FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

INTRUSION DETECTION & NETWORK FORENSICS (CISC 6680)

Lab: Investigating Network Attacks

Name: Gopi Gor

FDIN: A21370441

Contents

Port Scan Detection

As an SOC analyst, to analyse port scan detection, I would first look at specific filters and protocols used in the PCAP files of Cloudshark. I would check the source and destination IPv4 and IPv6 addresses, and find out the details of the IP address. Then, I would look into the tcp filter to understand the sequences that the source is sending to the destination. I would look for incomplete SYN requests, which indicate a closed port or firewall. Furthermore, the **Len** factor can tell us more about if there is a payload or not. Sequence of port numbers could denote a stealth scan for incomplete SYN requests and thus I would examine each packet to investigate the TCP ports, UDP ports, length, src and destination IP and RST packets. A constant RST packet could mean the sender is trying to reset the connection in order to send malicious packets. The criticality I would assign to this alert would be **high** because the open ports scanning could reveal a lot of information to the attacker and knowledge about open ports could lead to unauthorized entry into the network. The dashboard most useful for this would be one that shows incomplete SYN requests, continuous RST requests and Len >0 related dashboards. Mainly, network activity dashboards would be the most useful.

The business impacts for this kind of alert would be that the attacker gets entry into the network and launches malicious payloads, thereby harming the complete organization or disruption of all services. The short-term risks can be security breaches if vulnerabilities are discovered after the port scanning. Long-term risks could be that an APT could be running for a long time without being noticed and thus can be ready to launch a big attack on the organization thereby completely exfiltrating data or exploiting vulnerabilities over a very long time.

To remediate this kind of alert, the first thing is place is the incident response plan, and the network access to be limited only to certain resources in the network. Furthermore, there has to be a team deployed for constant patch management in the network side to keep fixing vulnerabilities incase an attacker gets access to network ports and traffic.

Worms – Slammer

As an SOC Analyst, to investigate the alert for worms, specifically that of the Slammer, the Slammer worm tries to exploit vulnerabilities in the MS SQL database server and thus, I would first filter the PCAP to look for all UDP packets because slammer uses UDP packets for transmission. Then I would look for the source and destination IP, which would majorly have different sources but a common destination IP. After this, I would analyse the UDP packets and try to find a pattern with the payload, which would be 376 bytes, being the slammer payload size. Additionally, I would look for destination ports where the port is 1434, which slammer uses to exploit the vulnerability on the MS SQL server. The criticality I would assign to this is **high** because the worms have a tendency to spread themselves, so once they are in the system, it is more likely to spread very quickly. As for a dashboard, I would use dashboards which show UDP requests and packet details like destination ports, payload length and destination IP addresses.

The business implications of a worm in a network could be vastly different because they could cause major disruptions to the services being provided by the server, thereby resulting in loss of productivity of the server. The short-term risks could be service unavailability and DDoS resulting in complete network congestion during the early stages. Long-term risks include persistent security risks and a lot of challenges with regards to business continuity. The server and domains can be completed banned, and there could be compliance-based charges imposed on the organization too.

To remediate this alert type, the affected systems can be made isolated systems and then they can investigate forensically to understand the cause of the attack. Moreover, security patches could be based on the analysis and investigations made. The antivirus and security softwares should be updated and policies could be reinforced to understand all different tactics the slammer has used to infiltrate the network. Lastly, all compromised accounts, PC’s and users may need to be newly created or updated in order to avoid future events like these.

Command & Control – Zeus

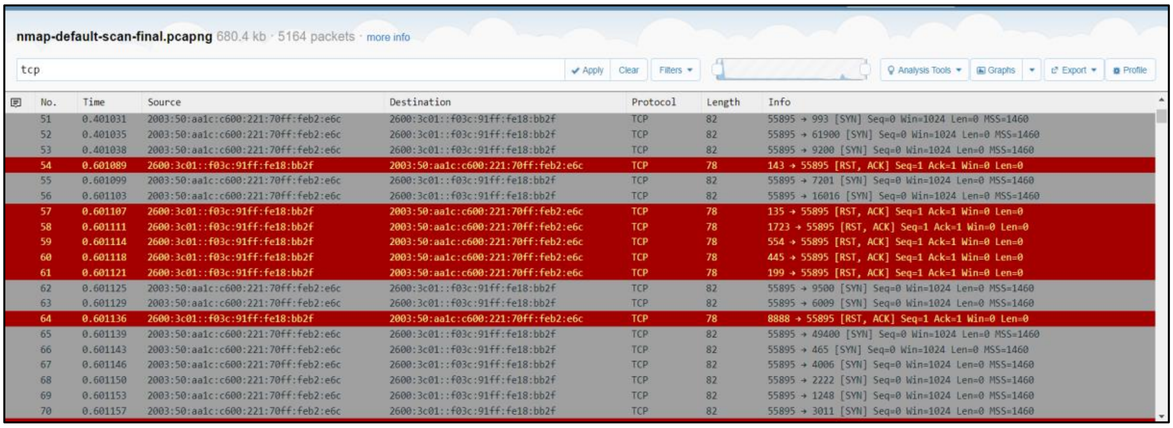
As an SOC Analyst, I would first look for investigation in the network traffic and irregular spikes in network traffic. Zeus botnets use a lot of HTTP and HTTPS traffic which may or may not have random user agent strings. I would also try to try to understand all random IP addresses an investigation on those IP addresses to understand the legitimacy of those IPs. The DNS traffic would show quite a lot of domain names if a Zeus botnet has been employed in the network. If we check the ports, there would be multiple random ports, where normal services don't run and they would be very high numbered ports. Additionally, a high payload in the len part could mean there is a malicious payload being injected into the system. The criticality I would assign to this alert type would be **high** due to the multiple botnets that can be employed if one part of the network gets filtrated. The dashboards that could be useful for investigating this alert type could be protocol-based dashboards like payloads, ssh, tls or https requests, packet analysis filters and timeline dashboards.

The Zeus botnet is designed to steal all kinds of sensitive data, so it could cost a lot of personal information to the organization along with financial loss. The short-term risks could be operational risk and service disruptions, along with stealing of personal data. In long-term risks, the data that was exfiltrated could be used to launch impersonation attacks or selling of data on the dark web. It could also cause loss of a competitive advantage for the organization.

For quick and long-term remediation, the network access should be immediately disabled to avoid any further botnets being created inside the network. The affected systems need to be completed wipes and sanitized to remove all the viruses that may have entered into the network. After this, network segmentation can be applied to keep all critical and sensitive servers on a local server to avoid any connections to the outside world. Lastly, continuous network monitoring needs to be implemented.

Appendix

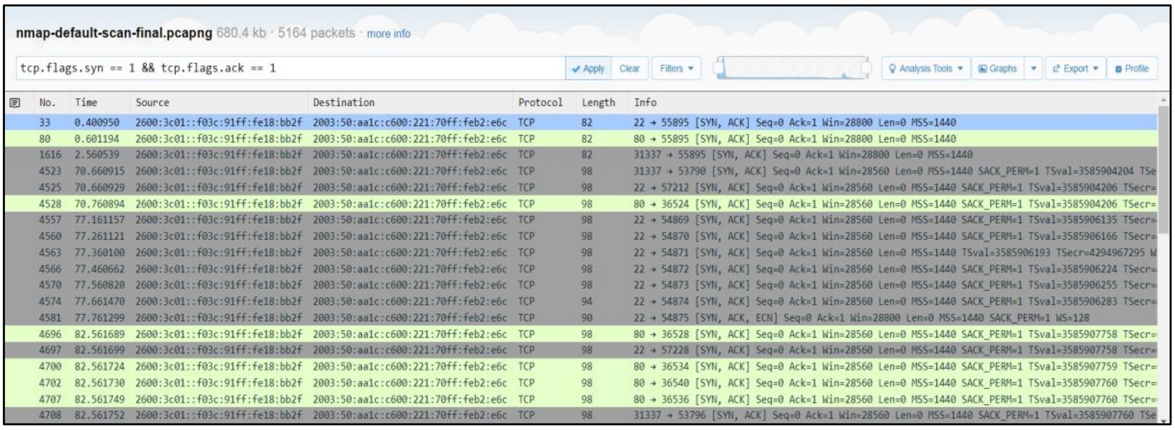
1. Port Scanning


nmap-default-scan-final.pcapng 680.4 kb · 5164 packets · more info
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

tcp

No.	Time	Source	Destination	Protocol	Length	Info
51	0.401031	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	0.401035	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 61900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	0.401038	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 9200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	0.601089	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	143 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	0.601099	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 7201 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	0.601103	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 16016 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
57	0.601107	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	135 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	0.601111	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	1723 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	0.601114	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	554 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	0.601118	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	445 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	0.601121	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	199 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	0.601125	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 9500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
63	0.601129	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 6009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
64	0.601136	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	78	8888 → 55895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	0.601139	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 49400 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	0.601143	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 465 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
67	0.601146	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
68	0.601150	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 2222 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
69	0.601153	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 1248 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
70	0.601157	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	TCP	82	55895 → 3011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

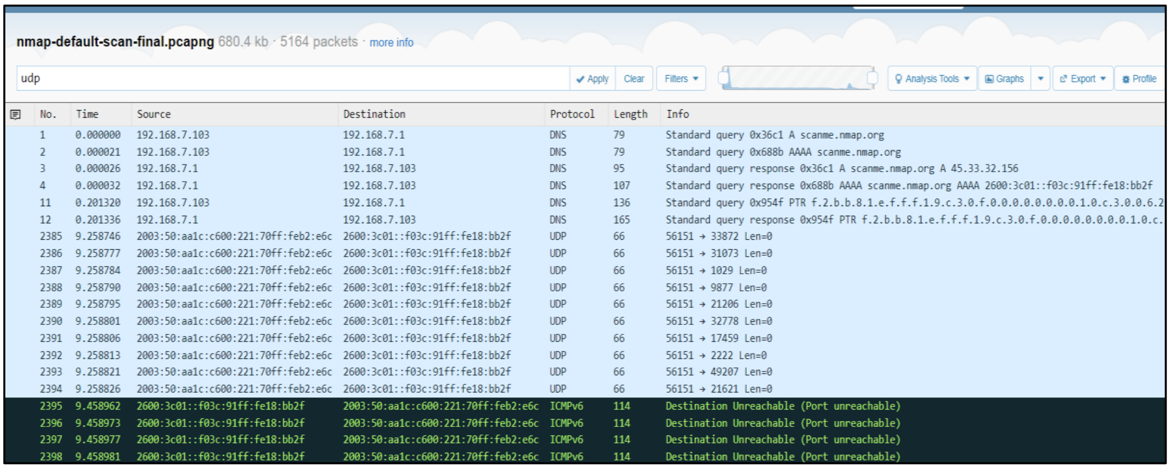
Fig. 1. TCP to notice open ports from destination.


nmap-default-scan-final.pcapng 680.4 kb · 5164 packets · more info
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

tcp.flags.syn == 1 && tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
33	0.400950	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	82	22 → 55895 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440
80	0.601194	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	82	80 → 55895 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440
1616	2.560539	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	82	31337 → 55895 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440
4523	70.660915	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	31337 → 53790 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585904204 TSe
4525	70.660929	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 57212 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585904206 TSecr=
4528	70.760894	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	80 → 36524 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585904206 TSecr=
4557	77.161157	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 54869 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585906135 TSecr=
4560	77.261121	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 54870 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585906166 TSecr=
4563	77.360100	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 54871 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 TSval=3585906193 TSecr=4294967295 W
4566	77.460662	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 54872 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585906224 TSecr=
4570	77.560820	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 54873 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585906255 TSecr=
4574	77.661470	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	94	22 → 54874 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585906283 TSecr=
4581	77.761299	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	90	22 → 54875 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440 SACK_PERM=1 WS=128
4696	82.561689	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	80 → 36528 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907758 TSecr=
4697	82.561699	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	22 → 57228 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907758 TSecr=
4700	82.561724	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	80 → 36534 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907759 TSecr=
4702	82.561730	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	80 → 36540 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907760 TSecr=
4707	82.561749	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	80 → 36536 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907760 TSecr=
4708	82.561752	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	TCP	98	31337 → 53796 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=3585907760 TSe

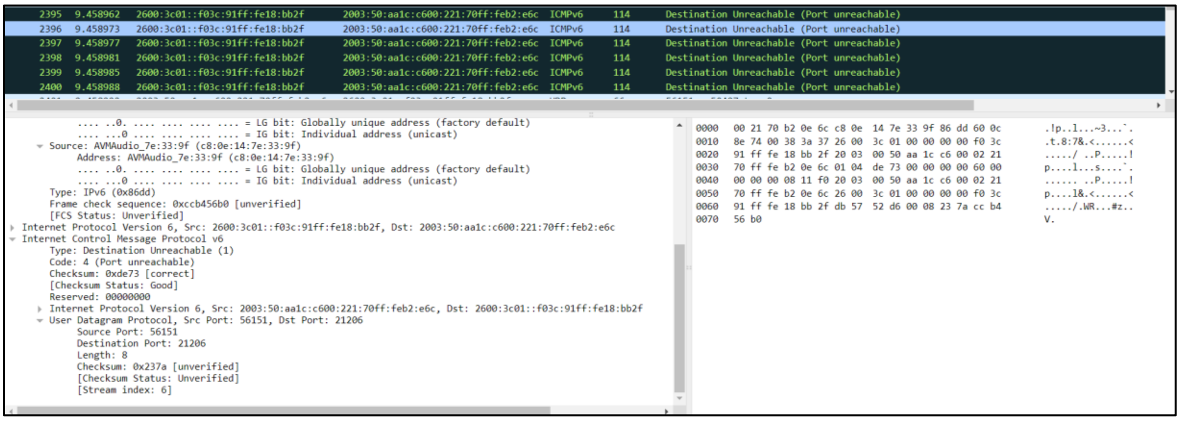
Fig. 2. TCP to set ack and syn flags as 1 to show complete connections


nmap-default-scan-final.pcapng 680.4 kb · 5164 packets · more info
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.7.103	192.168.7.1	DNS	79	Standard query 0x36c1 A scanme.nmap.org
2	0.000021	192.168.7.103	192.168.7.1	DNS	79	Standard query 0x688b AAAA scanme.nmap.org
3	0.000026	192.168.7.1	192.168.7.103	DNS	95	Standard query response 0x36c1 A scanme.nmap.org A 45.33.32.156
4	0.000032	192.168.7.1	192.168.7.103	DNS	107	Standard query response 0x688b AAAA scanme.nmap.org AAAA 2600:3c01::f03c:91ff:fe18:bb2f
11	0.201320	192.168.7.103	192.168.7.1	DNS	136	Standard query 0x954f PTR f.2.b.b.8.1.e.f.f.f.1.9.c.3.0.f.0.0.0.0.0.0.0.0.1.0.c.3.0.0.6.2
12	0.201336	192.168.7.1	192.168.7.103	DNS	165	Standard query response 0x954f PTR f.2.b.b.8.1.e.f.f.f.1.9.c.3.0.f.0.0.0.0.0.0.0.0.1.0.c.
2385	9.258746	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 33872 Len=0
2386	9.258777	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 31073 Len=0
2387	9.258784	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 1029 Len=0
2388	9.258790	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 9877 Len=0
2389	9.258795	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 21206 Len=0
2390	9.258801	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 32778 Len=0
2391	9.258806	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 17459 Len=0
2392	9.258813	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 2222 Len=0
2393	9.258821	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 49207 Len=0
2394	9.258826	2003:50:aa1c:c600:221:70ff:feb2:e6c	2600:3c01::f03c:91ff:fe18:bb2f	UDP	66	56151 → 21621 Len=0
2395	9.458962	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	ICMPv6	114	Destination Unreachable (Port unreachable)
2396	9.458973	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	ICMPv6	114	Destination Unreachable (Port unreachable)
2397	9.458977	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	ICMPv6	114	Destination Unreachable (Port unreachable)
2398	9.458981	2600:3c01::f03c:91ff:fe18:bb2f	2003:50:aa1c:c600:221:70ff:feb2:e6c	ICMPv6	114	Destination Unreachable (Port unreachable)

Fig. 3. UDP to check to check if ports are open now.

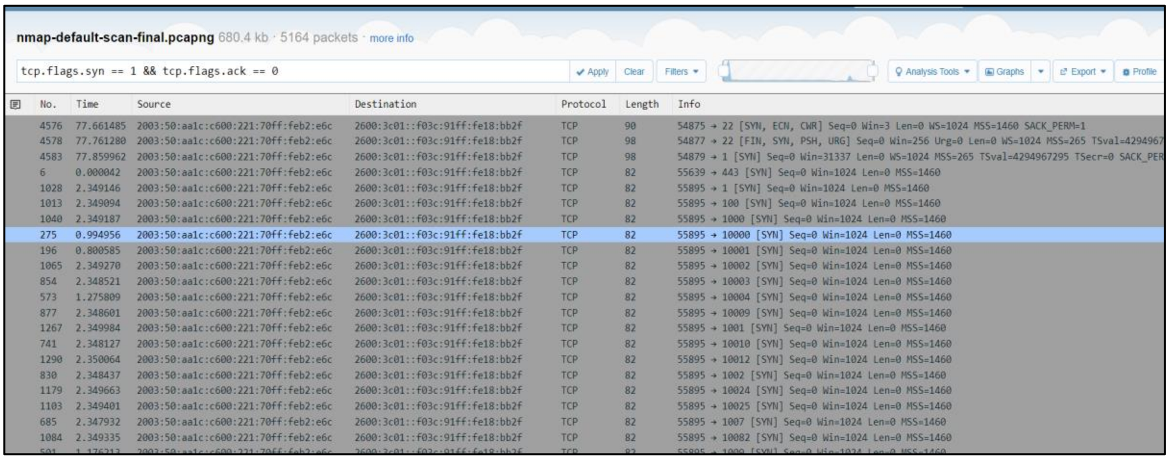


```
2395  9.458962  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
2396  9.458973  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
2397  9.458977  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
2398  9.458981  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
2399  9.458985  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
2400  9.458988  2600:3c01::f03c:91ff:fe18:bb2f  2003:50:aa1c:c600:221:70ff:feb2:e6c  ICMPv6  114  Destination Unreachable (Port unreachable)
```

```
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: AVMAudio_7e:33:9f (c8:0e:14:7e:33:9f)
        Address: AVMAudio_7e:33:9f (c8:0e:14:7e:33:9f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    Frame check sequence: 0xccb456b0 [unverified]
    [FCS Status: Unverified]
Internet Protocol Version 6, Src: 2600:3c01::f03c:91ff:fe18:bb2f, Dst: 2003:50:aa1c:c600:221:70ff:feb2:e6c
Internet Control Message Protocol v6
    Type: Destination Unreachable (1)
    Code: 4 (Port unreachable)
    Checksum: 0xde73 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Internet Protocol Version 6, Src: 2003:50:aa1c:c600:221:70ff:feb2:e6c, Dst: 2600:3c01::f03c:91ff:fe18:bb2f
    User Datagram Protocol, Src Port: 56151, Dst Port: 21206
        Source Port: 56151
        Destination Port: 21206
        Length: 8
        Checksum: 0x237a [unverified]
        [Checksum Status: Unverified]
        [Stream index: 6]
```

```
0000  00 21 70 b2 0e 6c c8 0e  14 7e 33 9f 86 dd 60 0c   .!p..l...~3...`.
0010  8e 74 00 38 3a 37 26 00  3c 01 00 00 00 00 f0 3c   .t.8:7&.<......<
0020  91 ff fe 18 bb 2f 20 03  00 50 aa 1c c6 00 02 21   ...../ ..P.....!
0030  70 ff fe b2 0e 6c 01 04  de 73 00 00 00 00 60 00   p....l...s....`.
0040  00 00 00 08 11 f0 20 03  00 50 aa 1c c6 00 02 21   ...... ..P.....!
0050  70 ff fe b2 0e 6c 26 00  3c 01 00 00 00 00 f0 3c   p....l&.<......<
0060  91 ff fe 18 bb 2f db 57  52 d6 00 08 23 7a cc b4   ...../.WR...#z..
0070  56 b0                                              V.
```

Fig. 4. UDP packets to see that ports are not reachable and same src and dest.IP.



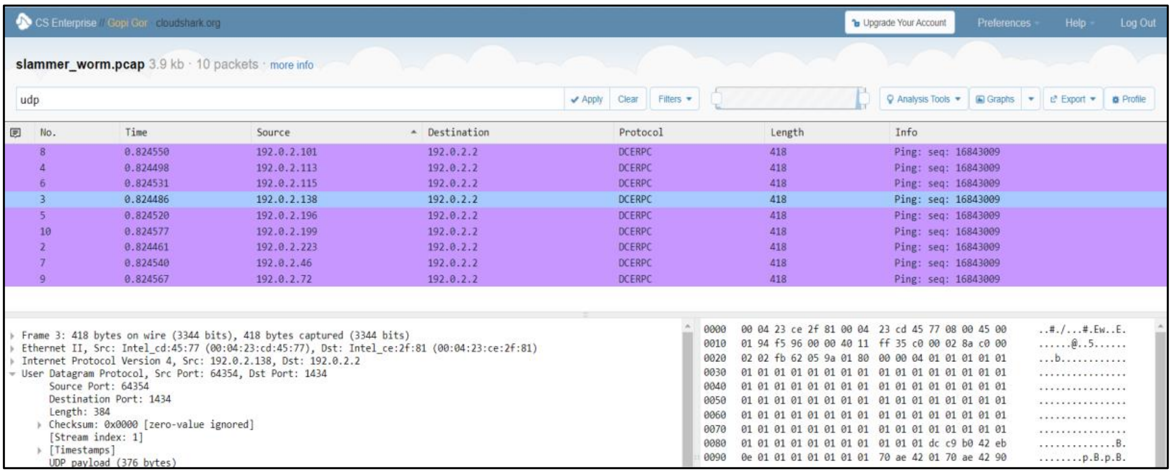
nmap-default-scan-final.pcapng 680.4 kb · 5164 packets · more info

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

```
No.   Time       Source                               Destination                     Protocol  Length  Info
4576  77.661485  2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       90      54875 → 22 [SYN, ECN, CWR] Seq=0 Win=3 Len=0 WS=1024 MSS=1460 SACK_PERM=1
4578  77.761280  2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       98      54877 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967
4583  77.859962  2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       98      54879 → 1 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PER
6     0.000042   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55639 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1028  2.349146   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1013  2.349094   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1040  2.349187   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 1000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
275   0.994956   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
196   0.800585   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1065  2.349270   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
854   2.348521   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
573   1.275809   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
877   2.348601   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1267  2.349984   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 1001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
741   2.348127   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1290  2.350064   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
830   2.348437   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1179  2.349663   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1103  2.349401   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
685   2.347932   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1084  2.349335   2003:50:aa1c:c600:221:70ff:feb2:e6c  2600:3c01::f03c:91ff:fe18:bb2f  TCP       82      55895 → 10082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Fig. 5. TCP flags to set syn to 1 and ack to 0 for incomplete transmission

2. Worms - Slammer



slammer_worm.pcap 3.9 kb · 10 packets · more info

```
udp
```

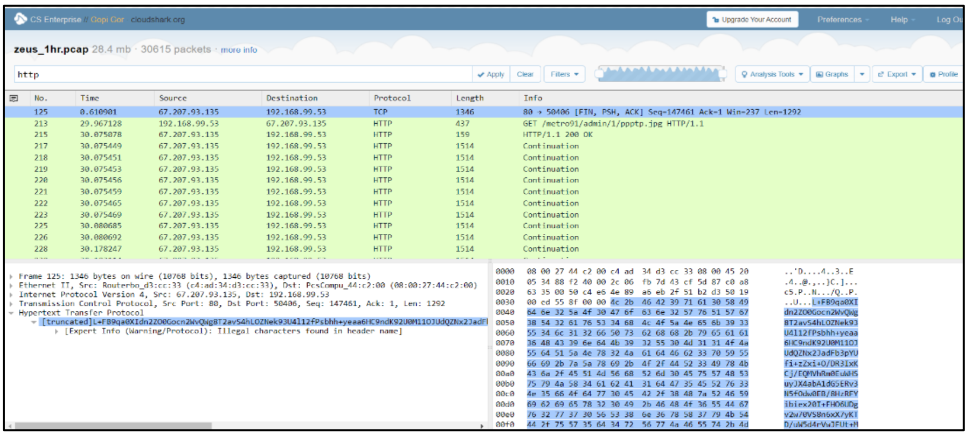
```
No.  Time      Source       Destination  Protocol  Length  Info
8    0.824550  192.0.2.101  192.0.2.2    DCERPC    418     Ping: seq: 16843009
4    0.824498  192.0.2.113  192.0.2.2    DCERPC    418     Ping: seq: 16843009
6    0.824531  192.0.2.115  192.0.2.2    DCERPC    418     Ping: seq: 16843009
3    0.824486  192.0.2.138  192.0.2.2    DCERPC    418     Ping: seq: 16843009
5    0.824520  192.0.2.196  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
2    0.824461  192.0.2.223  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
9    0.824567  192.0.2.72   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:81)
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)
```

```
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.
```

Fig. 6. UDP showing dest. port of 1434 to exploit MS SQL DB vulnerabilities

3. C&C – Zeus Botnet



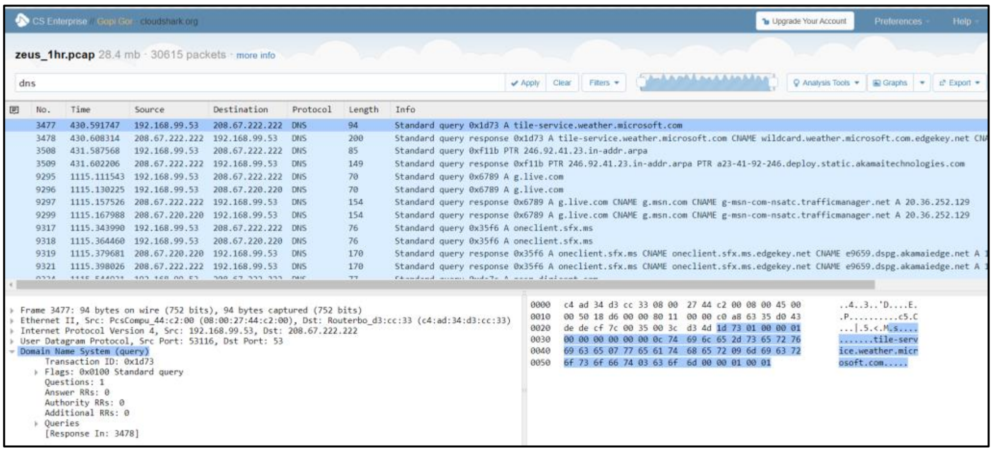
```
http

No.   Time        Source          Destination     Protocol  Length  Info
125   0.610901    67.207.93.135   192.168.99.53   TCP       1346    80 → 50406 [FIN, PSH, ACK] Seq=147461 Ack=1 Win=237 Len=1292
213   29.967128   192.168.99.53   67.207.93.135   HTTP      437     GET /metro91/admin/1/ppptp.jpg HTTP/1.1
215   30.075078   67.207.93.135   192.168.99.53   HTTP      159     HTTP/1.1 200 OK
217   30.075449   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
218   30.075451   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
219   30.075453   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
220   30.075456   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
221   30.075459   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
222   30.075465   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
223   30.075469   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
225   30.080685   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
226   30.080692   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
228   30.178247   67.207.93.135   192.168.99.53   HTTP      1514    Continuation
```

```
▸ Frame 125: 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 (08:00:27:44:c2:00)
▸ Internet Protocol Version 4, Src: 67.207.93.135, Dst: 192.168.99.53
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 50406, Seq: 147461, Ack: 1, Len: 1292
▾ Hypertext Transfer Protocol
    ▾ [truncated]L+FB9qa0XIdn2ZO0Gocn2WvQWg8T2avS4hLOZNek93U4l12fPsbhh+yeaa6HC9ndK92U0M11OJUdQZNx2JadFl
        ▸ [Expert Info (Warning/Protocol): Illegal characters found in header name]
```

```
0000  08 00 27 44 c2 00 c4 ad  34 d3 cc 33 08 00 45 20   ..'D....4..3..E
0010  05 34 88 f2 40 00 2c 06  fb 7d 43 cf 5d 87 c0 a8   .4..@.,..}C.]...
0020  63 35 00 50 c4 e6 4e 89  a6 eb 2f 51 b2 d3 50 19   c5.P..N.../Q..P.
0030  00 ed 55 8f 00 00 4c 2b  46 42 39 71 61 30 58 49   ..U...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
```

Fig. 7. UDP to check to check if ports are open now.


CS Enterprise // Gopi Gor cloudshark.org
Upgrade Your Account
Preferences
Help
zeus_1hr.pcap 28.4 mb · 30615 packets · more info
Apply
Clear
Filters
Analysis Tools
Graphs
Export

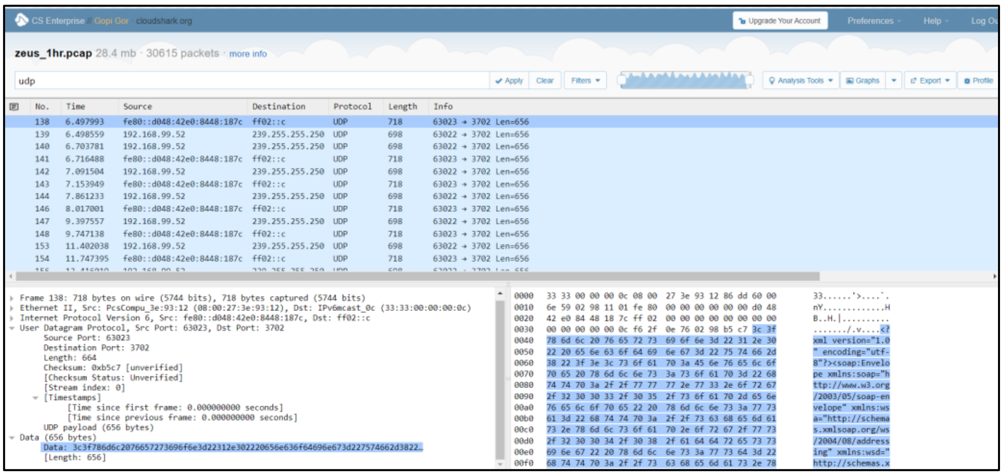
```
dns

No.   Time         Source          Destination     Protocol  Length  Info
3477  430.591747   192.168.99.53   208.67.222.222  DNS       94      Standard query 0x1d73 A tile-service.weather.microsoft.com
3478  430.608314   208.67.222.222  192.168.99.53   DNS       200     Standard query response 0x1d73 A tile-service.weather.microsoft.com CNAME wildcard.weather.microsoft.com.edgekey.net CNA
3508  431.587568   192.168.99.53   208.67.222.222  DNS       85      Standard query 0xf11b PTR 246.92.41.23.in-addr.arpa
3509  431.602206   208.67.222.222  192.168.99.53   DNS       149     Standard query response 0xf11b PTR 246.92.41.23.in-addr.arpa PTR a23-41-92-246.deploy.static.akamaitechnologies.com
9295  1115.111543  192.168.99.53   208.67.222.222  DNS       70      Standard query 0x6789 A g.live.com
9296  1115.130225  192.168.99.53   208.67.220.220  DNS       70      Standard query 0x6789 A g.live.com
9297  1115.157526  208.67.222.222  192.168.99.53   DNS       154     Standard query response 0x6789 A g.live.com CNAME g.msn.com CNAME g-msn-com-nsatc.trafficmanager.net A 20.36.252.129
9299  1115.167988  208.67.220.220  192.168.99.53   DNS       154     Standard query response 0x6789 A g.live.com CNAME g.msn.com CNAME g-msn-com-nsatc.trafficmanager.net A 20.36.252.129
9317  1115.343990  192.168.99.53   208.67.222.222  DNS       76      Standard query 0x35f6 A oneclient.sfx.ms
9318  1115.364460  192.168.99.53   208.67.220.220  DNS       76      Standard query 0x35f6 A oneclient.sfx.ms
9319  1115.379681  208.67.220.220  192.168.99.53   DNS       170     Standard query response 0x35f6 A oneclient.sfx.ms CNAME oneclient.sfx.ms.edgekey.net CNAME e9659.dspg.akamaiedge.net A 1
9321  1115.398026  208.67.222.222  192.168.99.53   DNS       170     Standard query response 0x35f6 A oneclient.sfx.ms CNAME oneclient.sfx.ms.edgekey.net CNAME e9659.dspg.akamaiedge.net A 1
```

```
▸ Frame 3477: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
▸ Ethernet II, Src: PcsCompu_44:c2:00 (08:00:27:44:c2:00), Dst: Routerbo_d3:cc:33 (c4:ad:34:d3:cc:33)
▸ Internet Protocol Version 4, Src: 192.168.99.53, Dst: 208.67.222.222
▸ User Datagram Protocol, Src Port: 53116, Dst Port: 53
▾ Domain Name System (query)
      Transaction ID: 0x1d73
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    ▸ Queries
      [Response In: 3478]
```

```
0000  c4 ad 34 d3 cc 33 08 00  27 44 c2 00 08 00 45 00   ..4..3..'D....E.
0010  00 50 18 d6 00 00 80 11  00 00 c0 a8 63 35 d0 43   .P..........c5.C
0020  de de cf 7c 00 35 00 3c  d3 4d 1d 73 01 00 00 01   ...|.5.<.M.s....
0030  00 00 00 00 00 00 0c 74  69 6c 65 2d 73 65 72 76   .......tile-serv
0040  69 63 65 07 77 65 61 74  68 65 72 09 6d 69 63 72   ice.weather.micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 01 00 01         osoft.com.....
```

Fig. 8. UDP to check to check if ports are open now.



```
udp

No.   Time        Source                     Destination      Protocol  Length  Info
138   6.497993    fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
139   6.498559    192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
140   6.703781    192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
141   6.716488    fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
142   7.091504    192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
143   7.153949    fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
144   7.861233    192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
146   8.017001    fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
147   9.397557    192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
148   9.747138    fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
153   11.402038   192.168.99.52              239.255.255.250  UDP       698     63022 → 3702 Len=656
154   11.747395   fe80::d048:42e0:8448:187c  ff02::c          UDP       718     63023 → 3702 Len=656
```

```
▸ Frame 138: 718 bytes on wire (5744 bits), 718 bytes captured (5744 bits)
▸ Ethernet II, Src: PcsCompu_3e:93:12 (08:00:27:3e:93:12), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
▸ Internet Protocol Version 6, Src: fe80::d048:42e0:8448:187c, Dst: ff02::c
▾ User Datagram Protocol, Src Port: 63023, Dst Port: 3702
      Source Port: 63023
      Destination Port: 3702
      Length: 664
      Checksum: 0xb5c7 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    ▾ [Timestamps]
          [Time since first frame: 0.000000000 seconds]
          [Time since previous frame: 0.000000000 seconds]
      UDP payload (656 bytes)
▾ Data (656 bytes)
      Data: 3c3f786d6c2076657273696f6e3d22312e302220656e636f64696e673d227574662d3822…
      [Length: 656]
```

```
0000  33 33 00 00 00 0c 08 00  27 3e 93 12 86 dd 60 00   33......'>....`.
0010  6e 59 02 98 11 01 fe 80  00 00 00 00 00 00 d0 48   nY.............H
0020  42 e0 84 48 18 7c ff 02  00 00 00 00 00 00 00 00   B..H.|..........
0030  00 00 00 00 00 0c f6 2f  0e 76 02 98 b5 c7 3c 3f   ......./.v....<?
0040  78 6d 6c 20 76 65 72 73  69 6f 6e 3d 22 31 2e 30   xml version="1.0
0050  22 20 65 6e 63 6f 64 69  6e 67 3d 22 75 74 66 2d   " encoding="utf-
0060  38 22 3f 3e 3c 73 6f 61  70 3a 45 6e 76 65 6c 6f   8"?><soap:Envelo
0070  70 65 20 78 6d 6c 6e 73  3a 73 6f 61 70 3d 22 68   pe xmlns:soap="h
0080  74 74 70 3a 2f 2f 77 77  77 2e 77 33 2e 6f 72 67   ttp://www.w3.org
0090  2f 32 30 30 33 2f 30 35  2f 73 6f 61 70 2d 65 6e   /2003/05/soap-en
00a0  76 65 6c 6f 70 65 22 20  78 6d 6c 6e 73 3a 77 73   velope" xmlns:ws
00b0  61 3d 22 68 74 74 70 3a  2f 2f 73 63 68 65 6d 61   a="http://schema
00c0  73 2e 78 6d 6c 73 6f 61  70 2e 6f 72 67 2f 77 73   s.xmlsoap.org/ws
00d0  2f 32 30 30 34 2f 30 38  2f 61 64 64 72 65 73 73   /2004/08/address
00e0  69 6e 67 22 20 78 6d 6c  6e 73 3a 77 73 64 3d 22   ing" xmlns:wsd="
00f0  68 74 74 70 3a 2f 2f 73  63 68 65 6d 61 73 2e 78   http://schemas.x
```

Fig. 9. UDP to check to check if ports are open now.

References

1. https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/
2. https://cloud.ibm.com/docs/codeengine?topic=codeengine-ts-app-toomanyports
3. https://www.geeksforgeeks.org/slammer-worm-in-information-security/
4. https://www.csoonline.com/article/566849/sql-slammer-16-years-later-four-modern-day-scenarios-that-could-be-worse.html
5. https://security.stackexchange.com/questions/59418/how-to-detect-the-so-called-undetectable-gameover-zeus