## OLD DOMINION UNIVERSITY CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

## ASSIGNMENT #3- SWORD AND SHIELD

JEGGO PAOLO V. DYCOK 01242866 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.



## **PROCEDURE:**

- I entered the command "nmap -sV 192.168.10.2/24" to get a scan of the topology within the subnet.
- 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.

|              |   |   | Obuniu 04-bit   | on CY301-JDYCO001   | >  |  | 😑 tı 🕅  | ◄)) 5:45 AM ()  |        |
|--------------|---|---|---|---|--|--|---|---|--------|
| O)           |   | 📮 🗋 🖹 🧕 🗬   | < > > 1+ -+   |   | ) 🛯 🎹  |  |   |   |        |
|              | Apply a display fil   | lter <ctrl-></ctrl->  |   |   |  |  | •   | Expression +  |        |
| <u>&gt;-</u> | 28 8.254579800<br>29 9.337713600<br>30 9.337761800  | Source<br>192.168.10.10<br>192.168.217.3<br>192.168.10.10   | Destination<br>192.168.10.2<br>192.168.10.10<br>192.168.217.3   | DNS<br>TCP<br>TCP   | Length Info<br>74 Standard q<br>58 54519 → 44<br>54 443 → 5451   | uery Oxcbd9<br>3 [SYN] Seq=<br>9 [RST, ACK]  | A ntp.ubur<br>0 Win=1024<br>Seq=1 Ack   | ntu.com<br>4 Len=0 MS<br>k=1 Win=0  |        |
|              | 31 9.337717500<br>32 9.337770900<br>33 9.337717900<br>34 9.337774400  | 192.168.217.3<br>192.168.10.10<br>192.168.217.3<br>192.168.10.10  | 192.168.10.10<br>192.168.217.3<br>192.168.10.10<br>192.168.217.3  | ICMP<br>ICMP<br>ICMP<br>ICMP  | 42 Echo (ping<br>42 Echo (ping<br>54 Timestamp<br>54 Timestamp   | ) request i<br>) reply i<br>request i<br>reply i   | d=0xcc84,<br>d=0xcc84,<br>d=0xaee5,<br>d=0xaee5   | seq=0/0,<br>seq=0/0,<br>seq=0/0,<br>seq=0/0   |        |
|              | 35 13.499452800<br>36 18.749855300<br>37 18.750644500   | 192.168.10.10<br>192.168.10.10<br>192.168.10.2  | 192.168.10.2<br>192.168.10.2<br>192.168.10.10   | DNS<br>TCP<br>TCP   | 74 Standard q<br>74 34108 → 53<br>74 53 → 34108  | Uery Oxcbd9<br>[SYN] Seq=0<br>[SYN, ACK]   | A ntp.ubur<br>Win=29200<br>Seq=0 Ack=   | D Len=0 MS  |        |
|              | 38 18.750665400<br>Total Lengt  | h: 60   | 192.168.10.2  | TCP   | 66 34108 → 53  | [ACK] Seq=1  | Ack=1 Wir   | 1=29312 Le  | r<br>• |
|              | <ul> <li>Flags: 0x02</li> <li>Fragment of</li> <li>Time to liv</li> </ul>   | (Don't Fragment)<br>fset: 0<br>e: 64  |   |   |  |  |   | _   | r.     |
| 2            | Protocol: U<br>Header chec<br>[Header che<br>Source: 192  | DP (17)<br>ksum: 0xedca [valid<br>cksum status: Unver<br>.168.10.10   | ation disabled]<br>ified]   |   |  |  |   |   |        |
| Ŀ            | Destination<br>[Source Geo<br>[Destinatio   | : 192.168.10.2<br>IP: Unknown]<br>n GeoIP: Unknown]<br>Protocol Src Port  | · 36089 Dst Port - 5  | 3   |  |  |   |   |        |
|              | 0000 00 15 5d<br>0010 00 3c b7  | 40 57 1e 00 15 5d<br>89 40 00 40 11 ed  | 40 57 0c 08 00 45 00<br>ca c0 a8 0a 0a c0 a8  | ]@W]@<br>.<@.@  | WE.  |  |   |   |        |
|              | 0030 00 00 00<br>0040 75 03 63  | 00 00 00 03 6e 74<br>6f 6d 00 00 01 00  | 70 06 75 62 75 6e 74<br>01  | n tp<br>u.com   | ubunt  |  |   |   |        |
|              |   |   |   |   |  |  |   |   |        |
|              |   |   |   |   |  |  |   |   |        |
|              |   |   |   |   |  |  |   |   |        |
|              | ○ 2 wireshark_e   | eth0_20230303053852_G   | N9rav   |   | Packets: 23  | 62 · Displayed: 2  | 362 (100.0%)  | ) Profile: Default  | t .    |
|              |   |   |   |   |  |  |   |   |        |
| *eth0        |   | lh. 🔫   | Ubuntu 64-bit o   | n CY301-JDYCO001  | ×  | / _  | ) tı 📖 i  | U)) 5:46.AM <b>₹¹</b> ⊁   |        |
|              |   | Q 🖏 🕅   | < > 3  - 4  📃   |   | A #  |  |   | ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~  | N      |
|              |   |   |   |   |  |  |   |   |        |
|              | Apply a display filte   | er <ctrl-></ctrl->  |   |   |  |  | <b>•</b> • E:   | xpression 🖟   |        |
|              | Apply a display filto<br>Time<br>61 22.448637500<br>62 22.448637500   | er <ctrl-></ctrl-> Source 192.168.217.3 192.168.10.10 122.168.217.2   | Destination<br>192.168.10.10<br>192.168.217.3   | Protocol Le<br>TCP<br>TCP   | ength Info<br>58 54775 → 53<br>54 53 → 54775<br>58 54775 → 22  | [SYN] Seq=0  <br>[RST, ACK] S  | E<br>Win=1024 L<br>eq=1 Ack=1   | xpression   |        |
|              | Apply a display filt<br>Time<br>61 22.44848400<br>62 22.448637500<br>63 22.448637500<br>64 22.4486490500<br>65 22.4486490500<br>66 22.448673300   | er <ctrl-></ctrl-> Source 192.168.217.3 192.168.10.10 192.168.217.3 192.168.10.10 192.168.10.10 192.168.10.10   | Destination<br>192.168.10.10<br>192.168.217.3<br>192.168.10.10<br>192.168.10.10<br>192.168.10.10<br>192.168.217.3   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP                      |  | [SYN] Seq=0'<br>[RST, ACK] S<br>[SYN] Seq=0'<br>[SYN] Seq=0'<br>[SYN] Seq=0'<br>[SYN, ACK] S   | Win=1024 L<br>eq=1 Ack=1<br>Win=1024 L<br>eq=1 Ack=1<br>Win=1024 L<br>eq=0 Ack=1  | xpression<br>en=0 MSS<br>Win=0 L<br>en=0 MSS<br>Win=0 L<br>en=0 MSS<br>i Win=292  |        |
|              | Apply a display filt           Time           61 22.448637500           63 22.448637500           63 22.448637500           64 22.448637600           65 22.448637300           66 22.448673300           67 22.44863300           68 22.44863300           67 22.44863800           67 22.44863800           67 22.44863800           69 22.44863800           69 22.44863800           69 22.44863800   | er <ctrl-></ctrl-> Source 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.10.10 192.168.10.10   | Destination<br>192,168,10,10<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,10,10  | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ength Info<br>58 54775 - 53<br>58 54775 - 22<br>58 54775 - 22<br>58 54775 - 22<br>58 54775 - 21<br>58 21 - 54775<br>58 54775 - 590<br>54 1723 - 5477<br>58 54775 - 590<br>54 5909 - 5477   | [SYN] Seq=0'<br>[RST, ACK] S<br>[SYN] Seq=0'<br>[SYN] Seq=0'<br>[SYN, ACK] S<br>[SYN] Seq=<br>5 [RST, ACK]<br>9 [SYN] Seq=<br>5 [RST, ACK]   |   | xpression<br>win=0 L.<br>win=0 L.<br>w  |        |
|              | Apply a display filt           Time           61 22, 448488408           62 22, 448687560           63 22, 44868760           63 22, 44869760           63 22, 44869760           65 22, 44849760           65 22, 448495800           67 22, 448695800           67 22, 448495800           70 22, 448495800           71 22, 448495800  | er <ctrl-></ctrl-> Source 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3 192.168.217.3   | Destination<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 217, 3   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ngth Info<br>58 5475 - 53<br>54 56 - 54775<br>58 54775 - 22<br>54 22 - 54775<br>58 54775 - 22<br>58 54775 - 12<br>58 54775 - 12<br>58 54775 - 12<br>58 54775 - 5990<br>58 54775 - 5990<br>58 54775 - 113   | [SYN] Seq=0<br>[RST, ACK] S<br>[SYN] Seq=0<br>[SYN] Seq=0<br>[SYN, ACK] S<br>[STN, ACK] S<br>[STN, ACK]<br>5 [RST, ACK]<br>5 [RST, ACK]<br>5 [RST, ACK]<br>[SYN] Seq=0   | Win=1024 L<br>eq=1 Ack=1<br>Win=1024 L<br>eq=1 Ack=1<br>Win=1024 L<br>eq=0 Ack=1<br>0 Win=1024<br>Seq=1 Ack<br>Seq=1 Ack<br>Seq=1 Ack<br>Win=1024   | xpression<br>en=0 MSS<br>win=0 L<br>en=0 MSS<br>win=0 L<br>uin=202<br>Len=0 MS<br>Len=0 MS<br>Len=0 MS<br>Len=0 MS<br>Len=0 MS  |        |
|              | ■   Apply a display filt           Time           61 22.448489760           62 22.44848760           63 22.44848760           65 22.44849760           65 22.44849760           65 22.44849760           65 22.44849760           65 22.44849760           65 22.44849760           67 22.44849760           67 22.4484910           67 22.4484910           67 22.4484910           67 22.4484910           67 22.4484910           67 22.4484910           67 22.4484910           67 22.4484910           67 21.410   | er <ctrl-><br/>Source<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3</ctrl-> | Destination<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 10, 10<br>192, 168, 10, 10   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ngth Info<br>56 64775 53<br>54 53 - 54775<br>58 54775 22<br>54 22 54775<br>58 54775 21<br>58 54775 21<br>58 54775 172<br>54 1723 54775<br>58 54775 590<br>54 5900 5477<br>58 54775 113   | [SYN] Seq=0<br>[RST, ACK] S<br>[SYN] Seq=0<br>[RST, ACK] S<br>[SYN] Seq=0<br>[SYN, ACK] S<br>[SYN] Seq=<br>5 [RST, ACK]<br>[SYN] Seq=<br>5 [RST, ACK]<br>[SYN] Seq=0   | E • E:<br>Win=1024 L<br>eq=1 Ack=1<br>eq=1 Ack=1<br>eq=0 Ack=1<br>0 Win=1024 L<br>Seq=1 Ack<br>0 Win=1024 L<br>Seq=1 Ack<br>Win=1024  | xpression<br>ken=0 MSS<br>vin=0 L<br>vin=0 L<br>vin=0 L<br>vin=0 MSS<br>vin=0 L<br>vin=0 MS<br>vin=0 L<br>vin=0 MS<br>vin=0 L<br>vin=0 MS<br>vin=0 L<br>vin=0 L |        |
|              | ▲ Apply a display filt           Time           61 22, 448488400           62 22, 448667590           63 22, 44869780           63 22, 44869780           65 22, 44849780           65 22, 44849780           65 22, 44869300           65 22, 44869300           67 22, 44869300           67 22, 44869300           71 22, 44869300           71 22, 44869300           71 22, 448495800           71 70tal Length           Total Length           Fragment off           Fragment off           Time to live           Protocol: TC           Header check           (Header check  | er <ctrl-></ctrl-> Source J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 J92.166.217.3 :40 on: 0xe14d (57677) (Don't Fragment) set: 0 :64 P (6) sum: 0xf523 [valida Kum status: Unveri   | Destination<br>132.168.10.10<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.10.10<br>132.166.10.10<br>132.166.10.10<br>132.166.10.10   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>start<br>st | [SYN] Seq=0 (<br>[RST, ACK] S<br>[SYN] Seq=0 (<br>[RST, ACK] S<br>[SYN] Seq=0 (<br>[SYN, SCq=0 (<br>[SYN, SCq=0 (<br>[SYN] Seq=0 (<br>[SYN                                 | <pre>Win=1024 L<br/>got=1 Ack=1<br/>win=1024 L<br/>got=1 Ack=1<br/>win=1024 L<br/>got=0 Ack=1<br/>0 Win=1024<br/>Seq=1 Ack<br/>0 Win=1024<br/>Win=1024</pre>                              | xpression A<br>en=0 MSS<br>win=0 L<br>en=0 MSS<br>win=0 L<br>len=0 MS<br>len=0 MS<br>len=0 MS<br>len=0 MS<br>len=0 MS<br>len=0 MS   |        |
|              | ▲ Apply a display filt           Time           61 22 .448483408           62 22 .448487500           63 22 .44849708           63 22 .44849708           65 22 .44849708           65 22 .44849708           65 22 .448495808           65 22 .448495808           65 22 .448495808           65 22 .448495808           65 22 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           71 .22 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .2 .448495808           72 .448495808           72 .448495808           72 .448495808           72 .448495808           72 .448495808           72 .448495808 </td <td>er<ctrl-><br/>Source<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>: 49<br/>on: 0xe14d (57677)<br/>(0on't Fragment)<br/>set: 0<br/>: 64<br/>P (6)<br/>192.168.217.3<br/>: 104<br/>sum: 0xf523 [valida<br/>ksum status: Unveri<br/>168.10.10<br/>192.168.217.3<br/>: Unknown]<br/>192.168.217.3</ctrl-></td> <td>Destination<br/>192, 168, 10, 10<br/>192, 168, 217, 3<br/>192, 168, 216, 217, 3<br/>192, 168, 216, 10<br/>192, 168, 217, 3<br/>192, 168, 10, 10</td> <td>Protocol Le<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP<br/>TCP</td> <td>ength Info<br/>58 54775 → 53<br/>54 53 → 54775<br/>58 54775 → 253<br/>58 54775 → 225<br/>58 54775 → 215<br/>58 54775 → 172<br/>58 54775 → 173<br/>54 1223 → 54775<br/>54 54775 → 54775<br/>58 54775 → 113</td> <td>[SYN] Seq=0<br/>(RST, ACK) S<br/>(SYN) Seq=0<br/>(RST, ACK) S<br/>(SYN) Seq=0<br/>(SYN) Seq=0<br/>5 (RST, ACK)<br/>3 (SYN) Seq=0<br/>5 (RST, ACK)<br/>5 (RST, ACK)<br/>5 (RST, ACK)</td> <td><pre>win=1024 t eq=1 Ack=1 win=1024 t eq=1 Ack=1 win=1024 t eq=1 Ack=1 o win=1024 t eq=0 Ack=1 o win=1024 o win=1024 o win=1024 win=1024</pre></td> <td>xpression<br/>xpression<br/>xvin=0 MSS<br/>vin=0 MSS<br/>vin=0 MSS<br/>Len=0 MSS<br/>Len=0 MS<br/>Len=0 MS<br/>vin=0 Len=0 MS vin=0 Len=0 MS<br/>vin=0 Len=0 MS</td> <td></td> | er <ctrl-><br/>Source<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>: 49<br/>on: 0xe14d (57677)<br/>(0on't Fragment)<br/>set: 0<br/>: 64<br/>P (6)<br/>192.168.217.3<br/>: 104<br/>sum: 0xf523 [valida<br/>ksum status: Unveri<br/>168.10.10<br/>192.168.217.3<br/>: Unknown]<br/>192.168.217.3</ctrl->   | Destination<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 216, 217, 3<br>192, 168, 216, 10<br>192, 168, 217, 3<br>192, 168, 10, 10   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ength Info<br>58 54775 → 53<br>54 53 → 54775<br>58 54775 → 253<br>58 54775 → 225<br>58 54775 → 215<br>58 54775 → 172<br>58 54775 → 173<br>54 1223 → 54775<br>54 54775 → 54775<br>58 54775 → 113  | [SYN] Seq=0<br>(RST, ACK) S<br>(SYN) Seq=0<br>(RST, ACK) S<br>(SYN) Seq=0<br>(SYN) Seq=0<br>5 (RST, ACK)<br>3 (SYN) Seq=0<br>5 (RST, ACK)<br>5 (RST, ACK)<br>5 (RST, ACK)  | <pre>win=1024 t eq=1 Ack=1 win=1024 t eq=1 Ack=1 win=1024 t eq=1 Ack=1 o win=1024 t eq=0 Ack=1 o win=1024 o win=1024 o win=1024 win=1024</pre>  | xpression<br>xpression<br>xvin=0 MSS<br>vin=0 MSS<br>vin=0 MSS<br>Len=0 MSS<br>Len=0 MS<br>Len=0 MS<br>vin=0 Len=0 MS vin=0 Len=0 MS<br>vin=0 Len=0 MS  |        |
|              | ■ Apply a display filt           Time           61 22, 448483408           62 22, 448637560           63 22, 448654808           64 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           65 22, 448654808           71 22, 4484954808           71 22, 4484954808           71 22, 4484954808           71 Total Length           Identificati           Fragment off           Time to live           Protocol; TC           Header check           Source: 192.           Destination:           [Source Geol]           [Destination]           [Destination]           [Source Geol]           [Destination]           [Beader check           Source Geol           [Destination]           [Source Geol]           [Destination]           [Beader check           [Beader check           [Beader check           [Beader check           [Beader check  | er <ctrl-><br/>Source<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.167.257.257.257.257.257.257.257.257.257.25</ctrl->  | Destination<br>192, 168, 10, 10<br>192, 168, 10, 10<br>192, 168, 10, 10<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 217, 3<br>192, 168, 217, 3<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 10, 10<br>192, 100<br>192, 100   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ength Info<br>58 54775 53<br>54 53 - 54775<br>58 54775 22<br>58 54775 22<br>58 54775 21<br>58 54775 172<br>54 1723 54775<br>54 1723 54775<br>54 3723 54775<br>54 54775 5173<br>54 54775 113<br>1, Ack: 1, Len:<br>,E.  | [SYN] Seq=0 (<br>[RST, ACK] S<br>[SYN] Seq=0 (<br>[RST, ACK] S<br>[SYN] Seq=0 (<br>[SYN, ACK] S<br>[SYN] Seq=0 (<br>[SYN]                                 | <pre>win=1024 L<br/>eq=1 Ack=1<br/>win=1024 L<br/>eq=1 Ack=1<br/>win=1024 L<br/>eq=0 Ack=1<br/>0 Win=1024<br/>0 Win=1024<br/>0 Win=1024<br/>0 Win=1024</pre>                              | xpression A<br>en=0 MSS<br>win=0 L<br>en=0 MSS<br>Len=0 MSS<br>Len=0 MS<br>Len=0 MS<br>Len=0 MS<br>P  |        |
|              | ▲ Apply a display filt           Time           61 22, 448667560           62 22, 448667560           63 22, 44867300           65 22, 44869780           65 22, 44869780           65 22, 44869780           65 22, 44869780           65 22, 44869780           65 22, 44869300           67 22, 44869300           67 22, 44869300           72 2, 44869300           72 2, 44869300           72 2, 44869300           72 2, 44869300           72 2, 448495800           71 20, 448495800  | er <ctrl-><br/>Source<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>192.168.217.3<br/>F. Unknown]<br/>Set: 0<br/>564<br/>P (6)<br/>922.168.217.3<br/>P: Unknown]<br/>Set: 0<br/>571 e 00 15 54 4<br/>04 40 e 04 66 f52 2<br/>5 d5 f7 e 08 e0 e0 e0</ctrl->  | Destination<br>132.168.10.10<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.166.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.217.3<br>132.165.  | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | section of the sectio   | [SYN] Seq=0 (<br>[RST, ACK] S<br>[SYN] Seq=0 (<br>[SYN, ACK] S<br>[SYN] Seq=0 (<br>[SYN, ACK] (<br>[SYN] Seq=0 (<br>[SYN]                                 | <pre>win=1024 L<br/>eq=1_Ack=1<br/>win=1024 L<br/>eq=1_Ack=1<br/>win=1024 L<br/>eq=1_Ack=1<br/>0 win=1024 L<br/>eq=0_Ack=1<br/>0 win=1024<br/>0 win=1024</pre>                            | xpression A<br>en=0 MSS<br>win=0 L<br>en=0 MSS<br>Len=0 MSS<br>Len=0 MS<br>Len=0 MS<br>A<br>Len=0 MS<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A<br>A   |        |
|              | ▲ Apply a display filt           Time           61 22.448483708           62 22.44848708           63 22.44848708           64 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849708           65 22.44849580           72 22.48  | er <ctrl-><br/>Source<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>192.166.217.3<br/>: 40<br/>on: 0xe14d (57677)<br/>(Don't Fragment)<br/>set: 0<br/>(Don't Fragment)<br/>set: 0<br/>192.166.217.3<br/>Pi0.168.217.3<br/>Pi0.168.10.10<br/>192.166.217.3<br/>Pi0.168.10.10<br/>192.166.217.3<br/>Pi0.168.10.10<br/>192.166.217.3<br/>Pi0.168.10.10<br/>192.166.217.3<br/>Pi0.168.10.10<br/>192.166.227.3<br/>Fi0.100 (Simple Contemported Contemported</ctrl->   | Destination<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 217, 3   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | Info<br>58 54775 → 53<br>54 53 → 54775<br>58 54775 → 253<br>58 54775 → 275<br>58 54775 → 275<br>58 54775 → 172<br>58 54775 → 172<br>58 54775 → 173<br>58 54775 → 113<br>1, Ack: 1, Len:<br>E.<br>8P.   | [SYN] Seq=0<br>[RST, ACK] S<br>[SYN] Seq=0<br>[SYN, ACK] S<br>[SYN] Seq=0<br>[SYN] Seq=0<br>5 [RST, ACK]<br>3 [SYN] Seq=0<br>5 [RST, ACK]<br>5 [RST, ACK]<br>[SYN] Seq=0   | <pre>win=1024 L<br/>eq=1 Ack=1<br/>Win=1024 L<br/>eq=1 Ack=1<br/>Win=1024 L<br/>eq=0 Ack=1<br/>Win=1024 L<br/>Win=1024 L<br/>Win=1024 L<br/>Win=1024 Win=1024<br/>Win=1024 Win=1024</pre> | xpression A<br>en=0 MSS<br>win=0 L<br>en=0 MSS<br>win=0<br>en=0 MSS<br>win=0<br>Len=0 MSS<br>c=1 Win=0<br>Len=0 M<br>c=1 Win=0<br>Len=0 M<br>win=0<br>win=0 Len=0 M<br>win=0 Len=0 M  |        |
|              | ■ Apply a display filt           Time           61 22, 44848300           62 22, 448637500           63 22, 44867300           64 22, 44867300           65 22, 44863300           65 22, 44863300           65 22, 44863300           65 22, 44863300           66 22, 44863300           71 22, 44863000           71 22, 44863000           71 22, 44863000           71 22, 448495000   | er <ctrl></ctrl> Source 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 192.166.217.3 : 40 on: 0xe14d (57677) (Don't Fragment) set: 0 (Don't Fragment) set: 0 P (6) sum: 0xf523 [valida ksum status: Unveri 168.10.10 192.168.217.3 P: Unknown] GeoIP: Unknown] GeoIP: Unknown] 0 57 1e 00 15 5d 4 d 40 00 40 66 f5 2 5 d5 f7 00 00 00 00 c 00 00   | Destination<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 217, 3   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ngth Info<br>58 54775 53<br>54 53 - 54775<br>58 54775 22<br>58 54775 22<br>58 54775 21<br>58 54775 172<br>54 1723 54775<br>54 1723 54775<br>54 1723 54775<br>54 54775 113<br>54 5900 5477<br>58 54775 113<br>1. Ack: 1, Len:<br>E.<br>   | [SYN] Seq=0<br>[RST, ACK] S<br>[SYN] Seq=0<br>[SYN, ACK] S<br>[SYN] Seq=0<br>5 [RST, ACK]<br>5 [RST, | <pre>win=1024 L<br/>eq=1 Ack=3<br/>win=1024 L<br/>eq=1 Ack=3<br/>win=1024 L<br/>eq=0 Ack=3<br/>0 Win=1024 L<br/>9 Win=1024 Seq=1 Ack<br/>0 Win=1024<br/>Win=1024</pre>                    | xpression A   |        |
|              | Apply a display filt           Time           61 22, 448483408           62 22, 448657500           63 22, 448657500           63 22, 44867308           65 22, 448497608           65 22, 448497608           66 22, 448497608           67 22, 448654808           67 22, 4484954808           71 22, 4484954808           80 20, 60 20, 61 20  | er <ctrl-><br/>Source<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3<br/>192,166,217.3</ctrl-> | Destination<br>192, 168, 10, 10<br>192, 168, 10, 10<br>192, 168, 10, 10<br>192, 168, 217, 3<br>192, 168, 217, 3   | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | ngth Info<br>58 54775 → 53<br>54 53 → 54775<br>58 54775 → 22<br>58 54775 → 22<br>58 54775 → 172<br>58 54775 → 172<br>58 54775 → 173<br>54 1723 → 54775<br>54 3723 → 54775<br>54 5900 → 54775<br>54 5900 → 54775<br>54 5900 → 54775<br>54 5900 → 54775<br>58 54775 → 113<br>1. Ack: 1, Len:<br>E.<br>E.<br>8P.  | [SYN] Seq=0 (<br>[SYN]  | <pre>win=1024 L<br/>eq=1 Ack=1<br/>win=1024 L<br/>eq=1 Ack=1<br/>win=1024 L<br/>eq=1 Ack=1<br/>0 win=1024 L<br/>eq=0 Ack=1<br/>0 win=1024<br/>0 win=1024</pre>                            | xpression A   |        |
|              | Apply a display filt           Time           61 22, 448483408           62 22, 448657500           63 22, 448657500           63 22, 44869780           65 22, 44849780           65 22, 44869780           65 22, 44869780           65 22, 44869780           67 22, 44869300           71 22, 44869300           71 22, 44869300           71 22, 44869300           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 22, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 72, 448495800           71 71 71 71 71 71 71 71 71 71 71 71 71 7  | er <ctrl></ctrl> Source J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 J92.168.217.3 : 40 on: 0xe14d (57677) (0on't Fragment) set: 0 : 64 P (6) J92.168.217.3 : Unknown] ontrol Protocol, Srr 0 57 1e 00 15 5d 4 d 40 00 40 66 f5 2 5 5d 5f 70 e0 00 or c 00 00  | Destination<br>192,168,10,10<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,10,10<br>192,168,217,3<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,10,10<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,168,217,3<br>192,17,17,17,17,17,17,17,17,17,17,17,17,17, | Protocol Le<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP<br>TCP | Info<br>58 54775 - 53<br>54 53 - 54775<br>58 54775 - 22<br>58 54775 - 275<br>58 54775 - 275<br>58 54775 - 172<br>58 54775 - 172<br>58 54775 - 173<br>58 54775 - 113<br>1, Ack: 1, Len:<br>E.<br>E.<br>8P.  | [SYN] Seq=0 (<br>[SYN]  | <pre>win=1024 L<br/>eq=1_Ack=1<br/>win=1024 L<br/>eq=1_Ack=1<br/>win=1024 L<br/>eq=0_Ack=1<br/>0_Win=1024<br/>0_Win=1024<br/>0_Win=1024<br/>Win=1024</pre>                                | xpression A   |        |

While running Wireshark, I observed that kali first sends ICMP requests to both the Ubuntu and the Windows server 2008. Wireshark then begins sending TCP requests and receives highlighted the TCP responses in red and sends out an "RST, ACK" in Flags. Plenty of packets were sent and plenty of them were dropped as well as indicated by black highlights. I also noticed that some of the TCP packets from

the subnet has been marked with red highlight as well as indicated by the source having the IP 192.168.10.2, forming a TCP connection with 192.168.10.10(Ubuntu) and 192.168.10.11(Windows Server 2008. By the end of the TCP transmissions, Kali sends TCP request to an open port which is port 21 and received an ACK reply. A couple of packets later, I see that there is an RST from the regular external Kali port used to send TCP packets 50088 to port 21 in Ubuntu. After the scan has been performed, external kali nmap scan returns a full port scan indicating that ports 21, 80, 135, 445 are open ports for windows server 2008 and port 21 for Ubuntu. It also displays the version under "Service Info". The scan went through a total of 256 IP addresses in total.

## TASK B:

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



| Rule # | Interface | Actio | Source IP     | Destination IP | Protocol (port# if applicable) |
|--------|-----------|-------|---------------|----------------|--------------------------------|
|        |           | n     |               |                |                                |
| 2      | WAN       | Block | 192.168.217.3 | 192.168.10.10  | ICMP(any)                      |
|        |           |       |               |                |                                |
|        |           |       |               |                |                                |

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

|                         | ( 🏪 Ubuntu 64-bit o                  | on CY301-JDYC | 0001 - Virtual | Machine Conne  | ection                 |         |                  |           |            |                         |                      | - 0  |
|-------------------------|--------------------------------------|---------------|----------------|----------------|------------------------|---------|------------------|-----------|------------|-------------------------|----------------------|--|
|                         | File Action                          | Media Clipb   | oard View      | Help           |                        |         |                  |           |            |                         |                      |  |
|                         |                                      | 🕘   II 🕩      | 😼 5 🖳          |                |                        |         |                  |           |            |                         |                      |  |
|                         | 1 🗯 💉 🕯 pfSense.CYSE                 | .com - Firev  | all: Rules     | WAN - Moz      | illa Firefox           | _       |                  |           |            |                         | 😑 🗘                  | <b>,                                    </b> |
|                         |                                      | Restore Ses   | sion           | 🗙 💆 pfs        | ense.CYSE.com          | ×       | +                |           |            |                         |                      |  |
| enTest: ~               | • • • • • •                          | 🛈 🕰 🛛 https   | ://192.168.    | 10.2/firewal   | l_rules.php?if=wan     | 1       |                  |           | ~ C        | Q Search                | ☆ 🖻                  |  |
|                         |                                      | WADA          | INC. The 'e    | dmin' a a a un | t poonword is est to t | ho dofe | aultualua. Chr   | on a o th |            | W<br>In the Lleer Menou | 107                  |  |
| any incorrect results a | at https://nma                       | WAR           | ing. me a      | umin accoun    | i password is set to t | ne dela |                  | ange u    | ie passwoi | tu in the Oser Manaj    | jei.                 |  |
| d in 13 90 seconds      |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| a in 19:50 Seconds      |                                      | Fire          | wall / F       | Rules / W      | /AN                    |         |                  |           |            |                         | ₽                    | : 📖 🖽 😮                                      |
| bytes of data.          |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| l=63 t1me=5.56 ms       |                                      | _             |                |                |                        |         |                  |           |            |                         |                      |  |
| l=63 time=7.44 ms       |                                      | The fi        | rewall rule o  | onfiguration   | has been changed       |         |                  |           |            |                         |                      | 1.01   |
| l=63 time=6.31 ms       |                                      | The c         | andes mus      | t he annlied f | or them to take effect |         |                  |           |            |                         | 🗸 🗸                  | oply Changes                                 |
| l=63 time=18.7 ms       |                                      | 1110 01       | iangeo mao     | c be applied i |                        |         |                  |           |            |                         |                      |  |
| l=63 time=12.5 ms       |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| l=63 time=8.32 ms       |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| L=63 T1Me=2.67 MS       |                                      | Floatin       | g WAN          | LAN            |                        |         |                  |           |            |                         |                      |  |
| at less time blue       |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| 4.580 ms                |                                      | Rule          | s (Drag t      | o Change       | Order)                 |         |                  |           |            |                         |                      |  |
| byton of data           |                                      |               | States         | Protocol       | Source                 | Port    | Destination      | Port      | Gateway    | Queue Schedule          | Description          | Actions                                      |
| bytes of data.          |                                      | ×             | 0/0 B          | *              | Reserved               | *       | *                | *         | *          | *                       | Block bogon networks | <b>n</b>                                     |
|                         |                                      |               |                |                | Not assigned by        |         |                  |           |            |                         |                      | · ·  |
| acket loss, time 487ms  |                                      |               |                |                | IANA                   |         |                  |           |            |                         |                      |  |
|                         |                                      |               | 0 /0 B         | IPv4           | 192.168.217.3          | *       | *                | *         | *          | none                    |                      | .f. ∕ □                                      |
|                         |                                      |               |                | ICMP           |                        |         |                  |           |            |                         |                      | Ň m  |
|                         |                                      |               |                | any            |                        |         |                  |           |            |                         |                      | <b>U</b>                                     |
|                         |                                      |               | 10/674         | IPv4+6 *       | WAN net                | *       | *                | *         | *          | none                    | Open Connection IPv4 | .f. ∥□                                       |
|                         |                                      |               | KiB            |                |                        |         |                  |           |            |                         | and IPv6             | Ŏ â  |
|                         |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| L.                      |                                      |               |                |                |                        |         |                  |           |            | 1 Add 1 Ad              | ld 前 Delete 🗟 Save   | + Separator                                  |
|                         |                                      | •             |                |                |                        |         |                  |           |            |                         |                      |  |
|                         |                                      |               |                |                |                        |         |                  |           |            |                         |                      |  |
| • 0 Hi 🖬 Huma           | r. V. Managor 👘 Attackor Kali - Exte | or 🚺 nEr      | onco - Firoual | 16 🗈 W         | indows Sonvor 20       | 🗅 Ubu   | untu 64-bit on C |           |            |                         |                      | 9:37 AM                                      |
| - >> H M Hype           |                                      | er 🤏 pris     | ense - Filewai | 10 🥪 🖬         | indows server 20       | < 000   | und 04-bit on C. |           |            |                         | ,                    | ` <del>⊨</del> ¶ <sup>№</sup> 3/3/2023       |
| <b>–</b> • •            |                                      |               |                |                |                        |         |                  |           |            | ation                   | Ducto col /:: -      |  |
| Rule #                  | Interface                            | Act           | ion            |                | Source                 | IP      |                  |           | Jestin     | ation                   | Protocol (po         | ort#   |
|                         |                                      |               |                |                |                        |         |                  | 1         | Р          |                         | if annlicable        |  |
|                         |                                      | -             | _              |                |                        |         |                  |           | •          |                         |                      |  |
| 2                       | WAN                                  | BLC           | ОСК            |                | 192.16                 | 8.2     | 17.3             | A         | ١NY        |                         | ICMP(ANY             | )  |
|                         |                                      |               |                |                | 1                      |         |                  |           |            |                         | •                    | -  |

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.

| on CY30        | 1-JDYC                  | 0001 - Virtual      | Machine Conr               | ection                              |          |                                    |               |                                   |                 |                                 |                        |                  | - [              | ×  |  |  |  |
|----------------|-------------------------|---------------------|----------------------------|-------------------------------------|----------|------------------------------------|---------------|-----------------------------------|-----------------|---------------------------------|------------------------|------------------|------------------|--|--|--|--|
| Media          | Clipb                   | oard View           | Help                       |                                     |          |                                    |               |                                   |                 |                                 |                        | 🖳 Attacker Ka    | ali - External \ | Workstation on (   | CY301-JDYCO001   | - Virtual Machine Connection   | on   |
| <b>()</b>   II | ▶                       | 🍢 5 i 🕎             |                            |                                     |          |                                    |               |                                   |                 |                                 |                        | File Action      | n Media          | Clipboard \  | iew Help   |  |  |
| .com -         | Firev                   | vall: Rules:        | WAN - Mo                   | zilla Firefox                       |          | × .                                |               |                                   |                 |                                 | E                      |                  | <b>0</b> 011     |  | Torminal 🛪   |  | Mon  |
| Resto          | ire Ses                 | ssion               | × 🗹 pf                     | Sense.CYSE.com                      | ×        | (+                                 |               |                                   |                 |                                 |                        | Аррисатіог       | 15 • P           | laces + L-   | i Terminal •   |  | Mon C  |
| i 陷            | https                   | ://192.168.         | 10.2/firewa                | Il_rules.php?if=w                   | /an      |                                    |               | C                                 | <b>Q</b> Search |                                 |                        |                  |                  |  |  |  |  |
| COT            |                         | ENSE S<br>Y EDITION | System → I<br>dmin' accour | nterfaces 👻 Fire                    | wall 👻   | Services 		 V<br>efault value. Cha | PN - Sta      | atus <del>-</del> D<br>assword in | Diagnostics     | s <del>▼</del> Help<br>Nanager. | •                      | V                | 'Mshare          | Nessus I   | nfo  | (  | root@CS2A  |
|                | Fire<br>The cl<br>Monit | wall / F            | Rules / V                  | VAN<br>kd successfully. The<br>ess. | efirewa  | II rules are now r                 | eloading in   | the backg                         | round.          |                                 |                        |                  |                  |  | File Edit<br>Service de<br>.org/submi<br>Nmap done:<br>root@CS2AP<br>Starting N<br>Nmap scan<br>Host is up<br>All 1000 s | View Search Term<br>tection performed<br>t/.<br>256 IP addresses<br>enTest:-# nmap -s<br>map 7.70 ( https:<br>report for 192.10<br>(0.0074s latenc;<br>canned ports on 5 | nal Help<br>1. Please repor<br>5 (3 hosts up)<br>5V 192.168.10.<br>68.10.2<br>7).<br>192.168.10.2 ar |
|                | Floating WAN LAN        |                     | LAN                        |                                     |          |                                    |               |                                   |                 |                                 | M                      |                  |                  | Mmap scan report for 192.168.10.10<br>Host is up (0.0071s latency).<br>All 1000 scanned ports on 192.168.10.10 a<br>Nmap scan report for 192.168.10.11 |  |  |  |
|                | Rule                    | s (Drag to          | o Change<br>Protocol       | Order)                              | Port     | Destination                        | Port          | Gataway                           | ( <u>Oueue</u>  | Schedule                        | Description            | -                |                  |  | Host is up<br>Not shown:   | (0.0057s latency<br>999 filtered por   | /).<br>-ts   |
|                | ×                       | 0 /0 B              | *                          | Reserved<br>Not assigned by<br>IANA | *        | *                                  | *             | *                                 | *               | Schedule                        | Block bogo<br>networks | 8                |                  |  | PORT STA<br>21/tcp ope<br>Service In<br>Service de   | TE SERVICE VERSIO<br>n ftp Micros<br>fo: OS: Windows;<br>tection performed   | DN<br>soft ftpd<br>CPE: cpe:/o:mi<br>d. Please repor   |
|                | <b>X</b>                | 0 /0 B              | IPv4<br>TCP                | 192.168.217.3                       | *        | 192.168.10.2                       | 53<br>(DNS)   | *                                 | none            |                                 |                        | <u>_</u>         |                  |  | .org/submi<br>Nmap done:<br><mark>root@CS2AP</mark>  | t/ .<br>256 IP addresse:<br><mark>enTest:~#</mark>   | s (3 hosts up)   |
|                | <b>×</b>                | 0 /88 B             | IPv4<br>TCP                | 192.168.217.3                       | *        | 192.168.10.10                      | ) 21<br>(FTP) | *                                 | none            |                                 |                        | =                |                  |  |  |  |  |
|                | <b>×</b>                | 0 /697<br>KiB       | IPv4<br>TCP                | 192.168.217.3                       | *        | *                                  | 80 -<br>49154 | *                                 | none            |                                 |                        |                  |                  |  |  |  |  |
| 4              | م                       | ₽i                  | Hyper-V                    | Manager                             | Attacker | r Kali - Exter 🚦                   | pFsense -     | Firewall 6                        | 🤩 ИЬ            | untu 64-bit (                   | on C 🔤 V               | Vindows Server 2 | 20               |  |  |  | へ 覧 4 8 3:40 AM<br>3/6/2023  |
| -              |                         |                     |                            | 1                                   |          |                                    |               |                                   |                 |                                 |                        |                  | -                |  |  |  |  |
| R              | ule                     | :#                  |                            | Interfa                             | ace      |                                    | Actio         | on                                |                 | So                              | ource                  | IP               |                  | Destina  | ation IP   | Prot<br>(por<br>app  | tocol<br>rt# if<br>licable   |
| 2              | ule                     | e #                 |                            | Interfa<br>WAN                      | ace      |                                    | Actic         | on<br>CK                          |                 | <b>So</b><br>19                 | <b>Durce</b>           | IP<br>3.217.3    | 3                | Destina<br>ANY   | ation IP   | Prot<br>(por<br>app<br>TCF   | tocol<br>rt# if<br>licable   |

192.168.217.3

ANY

ТСР PORT:21

ТСР POR:53

| 4. Keep the firewall policies you | ı created in Task B.3 and r | epeat Task A.1. What's th |
|-----------------------------------|-----------------------------|---------------------------|
| difference?                       |                             |                           |

BLOCK

WAN

4



Procedure

• By blocking all TCP packets except FTP port 21 on windows 2008 server, nmap yields no reports on open ports.