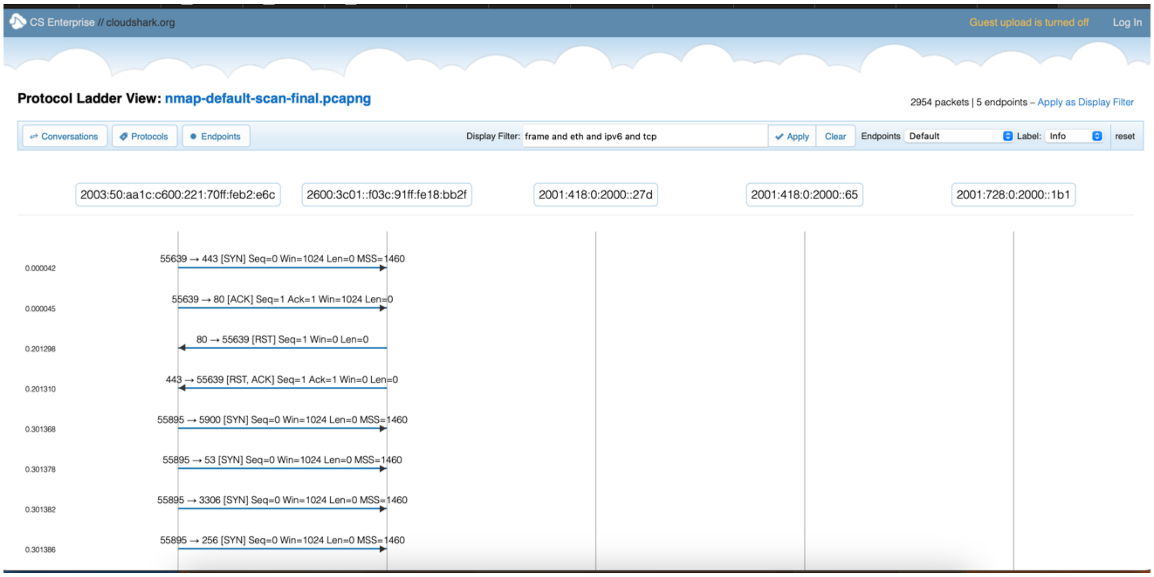
NETWORK INVESTIGATION LAB

STEPHEN MENSAH

Sample Lab Screenshots

PORT SCAN DETECTION

TCP Communications between IP addresses



Protocol Ladder View: nmap-default-scan-final.pcapng

2954 packets | 5 endpoints – Apply as Display Filter

Display Filter: frame and eth and ipv6 and tcp

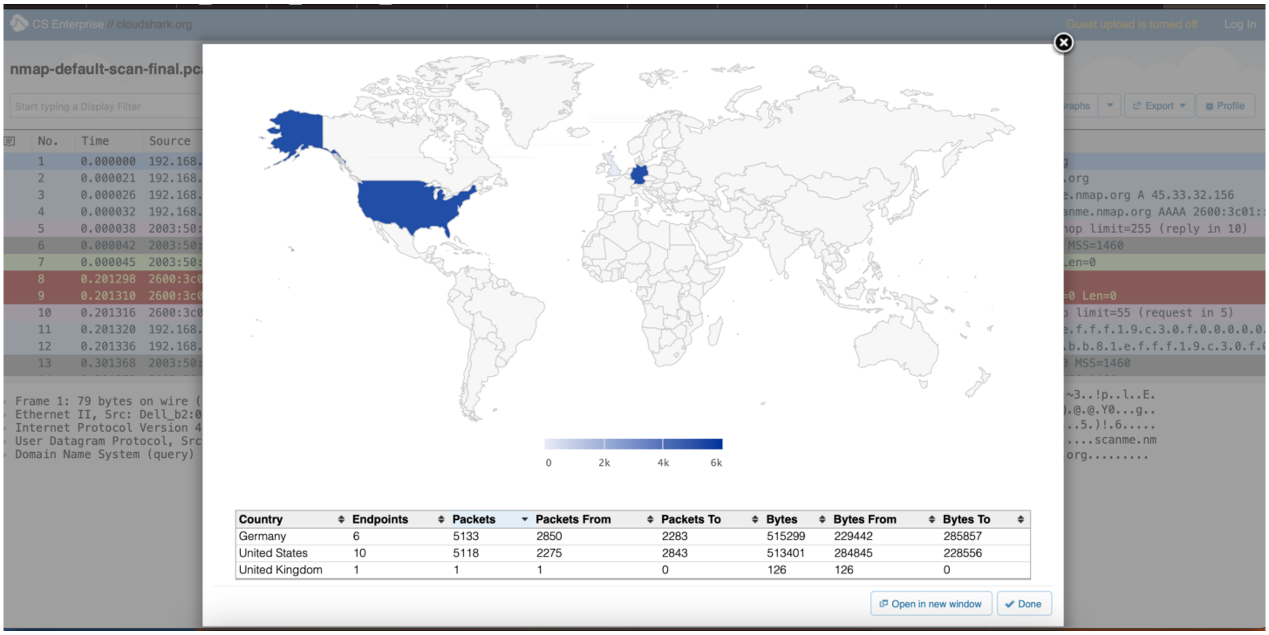
Endpoints: Default

Label: Info

2003:50:aa1c:c600:221:70ff:feb2:e6c | 2600:3c01::f03c:91ff:fe18:bb2f | 2001:418:0:2000::27d | 2001:418:0:2000::65 | 2001:728:0:2000::1b1

```
0.000042   55639 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000045   55639 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
0.201298   80 → 55639 [RST] Seq=1 Win=0 Len=0
0.201310   443 → 55639 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
0.301368   55895 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.301378   55895 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.301382   55895 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.301386   55895 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

GeoIP World Map Dashboard displaying source and destinations of TCP packets


CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
Start typing a Display Filter
raphs
Export
Profile
0
2k
4k
6k
Open in new window
Done

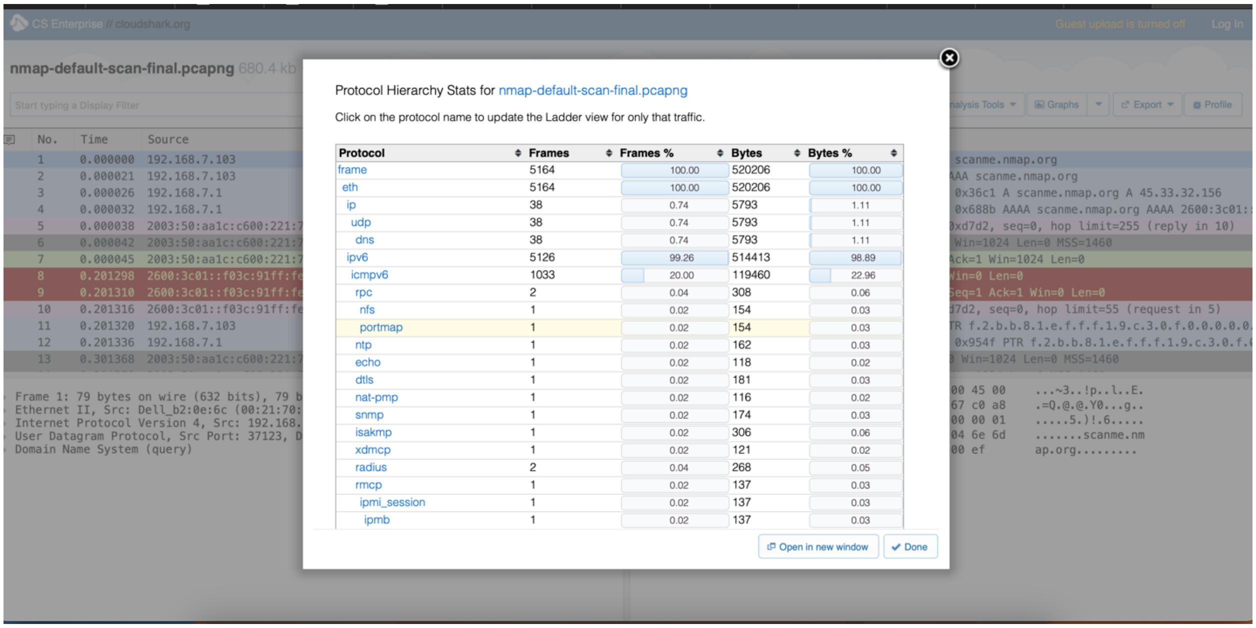
nmap-default-scan-final.pc

```
No.  Time      Source
1    0.000000  192.168.                    g
2    0.000021  192.168.                    .org
3    0.000026  192.168.                    e.nmap.org A 45.33.32.156
4    0.000032  192.168.                    anme.nmap.org AAAA 2600:3c01:
5    0.000038  2003:50:                    hop limit=255 (reply in 10)
6    0.000042  2003:50:                    MSS=1460
7    0.000045  2003:50:                    Len=0
8    0.201298  2600:3c0
9    0.201310  2600:3c0                    =0 Len=0
10   0.201316  2600:3c0                    limit=55 (request in 5)
11   0.201320  192.168.                    e.f.f.f.1.9.c.3.0.f.0.0.0.0.0.
12   0.201336  192.168.                    .b.b.8.1.e.f.f.f.1.9.c.3.0.f.
13   0.301368  2003:50:                    0 MSS=1460

Frame 1: 79 bytes on wire (                ~3..!p..l..E.
Ethernet II, Src: Dell_b2:0                ).@.@.Y0...g..
Internet Protocol Version 4                ..5.)!.6.....
User Datagram Protocol, Src                ....scanme.nm
Domain Name System (query)                 org.........
```

Country	Endpoints	Packets	Packets From	Packets To	Bytes	Bytes From	Bytes To
Germany	6	5133	2850	2283	515299	229442	285857
United States	10	5118	2275	2843	513401	284845	228556
United Kingdom	1	1	1	0	126	126	0

Protocol Hierarchy dashboard showing the number of packet per each protocol


CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
nmap-default-scan-final.pcapng 680.4 kb
Start typing a Display Filter
nalysis Tools
Graphs
Export
Profile

```
No.  Time      Source                                              
1    0.000000  192.168.7.103                                       scanme.nmap.org
2    0.000021  192.168.7.103                                      AAA scanme.nmap.org
3    0.000026  192.168.7.1                                         0x36c1 A scanme.nmap.org A 45.33.32.156
4    0.000032  192.168.7.1                                         0x688b AAAA scanme.nmap.org AAAA 2600:3c01:
5    0.000038  2003:50:aa1c:c600:221:7                            0xd7d2, seq=0, hop limit=255 (reply in 10)
6    0.000042  2003:50:aa1c:c600:221:7                             Win=1024 Len=0 MSS=1460
7    0.000045  2003:50:aa1c:c600:221:7                            Ack=1 Win=1024 Len=0
8    0.201298  2600:3c01::f03c:91ff:fe                            Win=0 Len=0
9    0.201310  2600:3c01::f03c:91ff:fe                            Seq=1 Ack=1 Win=0 Len=0
10   0.201316  2600:3c01::f03c:91ff:fe                            d7d2, seq=0, hop limit=55 (request in 5)
11   0.201320  192.168.7.103                                      TR f.2.b.b.8.1.e.f.f.f.1.9.c.3.0.f.0.0.0.0.0.
12   0.201336  192.168.7.1                                         0x954f PTR f.2.b.b.8.1.e.f.f.f.1.9.c.3.0.f.
13   0.301368  2003:50:aa1c:c600:221:7                            0 Win=1024 Len=0 MSS=1460

Frame 1: 79 bytes on wire (632 bits), 79 b                        00 45 00     ...~3..!p..l..E.
Ethernet II, Src: Dell_b2:0e:6c (00:21:70:                        67 c0 a8     .=Q.@.@.Y0...g..
Internet Protocol Version 4, Src: 192.168.                        00 00 01     .....5.)!.6.....
User Datagram Protocol, Src Port: 37123, D                        04 6e 6d     .......scanme.nm
Domain Name System (query)                                        00 ef        ap.org.........
```

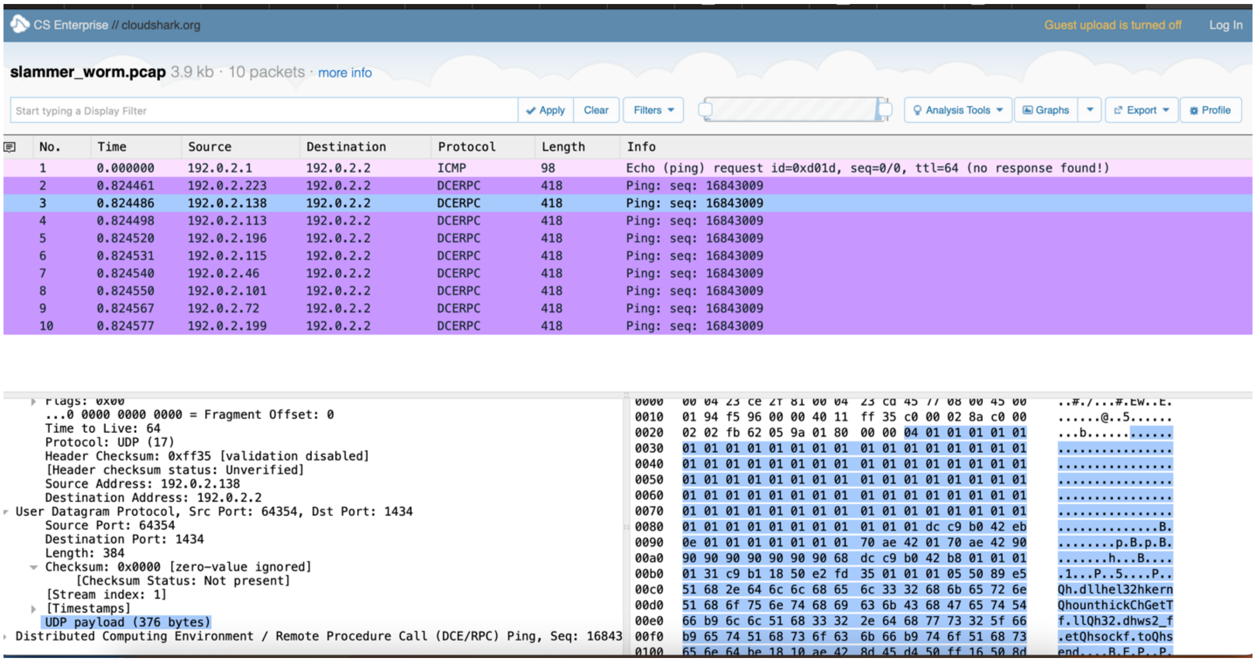
Protocol Hierarchy Stats for nmap-default-scan-final.pcapng

Click on the protocol name to update the Ladder view for only that traffic.

Protocol	Frames	Frames %	Bytes	Bytes %
frame	5164	100.00	520206	100.00
eth	5164	100.00	520206	100.00
ip	38	0.74	5793	1.11
udp	38	0.74	5793	1.11
dns	38	0.74	5793	1.11
ipv6	5126	99.26	514413	98.89
icmpv6	1033	20.00	119460	22.96
rpc	2	0.04	308	0.06
nfs	1	0.02	154	0.03
portmap	1	0.02	154	0.03
ntp	1	0.02	162	0.03
echo	1	0.02	118	0.02
dtls	1	0.02	181	0.03
nat-pmp	1	0.02	116	0.02
snmp	1	0.02	174	0.03
isakmp	1	0.02	306	0.06
xdmcp	1	0.02	121	0.02
radius	2	0.04	268	0.05
rmcp	1	0.02	137	0.03
ipmi_session	1	0.02	137	0.03
ipmb	1	0.02	137	0.03

SLAMMER WORM

The contents of one UDP payload from Slammer

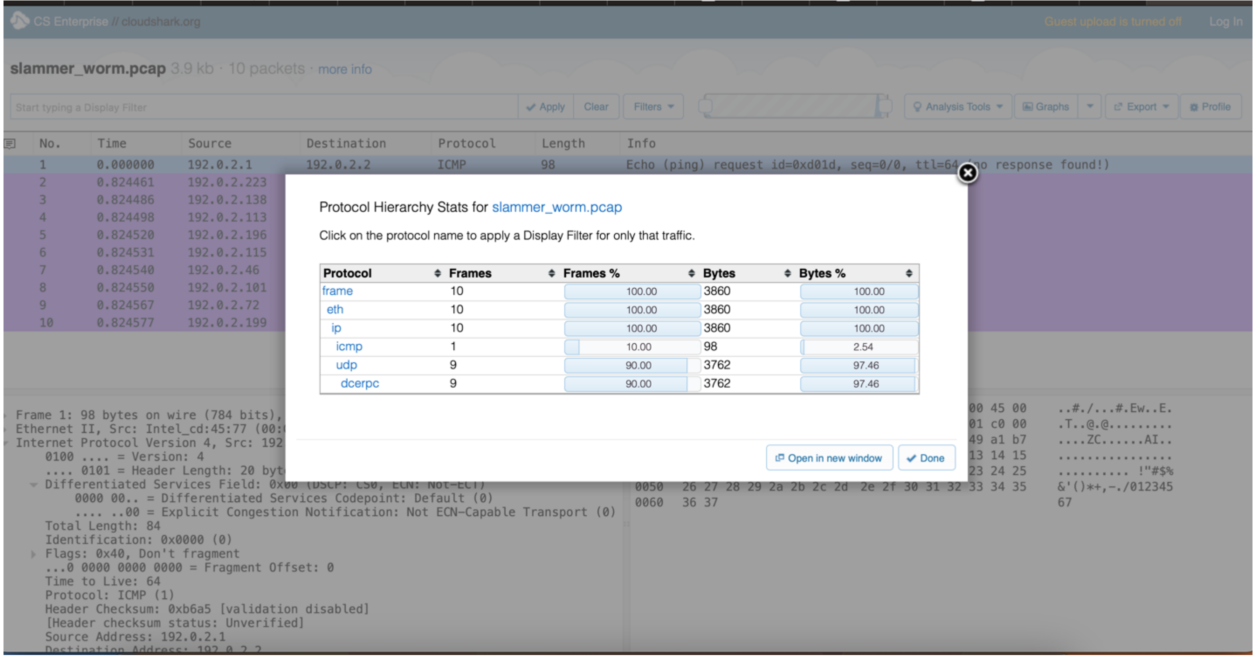

CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
slammer_worm.pcap 3.9 kb · 10 packets · more info
Start typing a Display Filter
✓ Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

```
No.  Time      Source         Destination  Protocol  Length  Info
1    0.000000  192.0.2.1      192.0.2.2    ICMP      98      Echo (ping) request id=0xd01d, seq=0/0, ttl=64 (no response found!)
2    0.824461  192.0.2.223    192.0.2.2    DCERPC    418     Ping: seq: 16843009
3    0.824486  192.0.2.138    192.0.2.2    DCERPC    418     Ping: seq: 16843009
4    0.824498  192.0.2.113    192.0.2.2    DCERPC    418     Ping: seq: 16843009
5    0.824520  192.0.2.196    192.0.2.2    DCERPC    418     Ping: seq: 16843009
6    0.824531  192.0.2.115    192.0.2.2    DCERPC    418     Ping: seq: 16843009
7    0.824540  192.0.2.46     192.0.2.2    DCERPC    418     Ping: seq: 16843009
8    0.824550  192.0.2.101    192.0.2.2    DCERPC    418     Ping: seq: 16843009
9    0.824567  192.0.2.72     192.0.2.2    DCERPC    418     Ping: seq: 16843009
10   0.824577  192.0.2.199    192.0.2.2    DCERPC    418     Ping: seq: 16843009
```

```
    Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xff35 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.0.2.138
    Destination Address: 192.0.2.2
User Datagram Protocol, Src Port: 64354, Dst Port: 1434
    Source Port: 64354
    Destination Port: 1434
    Length: 384
    Checksum: 0x0000 [zero-value ignored]
        [Checksum Status: Not present]
    [Stream index: 1]
    [Timestamps]
    UDP payload (376 bytes)
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Ping, Seq: 16843
```

```
0000  00 04 23 ce 2f 81 00 04  23 cd 45 77 08 00 45 00   ..#./...#.Ew..E.
0010  01 94 f5 96 00 00 40 11  ff 35 c0 00 02 8a c0 00   ......@..5......
0020  02 02 fb 62 05 9a 01 80  00 00 04 01 01 01 01 01   ...b............
0030  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ................
0040  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ................
0050  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ................
0060  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ................
0070  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ................
0080  01 01 01 01 01 01 01 01  01 01 01 dc c9 b0 42 eb   ..............B.
0090  0e 01 01 01 01 01 01 01  70 ae 42 01 70 ae 42 90   ........p.B.p.B.
00a0  90 90 90 90 90 90 90 68  dc c9 b0 42 b8 01 01 01   .......h...B....
00b0  01 31 c9 b1 18 50 e2 fd  35 01 01 01 05 50 89 e5   .1...P..5....P..
00c0  51 68 2e 64 6c 6c 68 65  6c 33 32 68 6b 65 72 6e   Qh.dllhel32hkern
00d0  51 68 6f 75 6e 74 68 69  63 6b 43 68 47 65 74 54   QhounthickChGetT
00e0  66 b9 6c 6c 51 68 33 32  2e 64 68 77 73 32 5f 66   f.llQh32.dhws2_f
00f0  b9 65 74 51 68 73 6f 63  6b 66 b9 74 6f 51 68 73   .etQhsockf.toQhs
0100  65 6e 64 be 18 10 ae 42  8d 45 d4 50 ff 16 50 8d   end....B.E.P..P.
```

Protocol Hierarchy Statistics for the Slammer worm


CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
slammer_worm.pcap 3.9 kb · 10 packets · more info
Start typing a Display Filter
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

```
No.   Time       Source          Destination    Protocol   Length   Info
1     0.000000   192.0.2.1       192.0.2.2      ICMP       98       Echo (ping) request id=0xd01d, seq=0/0, ttl=64 no response found!)
2     0.824461   192.0.2.223
3     0.824486   192.0.2.138
4     0.824498   192.0.2.113
5     0.824520   192.0.2.196
6     0.824531   192.0.2.115
7     0.824540   192.0.2.46
8     0.824550   192.0.2.101
9     0.824567   192.0.2.72
10    0.824577   192.0.2.199
```

Protocol Hierarchy Stats for slammer_worm.pcap

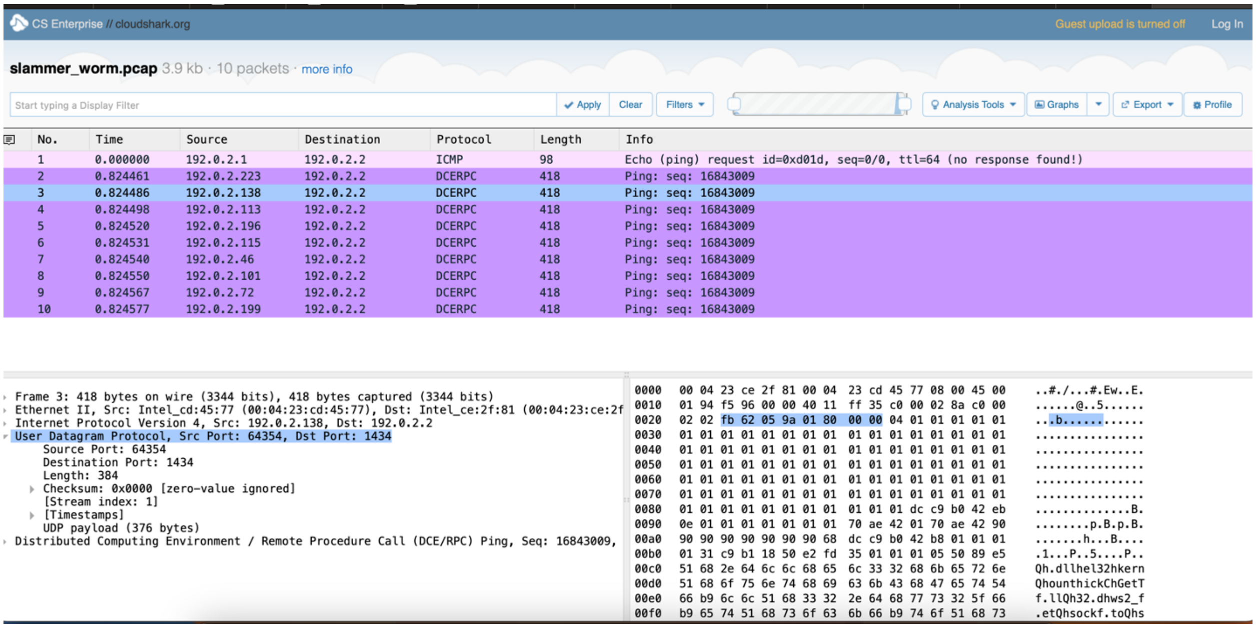
Click on the protocol name to apply a Display Filter for only that traffic.

Protocol	Frames	Frames %	Bytes	Bytes %
frame	10	100.00	3860	100.00
eth	10	100.00	3860	100.00
ip	10	100.00	3860	100.00
icmp	1	10.00	98	2.54
udp	9	90.00	3762	97.46
dcerpc	9	90.00	3762	97.46

```
Frame 1: 98 bytes on wire (784 bits),
Ethernet II, Src: Intel_cd:45:77 (00:
Internet Protocol Version 4, Src: 192
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 byt
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xb6a5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.0.2.1
    Destination Address: 192.0.2.2
```

```
                                     00 45 00     ..#./...#.Ew..E.
                                     01 c0 00     .T..@.@.........
                                     49 a1 b7     ....ZC......AI..
                                     13 14 15     ................
                                     23 24 25     .......... !"#$%
0050   26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35     &'()*+,-./012345
0060   36 37                                                67
```

Details of a header of a selected packet from the slammer worm capture


CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
slammer_worm.pcap 3.9 kb · 10 packets · more info
Start typing a Display Filter
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

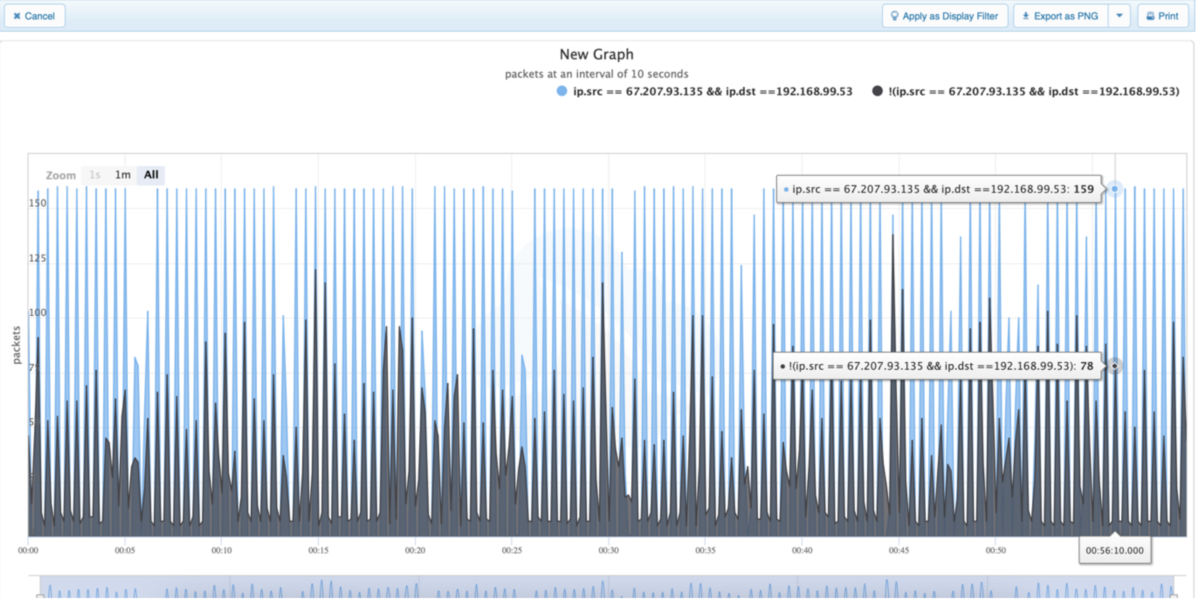
```
No.   Time       Source          Destination    Protocol   Length   Info
1     0.000000   192.0.2.1       192.0.2.2      ICMP       98       Echo (ping) request id=0xd01d, seq=0/0, ttl=64 (no response found!)
2     0.824461   192.0.2.223     192.0.2.2      DCERPC     418      Ping: seq: 16843009
3     0.824486   192.0.2.138     192.0.2.2      DCERPC     418      Ping: seq: 16843009
4     0.824498   192.0.2.113     192.0.2.2      DCERPC     418      Ping: seq: 16843009
5     0.824520   192.0.2.196     192.0.2.2      DCERPC     418      Ping: seq: 16843009
6     0.824531   192.0.2.115     192.0.2.2      DCERPC     418      Ping: seq: 16843009
7     0.824540   192.0.2.46      192.0.2.2      DCERPC     418      Ping: seq: 16843009
8     0.824550   192.0.2.101     192.0.2.2      DCERPC     418      Ping: seq: 16843009
9     0.824567   192.0.2.72      192.0.2.2      DCERPC     418      Ping: seq: 16843009
10    0.824577   192.0.2.199     192.0.2.2      DCERPC     418      Ping: seq: 16843009
```

```
Frame 3: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)
Ethernet II, Src: Intel_cd:45:77 (00:04:23:cd:45:77), Dst: Intel_ce:2f:81 (00:04:23:ce:2f
Internet Protocol Version 4, Src: 192.0.2.138, Dst: 192.0.2.2
User Datagram Protocol, Src Port: 64354, Dst Port: 1434
    Source Port: 64354
    Destination Port: 1434
    Length: 384
    Checksum: 0x0000 [zero-value ignored]
    [Stream index: 1]
    [Timestamps]
    UDP payload (376 bytes)
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Ping, Seq: 16843009,
```

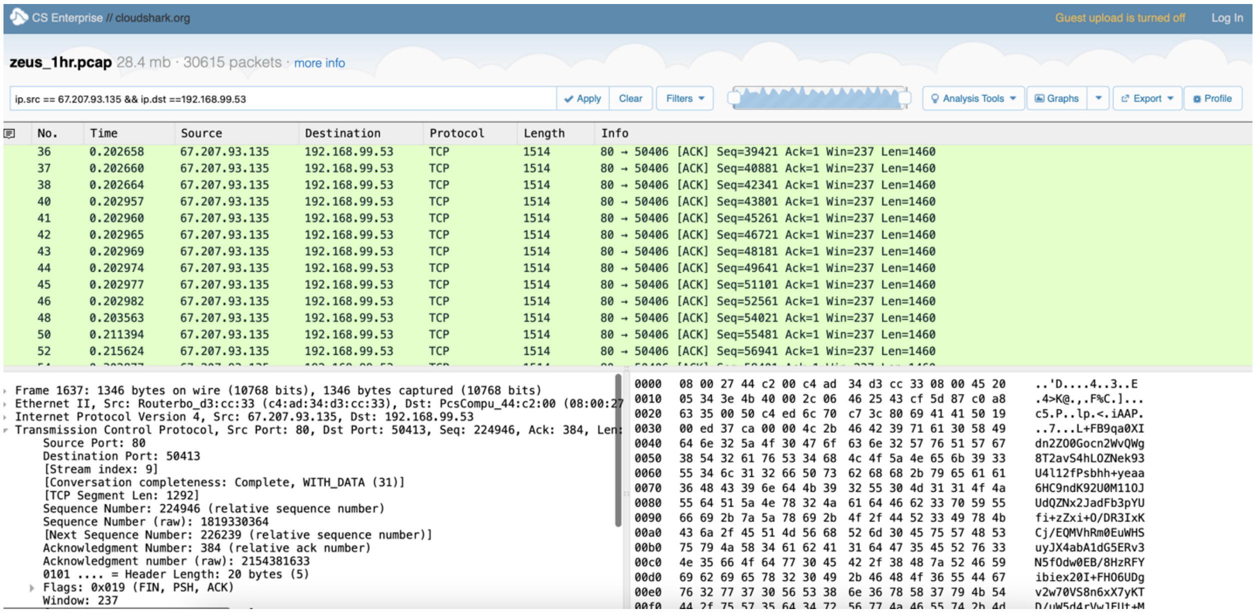
```
0000   00 04 23 ce 2f 81 00 04  23 cd 45 77 08 00 45 00     ..#./...#.Ew..E.
0010   01 94 f5 96 00 00 40 11  ff 35 c0 00 02 8a c0 00     ......@..5......
0020   02 02 fb 62 05 9a 01 80  00 00 04 01 01 01 01 01     ...b............
0030   01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01     ................
0040   01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01     ................
0050   01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01     ................
0060   01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01     ................
0070   01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01     ................
0080   01 01 01 01 01 01 01 01  01 01 01 dc c9 b0 42 eb     ..............B.
0090   0e 01 01 01 01 01 01 01  70 ae 42 01 70 ae 42 90     ........p.B.p.B.
00a0   90 90 90 90 90 90 90 68  dc c9 b0 42 b8 01 01 01     .......h...B....
00b0   01 31 c9 b1 18 50 e2 fd  35 01 01 01 05 50 89 e5     .1...P..5....P..
00c0   51 68 2e 64 6c 6c 68 65  6c 33 32 68 6b 65 72 6e     Qh.dllhel32hkern
00d0   51 68 6f 75 6e 74 68 69  63 6b 43 68 47 65 74 54     QhounthickChGetT
00e0   66 b9 6c 6c 51 68 33 32  2e 64 68 77 73 32 5f 66     f.llQh32.dhws2_f
00f0   b9 65 74 51 68 73 6f 63  6b 66 b9 74 6f 51 68 73     .etQhsockf.toQhs
```

ZEUS

Cloudshark inbuilt graph dashboard showing the consistent connections between two IP addresses at a 10-second interval.



Filtered Packets


CS Enterprise // cloudshark.org
Guest upload is turned off
Log In
zeus_1hr.pcap 28.4 mb · 30615 packets · more info
✔ Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

ip.src == 67.207.93.135 && ip.dst ==192.168.99.53

No.	Time	Source	Destination	Protocol	Length	Info
36	0.202658	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=39421 Ack=1 Win=237 Len=1460
37	0.202660	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=40881 Ack=1 Win=237 Len=1460
38	0.202664	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=42341 Ack=1 Win=237 Len=1460
40	0.202957	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=43801 Ack=1 Win=237 Len=1460
41	0.202960	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=45261 Ack=1 Win=237 Len=1460
42	0.202965	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=46721 Ack=1 Win=237 Len=1460
43	0.202969	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=48181 Ack=1 Win=237 Len=1460
44	0.202974	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=49641 Ack=1 Win=237 Len=1460
45	0.202977	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=51101 Ack=1 Win=237 Len=1460
46	0.202982	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=52561 Ack=1 Win=237 Len=1460
48	0.203563	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=54021 Ack=1 Win=237 Len=1460
50	0.211394	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=55481 Ack=1 Win=237 Len=1460
52	0.215624	67.207.93.135	192.168.99.53	TCP	1514	80 → 50406 [ACK] Seq=56941 Ack=1 Win=237 Len=1460

```
▸ Frame 1637: 1346 bytes on wire (10768 bits), 1346 bytes captured (10768 bits)
▸ Ethernet II, Src: Routerbo_d3:cc:33 (c4:ad:34:d3:cc:33), Dst: PcsCompu_44:c2:00 (08:00:27
▸ Internet Protocol Version 4, Src: 67.207.93.135, Dst: 192.168.99.53
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 50413, Seq: 224946, Ack: 384, Len:
    Source Port: 80
    Destination Port: 50413
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1292]
    Sequence Number: 224946 (relative sequence number)
    Sequence Number (raw): 1819330364
    [Next Sequence Number: 226239 (relative sequence number)]
    Acknowledgment Number: 384 (relative ack number)
    Acknowledgment number (raw): 2154381633
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x019 (FIN, PSH, ACK)
    Window: 237
```

```
0000   08 00 27 44 c2 00 c4 ad  34 d3 cc 33 08 00 45 20    ..'D....4..3..E
0010   05 34 3e 4b 40 00 2c 06  46 25 43 cf 5d 87 c0 a8    .4>K@.,.F%C.]...
0020   63 35 00 50 c4 ed 6c 70  c7 3c 80 69 41 41 50 19    c5.P..lp.<.iAAP.
0030   00 ed 37 ca 00 00 4c 2b  46 42 39 71 61 30 58 49    ..7...L+FB9qa0XI
0040   64 6e 32 5a 4f 30 47 6f  63 6e 32 57 76 51 57 67    dn2ZO0Gocn2WvQWg
0050   38 54 32 61 76 53 34 68  4c 4f 5a 4e 65 6b 39 33    8T2avS4hLOZNek93
0060   55 34 6c 31 32 66 50 73  62 68 68 2b 79 65 61 61    U4l12fPsbhh+yeaa
0070   36 48 43 39 6e 64 4b 39  32 55 30 4d 31 31 4f 4a    6HC9ndK92U0M11OJ
0080   55 64 51 5a 4e 78 32 4a  61 64 46 62 33 70 59 55    UdQZNx2JadFb3pYU
0090   66 69 2b 7a 5a 78 69 2b  4f 2f 44 52 33 49 78 4b    fi+zZxi+O/DR3IxK
00a0   43 6a 2f 45 51 4d 56 68  52 6d 30 45 75 57 48 53    Cj/EQMVhRm0EuWHS
00b0   75 79 4a 58 34 61 62 41  31 64 47 35 45 52 76 33    uyJX4abA1dG5ERv3
00c0   4e 35 66 4f 64 77 30 45  42 2f 38 48 7a 52 46 59    N5fOdw0EB/8HzRFY
00d0   69 62 69 65 78 32 30 49  2b 46 48 4f 36 55 44 67    ibiex20I+FHO6UDg
00e0   76 32 77 37 30 56 53 38  6e 36 78 58 37 79 4b 54    v2w70VS8n6xX7yKT
00f0   44 2f 75 57 35 64 34 72  56 77 4a 46 55 74 2b 4d    D/uW5d4rVwJFUt+M
```

Exercise
Scenario 1: Port Scan Detection

1. Threat Simulation

To investigate a malicious port scanning activity, it is essential that I apply filters to the captured packets. Most communications used ipv6 address. However, since clowdshark only supports filtering with ipv4, I will filter based on the protocol used. By using the protocol ladder button, I will be able to determine the number of TCP packets (which was 2968), the source of each request, and visualize all the communications that took place between IP addresses. From the capture, I saw that most TCP requests (a total of 2951) originated from an ipv6 address to another ipv6 address on different ports within a period of 2 minutes and 27 seconds. But most of these connection requests were blocked (either by a firewall or the ports were closed). By establishing the number of port requests from a source IP address in each period, I will be able to detect a port scan and take the necessary measures to address the threat. I will use the threat assessment and protocol ladder dashboard to assess the severity levels, the number of frames per each protocol and IP address, the locations of each request, and generate additional packet insights. I will assign a low criticality level. The firewall signatures and threat intel will be updated, and an incident report will be written after the analysis.

2. Business Impacts

Port scan techniques are used to learn more about a network and identify vulnerable ports that can be used as attack vectors. If such weaknesses are not resolved on time, attackers can send massive port scans which can lead to a Dos attack and disrupt business activities. Short-term risks are disruption of business activities and loss of productivity. Long-term risks are financial loss from DoS attacks and loss of business revenue.

3. Remediation.

To prevent attackers from conducting port scanning on my network, I will employ strong firewall protection and define ACLs to block any request from the identified source IP address, conduct regular vulnerability scans, and close all unused ports.

Worms – Slammer

1. Threat Simulation

Patterns or features will be used to perform the analysis. Slammer is very robust and uses UDP to propagate very fast and the program payload is 376 bytes. After affecting a computer that has Microsoft SQL Server 2000 running on it, it generates a random IP address and a source port and tries to replicate itself to other devices by repeatedly sending UDP packets to a randomly selected IP address with UDP port 1434 as the destination port. As such, I will set a display filter to retrieve all packets that have UDP port 1434, analyze the UDP headers for packets with a payload size of 376 bytes, and examine the binary code in the payload for buffer overflow exploitation. Since the slammer generates random source IP addresses to send UDP packets to random destination addresses, I will trace all unique source and destination addresses to learn about the propagation rate. From the capture, 9 UDP packets were sent by 9 unique IP addresses to the same destination IP address on UDP port 1434 with a payload of 376 bytes. Worms pose a great threat, as such, I will assign a high severity level. The protocol conversation and protocol hierarchy panels will be used to monitor conversations between nodes and the number of packets communicated per protocol. An incident response report will be written to document the investigation and the threat intelligence will equally be updated.

2. Business Impacts

The slammer worm generates massive packets that can overload servers. Short-term risks are; it slows network and server performance, causes a denial of service, and disrupts business operations. Huge financial losses from downtime and expensive business recovery are long-term risks.

3. Remediation

The address the incident, I will implement both ingress and egress filters on the company's firewalls and routers to block outbound and inbound UDP packets with 1434 as the destination port. This will prevent infected packets from leaving or entering the network. I will also harden the company's systems to block all unsolicited services and unused ports like port 1434.

Command and Control (C2) – Zeus

1. Threat Simulation

To analyze the incident, I will look out for patterns and behaviors for any beacon activity – connections between two nodes at regular intervals. Compromised host devices communicate with the C2 server for matching orders to be executed and both parties communicate consistently. I will filter the packets using source and destination IPs to analyze the traffic between such addresses. Regular connections will indicate a C2 session. From the packet capture, there were multiple ACK flags without initial SYN flags. Most HTTP and TCP packets had the same payload size of 1460 bytes. 159 connections at a 5-second interval, 159 at a 10-second interval, and 159 at a 15-second interval. This pattern indicates that IP 192.168.99.53 and IP 67.207.93.135 were consistently communicating. I will an in-built graph dashboard to visualize the traffic between the two IP addresses and detect the connection interval. Zeus poses a great threat to the business and will be assigned a high criticality level. An incident response report will be written to document the incident and update the business' threat intelligence.

2. Business Impacts

The Zeus worm impacts businesses based on its payload. Short-term risks include unauthorized access to business resources, stealing sensitive data, disrupting business activities, causing DoS attacks, and huge financial loss. Zeus worm attacks can have long-term impacts on the business. These include shutting down the business network, legal actions against the business, damaging the company's brand, and opening the business to ransomware attacks.

3. Remediation

The remediation process will include both human and technological measures. Educate employees on online safety and security practices, conduct regular beacon analysis, regularly patch computing systems, and update software in a timely fashion.

References

Boutin, P (2003, July 1). Wired! Retrieved February 10, 2023 from https://www.wired.com/2003/07/slammer/

Brenton, C (2018, August 6). Beacon Analysis – The Key to Cyber Threat Hunting. Retrieved February 10, 2023 from https://www.activecountermeasures.com/blog-beacon-analysis-the-key-to-cyber-threat-hunting/

Chew, K. (2020, June 23). Malware of the Day – Zeus . Retrieved February 12, 2023 from https://www.activecountermeasures.com/malware-of-the-day-zeus/

Geeksforgeeks (2022, July 31). Slammer Worm in Information Security. Retrieved February 11, 2023 from https://www.geeksforgeeks.org/slammer-worm-in-information-security/

Huang, D (2003). Attack of slammer worm – A practical case study. Sans Institute.

Paloalto (n.d). Command and Control Explained. Retrieved February 12, 2023, from https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained.

Ring, M., Landes, D., & Hotho, A. (2018). Detection of slow port scans in flow-based network traffic. *PloS one*, *13*(9), e0204507. https://doi.org/10.1371/journal.pone.0204507

Sengupta, S (2022, September 12). What is port scan attack? Retrieved February 10, 2023 from https://crashtest-security.com/port-scan-attacks/