Global Information Assurance Certification Paper

GIAC Level Two Certification Practical

Intrusion Detection Curriculum

Susan Tanoe

September 15, 2000

Assignment 1

Capture 1

	Date/Time	Src IP	Dest IP
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.16
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.17
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.208
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223
High	2000/08/25 18:11:16.00	210.67.172.9	1.76.102.223

1. Source of trace
    a. My network
2. Detect was generated by:

a. Network Intrusion Detection System

3. Probability the source address was spoofed

   Low, the IP address is registered to Chinfon Life Insurance Co., LTD, a corporation in Taiwan. Resolved through APNIC.net.

4. Description of attack:
   a. Attacker seems to be utilizing an automated tool such as a script kiddie. The fact that the IPs weren't randomized shows that it is a relatively crude tool and the time sequence shows that the tools are automated.
   b. Normally in this type of attack you expect to find that the source is trolling for Trojans but with without the source and destination port information listed one cannot make this assumption straight of the bat.
   c. Real Secure reported this attack as an IP HalfScan

5. Attack mechanism:
   a. While not shown on the report, further investigation of the event showed that the source and destination port was POP. Unfortunately it does not state whether it was POP2 or POP3.
   b. Source hit each destination 26 times and scanned from IP 1.76.102.16 through 1.76.102.31 and again from IP 1.76.102.208 to 1.76.102.223 but only on the specific destination port. Scan was also not randomized. This also leads me to conclude that alleged perpetrator was attempting to do some reconnaissance and trying to see if network was subnetted as well as checking to see it any of our hosts was a POP server or client. Interestingly they started at 1.76.102.16 and not 1.76.102.0.

6. Correlation:

   This was a reconnaissance attack as described in the SANS 2000 Intrusion Detection seminar.

7. Evidence of active targeting:

   This attack was generated against a specific port, not necessarily against a specific host, and may have been looking to probe the vulnerabilities of the POP service.

8. Severity:
   a. (critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (3 + 3) - (0 + 0) = 6

9. Defensive recommendation:

   Attack was not seen by firewall. Verify that appropriate ports are blocked on firewall. Some systems enable these ports for backward compatibility to old mail systems.

10. Multiple choice test question:
    This trace is best described as a:

    a) DNS Zone Transfer
    b) DNS Inverse Query

c) DNS Version Scan
d) Subnet scan

Answer: d

Capture 2

Sep 2 14:50:02.282 kernel: 120 ICMP Info: Not sending ICMP Unreachable in response to non-information ICMP (POS3-2.hsa1.sdg1.level3.net[209.245.56.13]->1.253.5.62: Protocol=ICMP[Unreachable (host)] {Inner: 1.253.5.62->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 44301->12489}) received on interface 1.253.4.1
Sep 2 15:26:07.955 kernel: 120 ICMP Info: Not sending ICMP Unreachable in response to non-information ICMP (pb-nap.eni.net[1.32.128.39]->1.253.2.52: Protocol=ICMP[Unreachable (host)] {Inner: 1.253.2.52->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 1611->7024}) received on interface 1.253.4.1
Sep 2 15:52:56.268 kernel: 120 ICMP Info: Not sending ICMP Unreachable in response to non-information ICMP (loopback1.hsipaccess2.Seattle1.Level3.net[209.244.2.23]->1.253.5.86: Protocol=ICMP[Unreachable (host)] {Inner: 1.253.5.86->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 48137->17684}) received on interface 1.253.4.1
Sep 2 15:53:27.755 kernel: 120 ICMP Info: Not sending ICMP Unreachable in response to non-information ICMP (above-level3.sea.above.net[208.185.175.105]->1.253.5.12: Protocol=ICMP[Unreachable (host)] {Inner: 1.253.5.12->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 39965->6563}) received on interface 1.253.4.1

1. Source of trace
   a. My network
2. Detect was generated by:
   a. Raptor Firewall Logs
   b. Explanation of fields:

      Sep 2 15:53:27.755 **[Timestamp],** kernel **[Device name],** 120 ICMP **[service error],** Info: Not sending ICMP Unreachable in response to non-information ICMP **[Informational field]** above-level3.sea.above.net[208.185.175.105 **[source name, IP address],** 1.253.5.12 **[destination IP address],** Protocol=ICMP **[protocol]**
3. Probability the source address was spoofed

   Probability – high. Source is doing reconnaissance.
4. Description of attack:
   a. Source is sending ICMP packets with TCP options flags set.

b. Source and destination ports are random. Source IPs is different but the destination receiver data pool is the same. Can extrapolate two (2) things from this:

1. My network may not be the ultimate target of the denial of service attack since the replies from my network is destined for a place other than the originator of the packet.
2. Destination IP for data can also be a data reservoir which can be a previously compromised host, which then makes the probability that the source IP being spoofed being high and this in turn makes the instigator fairly hard to trace. {Inner: 1.253.5.12->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 39965->6563})
3. Destination IP is actually where the perpetrator is that wishes to collect the data. Since he spoofed the source IP, this give him some credibility if someone comes looking to say that he is also being targeted since he is receiving packets from us. {Inner: 1.253.5.12->202.158.59.65: Protocol=TCP[PUSH URG FIN RST ACK] Port 39965->6563})

5. Attack mechanism:

The attack works by eliciting different responses from different operating systems beneath the entry barrier. Source seems to be either attempting to gather data on our network or utilizing us as a launch point for an attack on another network by sending to our network ICMP packets that are directing our network to send a TCP response to another network. This may make the source hard to trace.

6. Correlation:

Have never seen an attack like this and was not able to find any evidence of correlation at the www.sans.org website or via the search engines. Also checked the following websites:
www.cert.org
http://cve.mitre.org/
www.doshelp.com
www.robertgraham.com

7. Evidence of active targeting:

Does not seem to be singling out a specific host on our network per se. The specific host that seems to be singled out is the one where we are supposed to send the data which as illustrated above may in actuality be the person perpetrating the attack or the intended victim.

8. Severity:

a. (critical + Lethal) – (System + Net Countermeasures) = Severity

b. (3 + 4) - (5 + 5) = -3

9. Defensive recommendation:

Defenses are fine; attack was blocked by firewall. Firewall logs shows that firewall are not sending any IP unreachable information back to the source IP in response to these packets.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) DNS Zone Transfer
b) Subnet scan
c) DNS Version Scan
d) Data reservoir

Answer: d

Capture 3

Sep 9 13:02:38.137 Acheron-b kernel: 232 Sending ICMP port unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->Acheron-b-hme0.state.gov[1.253.4.2]: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:02:38.481 Acheron-b kernel: 232 Sending ICMP port unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->Acheron-b-hme0.state.gov[1.253.4.2]: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:06.949 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.2: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:07.041 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.4: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:07.193 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.6: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:07.404 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.8: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:07.649 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.10: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:07.862 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.12: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:08.104 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.14: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2

Sep 9 13:03:08.361 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.16: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:08.767 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.18: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:08.982 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.20: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:09.347 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.22: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:09.376 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.24: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:09.426 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.26: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:09.574 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.28: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:09.784 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->169.253.5.30: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:10.070 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.32: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:10.338 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.34: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:10.594 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.36: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:10.932 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.38: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:11.081 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.40: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2
Sep 9 13:03:11.153 Acheron-b kernel: 232 Sending ICMP host (prohibited) unreachable. Original packet (ppp-196-42-38-21.coqui.net[196.42.38.21]->1.253.5.42: Protocol=UDP Port 60000->2140) received on interface 1.253.4.2

1. Source of trace
    a. My network
2. Detect was generated by:

a. Raptor Firewall Logs

b. Explanation of fields:

Sep 9 13:03:11.153 **[Timestamp]**, Acheron-b **[Device name],** 232 **[service error],** Sending ICMP host (prohibited) unreachable. **[Information],** (ppp-196-42-38-21.coqui.net[196.42.38.21 **[source IP address],** dstif=qfe1 1.253.5.42 **[destination IP address],** protocol=UDP **[protocol]**

3. Probability the source address was spoofed

Medium to high.

4. Description of attack:

Source and destination ports are both high order ports, both static which immediately brings to mind trojans

5. Attack mechanism:

The attack works by requesting a response from the host infected with the trojan. In this case the Deep Throat trojan. Protocol is UDP so there will be no 3-way handshake and source is scanning entire network looking for infected host.

6. Correlation:

tcp/udp ports 2140, 3150, 6670, and 6771 - Deep Throat trojan horse(see http://members.xoom.com/big_chicken/trojans/deepthroat/ss.jpg)

tcp port 2140 - The Invasor trojan horse (seehttp://members.xoom.com/big_chicken/trojans/invasor/invasor.jpg)

Lastest version is 3.0, but it is fairly buggy. It uses TCP port 999 for its keylogger (default), and port 41 for its FTP service.

Detection/removal

Puts the file *C:\Windows\systray.exe* on your disk. The idea is to masquerade as the real *systray.exe* program located in *C:\Windows\system*. It changes the existing "Run" registry setting for SystemTray to the new program. Simply removing the "Run" entries or removing the systray.exe program will remove the Trojan.

Ports

The trojan will listen on: 6670/tcp, 3150/tcp, 2140/tcp, 2140/udp, 3150/udp.

When scanning for servers, the client will use source port of 60000 and scan for ports like 2140.

Variants

- **Main Site**
- **DarkLight**

7. Evidence of active targeting:

Source is going after a specific port not necessarily host.

8. . Severity:

a. (critical + Lethal) – (System + Net Countermeasures) = Severity

b. (3 + 4) - (5 + 5) = -3

9. Defensive recommendation:

Defenses are fine, attack was blocked by firewall. Firewall sending ICMP host unreachable packets. Need to silence the Firewall, if unable to do so, may need to block this specific port on the point of presence router and also make sure the router is silenced.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Port scan
b) DNS Inverse Query
c) Trojan
d) High port scan

answer: c

Capture 4

Aug 22 07:36:38.726 smtp[3063]: 121 Statistics: duration=0.34 id=dCzJO rcvd=85 srcif=hme0 src=200.252.8.69/3619 dstif=qfe1 dst=1.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:38.725 gwcontrol: 201 smtp[4264428085]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:39.878 smtp[3063]: 121 Statistics: duration=0.00 id=dCzJP rcvd=85 srcif=hme0 src=200.252.8.69/3621 dstif=qfe1 dst=1.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:39.876 gwcontrol: 201 smtp[4264428086]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:41.067 smtp[3063]: 121 Statistics: duration=0.00 id=dCzJQ rcvd=85 srcif=hme0 src=200.252.8.69/3624 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:41.059 gwcontrol: 201 smtp[4264428087]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:45.269 smtp[3063]: 121 Statistics: duration=0.00 id=dCzJV rcvd=85 srcif=hme0 src=200.252.8.69/3625 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:45.269 gwcontrol: 201 smtp[4264428092]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:46.576 smtp[3063]: 121 Statistics: duration=0.00 id=dCzJX rcvd=85 srcif=hme0 src=200.252.8.69/3628 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:46.575 gwcontrol: 201 smtp[4264428094]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]

Aug 22 07:36:47.932 smtp[3063]: 121 Statistics: duration=0.00 id=dCzJZ rcvd=85 srcif=hme0 src=200.252.8.69/3630 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:47.931 gwcontrol: 201 smtp[4264428095]: access denied for 200.252.8.69 to InterscanA.s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:49.104 smtp[3063]: 121 Statistics: duration=0.00 id=dCzK0 rcvd=85 srcif=hme0 src=200.252.8.69/3631 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)
Aug 22 07:36:49.104 gwcontrol: 201 smtp[4264428096]: access denied for 200.252.8.69 to InterscanA..s.gov [rule id 237] [explicit deny rule]
Aug 22 07:36:53.772 smtp[3063]: 121 Statistics: duration=0.00 id=dCzK7 rcvd=85 srcif=hme0 src=200.252.8.69/3633 dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov proto=smtp (Not authorized)

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Raptor Firewall Logs
    b. Explanation of fields:

        Aug 22 07:36:53.772 **[Timestamp]**, gwcontrol **[Device name],** smtp[3063] **[service error],**121 Statistics: duration=0.00 id=dCzK0 rcvd=85 **[],**srcif=hme0 src=200.252.8.69/3631 **[source interface, IP address/port number],** dstif=qfe1 dst=169.253.8.3/25 dstname=InterscanA.s.gov **[destination interface, IP address/port number],** proto=smtp (Not authorized) **[protocol]**
3. Probability the source address was spoofed

    Probability is medium to high
4. Description of attack:
    a. Large number of packets against TCP port 25 SMTP, which constitutes a mail bomb attack.
    b. Further investigation showed via our Intrusion detection system that we were receiving Real Secure Kills from the apparent source IP. In communication via a third party, found out that the supposed source advised that they were not sending us any data but was receiving resets from us. Our logs show that our Firewall was involuntary sending the supposed source reset packets because source network is being shunned.
5. Attack mechanism:
    a. This leads me to conclude that the chance that the source IP is spoofed is high.
    b. The supposed source network may ultimately be the target of the denial of service. They are receiving the collateral effect of their IPs being spoofed.

6. Correlations:

Collateral effect attack described in Stephen Northcutt's SANS2000 Advanced Network Intrusion Detection Analysis seminar.

7. Evidence of active targeting:

Attacker is going after our mail host.

8. Severity:

a. (critical + Lethal) – (System + Net Countermeasures) = Severity

b. (5 + 4) - (5 + 5) = -1

9. Defensive recommendation:

Defenses are fine, attack was blocked by firewall. Currently have a specific rule in place to shun this network. Need to silence firewall. Do not need to send out ICMP informational replies.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) DNS Zone Transfer
b) DNS Inverse Query
c) Mail bomb
d) DNS buffer overflow

answer: c

Assignment 2

Capture 5

Priority Date/Time Src Logicall Src Port Dest Logical Dst Port -

Event: Queso_Scan

Priority	Date	From	From Port	To	To Port	Informati
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:45.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	
High	2000/09/11 04:11:46.0	213.150.139.15	5661	198.76.102.24	23	

Received this report from my Network Intrusion Detection Team. The NIDS device logged this as a Queso scan. Immediately, the Firewall staff was contacted and given the source and destination IP address. This was our first means of correlation of events. The Firewall staff was unable to verify that they had seen these events. Our point of

presence router does not have SNMP enabled so we could not pull the RIT table to verify that these connections were attempted. Analysis show that source IP belongs to the Chimney Pot/Sweden. This information was gathered via the RIPE.NET. Though not shown, the protocol was TCP. Source scanned destination in excess of 400 times and as shown both source and destination IP and port number was static indicating a script kiddie. Destination port 23, while it has legitimate uses (telnet), if packets sent to it are malformed, the source can be trolling for things such as Prosiak, Tiny Telnet server, Truva Atl or Utlors Telnet trojan. Given the unauthorized use that can be made of this port, more care should be made by the security staff to make sure if port is not being used on the network that it is disabled on all boxes and that this port is blocked at the networks point of entry. Coordinated with the firewall team to make certain that telnet port is blocked at both the point of presence router and or the firewall itself. Also verified that when packets are received directed specifically at this port that they are silently dropped.

Assignment 3

My organization has been asked to provide a bid to provide security services, and therefore I have been allowed to run a Snort system with a fairly standard rulebase for about one month. During this time, the power has failed on several occasions, or the data disk became filled to capacity so I do not have data for the whole month. My task is to analyze the data that was collected and produce an analysis report.

Logs analysis for ***my.net's*** network shows that this network is being constantly scanned from several other networks. Scans range from assessment of what host type/operating systems are being utilized on the internal to major network vulnerabilities. What is obvious is that only one side of the traffic is shown. There are many reasons for this phenomenon:

- The snort device is not in an appropriate location
- The snort device resides on a tap, which allows only one side of the traffic to be seen. Snort recommends a mod tap for their device but I would have preferred to span a port on a switch so I could have seen both sides to a connection.
- The rule-set being utilized by the snort device did not include collecting both sides of a connection.

Only internal connections seen during the capture was UDP queries, this led me to conclude that network configuration setting may have a forwarding type DNS device for its internal hosts lookups, and therefore the main DNS server is either in the unprotected DMZ or a screened DMZ where the snort may have also been located, or the my.net to my.net traffic that was created was because my net's IP address was spoofed. I think this scenario is highly unlikely because more of this type traffic would have been produced to other IPs within the network.

No tools available to parse all this data to look for correlations between the source IPs doing the scanning and the subsequent apparent host devices compromised. Source IPs pushing packets with reserved bits set are shown. There are not major multiple hits of this type to a lot of IPs within my.net so my theory is that sources are pushing to internal hosts that have responded to previous scans, thereby revealing vulnerabilities. Could not see if any hosts answered since only had one side of the conversation.

Exhibit Snort s6a

Jul 28 14:31:26 63.29.27.192:1979 -> MY.NET.120.6:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1977 -> MY.NET.120.4:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1987 -> MY.NET.120.14:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1983 -> MY.NET.120.10:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1982 -> MY.NET.120.9:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1989 -> MY.NET.120.16:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1976 -> MY.NET.120.3:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1980 -> MY.NET.120.7:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1991 -> MY.NET.120.18:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1984 -> MY.NET.120.11:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1978 -> MY.NET.120.5:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1988 -> MY.NET.120.15:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1990 -> MY.NET.120.17:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1986 -> MY.NET.120.13:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1992 -> MY.NET.120.19:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:1994 -> MY.NET.120.21:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:2010 -> MY.NET.120.37:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:2014 -> MY.NET.120.41:21 SYN **S*****
Jul 28 14:31:27 63.29.27.192:2008 -> MY.NET.120.35:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:2016 -> MY.NET.120.43:21 SYN **S*****
Jul 28 14:31:26 63.29.27.192:2012 -> MY.NET.120.39:21 SYN **S*****

The Exhibit Snort s6a shows a sample of data in which:

- Source ports are changing, but the destination ports are not.
- The source IP's are static, but the destination IP's is not.

The source is host scanning the destination network looking for a FTP server. What is not seen is ***my.net*** network's response to these events. It cannot be concluded that this scan is not yielding any information at this time because do not see source transferring any packets. Source may prefer to return at a later time to compromise any vulnerability found. This scan is an exhaustive search through the whole network and lasts quite a while. The time frame between the source packets is fairly short which shows an automated tool. Source is initiating a connection with no intention of completing the 3-way handshake.

Exhibit Snort s6b

```
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.37:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.38:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.39:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.40:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.41:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.42:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.43:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.44:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.45:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.46:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.47:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.48:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.49:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.50:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.51:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.52:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.53:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.54:53 UDP
Jul 17 01:07:05 24.2.123.9:1693 -> MY.NET.1.55:53 UDP
```

The Exhibit Snort s6b shows a sample of data where a UDP scan of our network is being accomplished.

- Source IP and ports are static, but the destination IPs while changing the port is static

- Source is looking for DNS servers or other devices listening on this port in the network. Source is using a script kiddie. The script does not seem to be very sophisticated.

Exhibit Snort sca

```
Jul 24 15:29:37 MY.NET.1.3:53 -> MY.NET.101.89:42378 UDP
Jul 24 15:29:38 MY.NET.1.3:53 -> MY.NET.101.89:42378 UDP
Jul 24 15:29:38 MY.NET.1.3:53 -> MY.NET.101.89:42381 UDP
Jul 24 15:29:38 MY.NET.1.3:53 -> MY.NET.101.89:42382 UDP
Jul 24 15:29:38 MY.NET.1.3:53 -> MY.NET.101.89:42383 UDP
Jul 24 15:29:38 MY.NET.1.3:53 -> MY.NET.101.89:42384 UDP
Jul 24 15:29:39 MY.NET.1.3:53 -> MY.NET.101.89:42385 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42386 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42387 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42388 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42389 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42390 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42391 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42392 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42393 UDP
Jul 24 15:29:40 MY.NET.1.3:53 -> MY.NET.101.89:42395 UDP
Jul 24 15:29:41 MY.NET.1.3:53 -> MY.NET.101.89:42396 UDP
Jul 24 15:29:42 MY.NET.1.3:53 -> MY.NET.101.89:42397 UDP
```

The Exhibit Snort sca shows a sample of data that looks like a recursive lookup reply to IP within our network. There is a probability that this *my.net* ip address may be spoofed. Do not see the initiating connection for the query, interestingly have multiple replies from my.net.1.3 to same destination IP whose port are advancing, all within a few minutes

Exhibit Snort sca-b

```
Jul 24 21:56:54 209.123.109.175:4958 -> MY.NET.98.118:2627 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4959 -> MY.NET.98.118:2065 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4963 -> MY.NET.98.118:239 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4964 -> MY.NET.98.118:203 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4965 -> MY.NET.98.118:993 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4966 -> MY.NET.98.118:462 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4967 -> MY.NET.98.118:1410 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4968 -> MY.NET.98.118:5900 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4969 -> MY.NET.98.118:342 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4970 -> MY.NET.98.118:213 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4971 -> MY.NET.98.118:449 SYN **S*****
Jul 24 21:56:54 209.123.109.175:4972 -> MY.NET.98.118:167 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1032 -> MY.NET.98.118:250 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1033 -> MY.NET.98.118:665 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1034 -> MY.NET.98.118:709 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1036 -> MY.NET.98.118:422 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1037 -> MY.NET.98.118:521 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1038 -> MY.NET.98.118:737 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1039 -> MY.NET.98.118:1003 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1040 -> MY.NET.98.118:6148 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1041 -> MY.NET.98.118:1600 SYN **S*****
```

Jul 24 21:56:55 209.123.109.175:1042 -> MY.NET.98.118:2784 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1044 -> MY.NET.98.118:1497 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1045 -> MY.NET.98.118:531 SYN **S*****
Jul 24 21:56:55 209.123.109.175:1046 -> MY.NET.98.118:5510 SYN **S*****

The above Exhibit Snort sca-b sample data, reveals source IP seems to be initiating a lot of SYN connections to my.net within a relatively short period of time it seems with no intention of completing the 3-way handshake. Again, do not see the response of my.net to these initiating connections. Both source and destination ports are random but they are also both high order ports so I am assuming that source is trolling for trojans listening on those ports. There are some well known destination ports such as 213 (udp IPX, tcp IPX), 342, 521 (udp ripng , tcp ripng), etc , interspersed but the majority of the ports are high order – both source and destination.

Exhibit Snort s24

Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.15:5632 UDP
Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.25:5632 UDP
Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.31:5632 UDP
Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.32:5632 UDP
Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.36:5632 UDP
Aug 10 06:15:54 MY.NET.5.37:2600 -> MY.NET.5.36:22 UDP
Aug 10 06:15:56 MY.NET.5.37:2600 -> MY.NET.5.101:5632 UDP
Aug 10 06:15:57 MY.NET.5.37:2600 -> MY.NET.5.103:5632 UDP
Aug 10 06:15:57 MY.NET.5.37:2600 -> MY.NET.5.108:5632 UDP
Aug 10 06:15:57 MY.NET.5.37:2600 -> MY.NET.5.109:5632 UDP
Aug 10 06:15:57 MY.NET.5.37:2600 -> MY.NET.5.120:5632 UDP
Aug 10 06:15:57 MY.NET.5.37:2600 -> MY.NET.5.124:5632 UDP
Aug 10 06:16:00 MY.NET.5.37:2600 -> MY.NET.5.200:5632 UDP
Aug 10 06:16:00 MY.NET.5.37:2600 -> MY.NET.5.200:22 UDP
Aug 10 06:16:01 MY.NET.5.37:2600 -> MY.NET.5.246:5632 UDP
Aug 10 06:16:01 MY.NET.5.37:2600 -> MY.NET.5.247:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 -> MY.NET.5.11:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 -> MY.NET.5.12:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 -> MY.NET.5.12:22 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 -> MY.NET.5.13:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 -> MY.NET.5.13:22 UDP

5632 udp - pcANYWHEREstat
5632 tcp - pcANYWHEREstat
2600 udp - HPSTGMGR
2600 tcp - HPSTGMGR
22 udp - depreciated PCAnywhere
22 udp - SSH Remote login protocol
22 tcp - SSH Remote login protocol

The above Exhibit Snort s24 sample shows source is IP scanning ***my.net's*** network looking for hosts listening on PCAnywhere clients. This looks like the console polling network to retrieve information.

Exhibit Snort s24

Aug 10 17:34:38 64.244.202.66:64747 -> MY.NET.179.56:5300 SYN **S*****
Aug 10 17:48:34 128.61.105.103:6699 -> MY.NET.162.134:1424 VECNA 21***P*U
RESERVEDBITS
Aug 10 18:02:18 168.120.12.110:1721 -> MY.NET.98.197:54206 SYN **S*****
Aug 10 18:02:18 168.120.12.110:1722 -> MY.NET.98.197:29999 SYN **S*****
Jul 28 04:44:20 24.165.105.213:6699 -> MY.NET.97.196:1392 NOACK 2*S**P**
RESERVEDBITS
Jul 28 04:55:12 24.234.91.14:2742 -> MY.NET.100.236:6346 VECNA *****P**
Jul 28 05:12:37 24.165.105.213:6699 -> MY.NET.97.196:1392 NOACK 2*S**P**
RESERVEDBITS
Jul 28 05:18:00 24.234.91.14:2742 -> MY.NET.100.236:6346 NOACK ****R**U
Jul 28 05:23:00 24.234.91.14:2742 -> MY.NET.100.236:6346 UNKNOWN *1**R***
RESERVEDBITS
Jul 28 05:23:11 212.55.144.122:1356 -> MY.NET.100.236:6346 INVALIDACK 2**FRPAU
Jul 28 06:45:11 212.4.207.26:1649 -> MY.NET.100.236:6346 XMAS 21*F*P*U
RESERVEDBITS
Jul 28 06:45:12 212.4.207.26:1649 -> MY.NET.100.236:6346 UNKNOWN *1****AU
RESERVEDBITS
Jul 28 06:45:17 212.4.207.26:1649 -> MY.NET.100.236:6346 INVALIDACK **SFR*A*
Jul 28 06:45:33 212.4.207.26:1649 -> MY.NET.100.236:6346 NULL ********
Jul 28 06:47:02 212.4.207.26:0 -> MY.NET.100.236:1649 VECNA 21***P** RESERVEDBITS
Jul 28 06:47:25 212.4.207.26:1649 -> MY.NET.100.236:6346 VECNA ***F*P**
Jul 28 06:58:11 24.234.91.14:1 -> MY.NET.100.236:2742 INVALIDACK 21**RPAU
RESERVEDBITS

1424 udp Hybrid Encryption Protocol
1424 tcp Hybrid Encryption Protocol

Exhibit Snort s24 shows that it is highly likely that several ***my.net*** destination IPs have been compromised with a virus or other trojans. Source IPs have scanned previously and seemed to have return to exploit vulnerabilities that they had found, or the source may be using multiple IPs from which to affect hosts. In one instance, source seemed to have utilized the above protocol as the transport mechanism for the virus vecna.

VECNA

It is a very dangerous memory resident multipartite stealth virus. It writes itself to the MBR of the hard drive, to boot sectors of floppy disks and overwrites EXE files on floppy disks. While executing an infected EXE file the virus infects the MBR, decrypts and displays the message and then returns to DOS. The message is: Out of memory.

While loading from infected disk (HD or floppy) the virus hooks INT 13h, stays memory resident and infects disks and files.
Under debugger and on Pentium computers the virus displays the message: "Vecna Live"

The virus has quite a serious bug - it may continue INT 13h flow with wrong AX register. That may cause damage for disks, including disk formatting.

Vecna.313

It is not a dangerous memory resident stealth multipartite virus. It hooks INT 21h and writes itself to the end of COM files that are executed. The virus writes itself to the MBR sector when an infected COM file is started, it then returns control back to the host file. On loading from the MBR sector the virus hooks INT 13h that then hides virus code in the MBR sector and hooks INT 21h.

Vecna.Outsider

It is a very dangerous memory resident encrypted multipartite virus. It infects .EXE files and boot sector on floppy disks. EXE files get infection in "DirII" virus way. The virus hooks INT 13h, 28h.
In three month after infecting the computer, or under debugger the virus corrupts the CMOS (writes a password?) and displays the message:

"[OUTSIDER]
Esta e minha vinganca contra esta sociedade injusta
E eu ainda n+o estou satisfeito
Espere e ver+o..."

The virus also contains the text strings:
Written by Vecna/SGWW in Brazil 1997

Vecna.Tron

It is a harmless memory resident boot virus. It hooks INT 1, 8, 13h and writes itself to the MBR of the hard drive and boot sectors of floppy disks. The virus contains the text:
[ORGASMATRON] by Vecna/SGWW in Brazil 1997.

To hook INT 13h the virus uses i386 debug registers DR0, DR6 and DR7. By using these registers it sets break point on BIOS INT 13h handler. When this handler takes control the processor generates INT 1, and control is passed to virus INT 1 handler. The virus disables debug break point, checks registers and calls its infection and stealth routines in case of need and then returns to original BIOS INT 13h handler. To reset break point and to keep INT 1 hook the virus uses INT 8 hook (timer).

Exhibit Snort a17

06/29-00:06:24.298007 [**] WinGate 8080 Attempt [**] 128.231.171.123:2612 -> MY.NET.253.105:8080
06/29-00:08:24.581511 [**] WinGate 8080 Attempt [**] 128.231.171.123:2615 -> MY.NET.253.105:8080
06/29-00:14:24.727174 [**] WinGate 8080 Attempt [**] 128.231.171.123:2621 -> MY.NET.253.105:8080
06/29-00:15:24.796943 [**] WinGate 8080 Attempt [**] 128.231.171.123:2622 -> MY.NET.253.105:8080
06/29-00:15:55.846990 [**] WinGate 8080 Attempt [**] 212.119.97.20:1169 -> MY.NET.20.10:8080
06/29-00:15:56.522961 [**] WinGate 8080 Attempt [**] 212.119.97.20:1169 -> MY.NET.20.10:8080
06/29-00:15:57.377672 [**] WinGate 8080 Attempt [**] 212.119.97.20:1169 -> MY.NET.20.10:8080
06/29-00:16:24.784705 [**] WinGate 8080 Attempt [**] 128.231.171.123:2623 -> MY.NET.253.105:8080
06/29-00:21:24.967186 [**] WinGate 8080 Attempt [**] 128.231.171.123:2629 -> MY.NET.253.105:8080
06/29-00:23:24.991912 [**] WinGate 8080 Attempt [**] 128.231.171.123:2631 -> MY.NET.253.105:8080
06/29-00:25:25.026632 [**] WinGate 8080 Attempt [**] 128.231.171.123:2633 ->
06/29-05:23:27.156698 [**] WinGate 1080 Attempt [**] 200.51.33.202:3659 -> MY.NET.97.161:1080
06/29-05:23:30.111906 [**] WinGate 1080 Attempt [**] 200.51.33.202:3659 -> MY.NET.97.161:1080
06/29-05:23:30.655308 [**] WinGate 1080 Attempt [**] 200.51.33.202:3659 -> MY.NET.97.161:1080
06/29-05:23:34.214619 [**] WinGate 8080 Attempt [**] 128.231.171.123:2963 -> MY.NET.253.105:8080
06/29-05:23:34.672738 [**] WinGate 1080 Attempt [**] 200.51.33.202:3659 -> MY.NET.97.161:1080

The above sample shows port 8080 web proxy attempt, and socks proxy attempts. Does not state what protocol initiating IP is utilizing. Suspect TCP.

Assignment 4

Did not use any specific tools per se to parse data. Data was imported into WinWord or Word 97 and the find command utilized. Data was parsed, cut and pasted based on source IP at one point, destination IP at another, soure port at another juncture, and destination port. All data that was left over was accummulated into one final document and visual analysis was used to fine tune.