bogon networks
0 /2 KiB
IPv4
ICMP
any
192.168.217.3
LAN net
none
4 /76
KiB
IPv4+6 *
WAN net
Open Connection IPv4
and IPv6
Add
Delete
Save
Separator


Monarch-Key
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week (p
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
pfsense
COMMUNITY EDITION
System
Ubuntu 64-bit on CS301-BWATK008
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0 /0 B
*
Reserved
Not assigned by
IANA
Block bogon networks
0 /2
KiB
IPv4
ICMP
any
192.168.217.3
192.168.10.10
none
5 /81
KiB
IPv4+6 *
WAN net
Open Connection IPv4
and IPv6
Add
Delete
Save
Separator


Monarch-Key
cyse301bwatk008
Assignment 3 - Sword vs. Sh
Week 7 | To Do This Week (p
APznzaZb8JW87Ruik4awjYw
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/ODAxAGMAbXlzcWw
All Bookmarks
Attacker Kali - External Workstation on CS301-BWATK008 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 01:42
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # nmap 192.168.10.10
Starting Nmap 7.70 (https://nmap.org) at 2024-02-26 01:41 EST
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 3.18 seconds
root@CS2APenTest: #
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
Activate Windows
Go to Settings to activate Windows.
VMware Workstatio...
Hyper-V Manager
Windows Server 20...
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
1:42 AM
2/26/2024