Global Information Assurance Certification Paper

*** Northcutt, another of the self generated exploits. Judge Judy scores this 86, lot of effort and therefore research. Some accuracy problems in 2, 5 (urg value must be 3), 6 and 10. That said, I found this a great read, thank you! 86 *

Practical Examination for GCIA

Charles McCants

April 12, 2000

Background

Most detects below are from self inflicted exploits run against an Internet connected non-production network at my office or on my home network. The exploit machine is a Redhat Linux 6.0 server, victim machines are varied (Linux, Solaris 2.6, and NT4.0). Other detects are from the firewall logs of each network. More than the required 10 detects are submitted, since a couple of them are similar in nature.

Severity of the attacks were based on the formula:
(Criticality + Lethality)-(System + Network countermeasures) = Severity

For the self induced exploits, additional information such as nmap and tcpshow outputs are also provided.

Detect 1 icmp-amplifier (part1)

```
19:11:04.804386 192.168.1.18 > 10.10.10.0: icmp: echo request (DF) (ttl 244, id
32279)
19:11:04.804477 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
17791)
19:11:04.804497 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5506)
19:11:05.636020 192.168.1.18 > 10.10.10.0: icmp: echo request (DF) (ttl 244, id
32280)
19:11:05.636053 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
17792)
19:11:05.636111 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5507)
19:11:06.649093 192.168.1.18 > 10.10.10.0: icmp: echo request (DF) (ttl 244, id
32281)
19:11:06.649126 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
17793)
19:11:06.649184 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5508)
19:11:07.631774 192.168.1.18 > 10.10.10.0: icmp: echo request (DF) (ttl 244, id
32282)
19:11:07.631808 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
17794)
19:11:07.631864 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5509)
```

Detect 1 icmp-amplifier (part2)

```
19:14:26.326747 192.168.1.18 > 10.10.10.255: icmp: echo request (DF) (ttl 244,
id 37361)
19:14:26.326842 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
18112)
19:14:26.326871 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5510)
19:14:27.333125 192.168.1.18 > 10.10.10.255: icmp: echo request (DF) (ttl 244,
id 37362)
19:14:27.333160 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
18113)
19:14:27.333225 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5511)
19:14:28.324901 192.168.1.18 > 10.10.10.255: icmp: echo request (DF) (ttl 244,
id 37363)
19:14:28.324937 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
18114)
19:14:28.324993 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5512)
19:14:29.326256 192.168.1.18 > 10.10.10.255: icmp: echo request (DF) (ttl 244,
id 37364)
19:14:29.326289 10.10.10.15 > 192.168.1.18: icmp: echo reply (ttl 255, id
18115)
19:14:29.326353 10.10.10.30 > 192.168.1.18: icmp: echo reply (ttl 64, id 5513)
```

Active Targeting?	Yes
Analysis	**Icmp amplifier probe** ICMP echo requests were sent from 192.168.1.18 to the 10.10.10.0 network address then to the 10.10.10.255 network broadcast address. The technique used on these attacks were simple pings directed to the network and it's broadcast addresses. This attack could be used in determining if a network could be used as a participant in a DDOS attack against another machine. It was also effective for mapping machines on the network since all connected machines replied to the echo request. While the

	severity of this attack is low, attention should be paid to the fact that it was successful.
Intent	Network Mapping
Severity	(4+2)-(5+2)=-1 Low, but immediate steps should be taken to correct. (i.e. blocking at router)

Detect 2 – identd scan

```
21:04:52.690006 yoshi.1935 > victim.smtp: S 3651585487:3651585487(0) win 32120
<mss 1460,sackOK,timestamp 22468556[|tcp]> (DF) (ttl 64, id 57678)
21:04:52.690601 yoshi.1935 > victim.smtp: . ack 1 win 32120 (DF) (ttl 64, id
57681)
21:04:52.811841 yoshi.2049 > victim.telnet: S 3648353063:3648353063(0) win
32120 <mss 1460,sackOK,timestamp 22468568[|tcp]> (DF) (ttl 64, id 57803)
21:04:52.812093 victim.telnet > yoshi.2049: S 332017082:332017082(0) ack
3648353064 win 32736 <mss 1460> (ttl 64, id 21821)
21:04:52.812312 yoshi.2049 > victim.telnet: . ack 1 win 32120 (DF) (ttl 64, id
57805)
21:04:52.872967 yoshi.2073 > victim.auth: S 3647040193:3647040193(0) win 32120
<mss 1460,sackOK,timestamp 22468575[|tcp]> (DF) (ttl 64, id 57828)
21:04:52.873185 victim.auth > yoshi.2073: S 3867343348:3867343348(0) ack
3647040194 win 32736 <mss 1460> (ttl 64, id 21845)
21:04:52.873419 yoshi.2073 > victim.auth: . ack 1 win 32120 (DF) (ttl 64, id
57829)
21:04:52.873548 yoshi.2073 > victim.auth: P 1:11(10) ack 1 win 32120 (DF) (ttl
64, id 57830)
21:04:52.886230 victim.auth > yoshi.2073: . ack 11 win 32726 (DF) (ttl 64, id
21846)

Many lines removed

21:05:01.251255 victim.www > yoshi.3081: . ack 2 win 32735 (DF) (ttl 64, id
23043)
21:05:01.252079 victim.www > yoshi.3081: F 1:1(0) ack 2 win 32736 (ttl 64, id
23044)
21:05:01.252329 yoshi.3081 > victim.www: . ack 2 win 32120 (DF) (ttl 64, id
59022)
21:05:02.420976 yoshi.3314 > victim.ftp: S 3671362193:3671362193(0) win 32120
<mss 1460,sackOK,timestamp 22469529[|tcp]> (DF) (ttl 64, id 59187)
21:05:02.421295 victim.ftp > yoshi.3314: S 3115109965:3115109965(0) ack
3671362194 win 32736 <mss 1460> (ttl 64, id 23211)
21:05:02.421722 yoshi.3314 > victim.ftp: . ack 1 win 32120 (DF) (ttl 64, id
59191)
```

Active Targeting?	Yes
Analysis	**Identd scan** The packets are obviously forged as shown by the [|tcp] in the initial packet sent from the attacker (yoshi). Using nmap pointed toward a machine running the identd service an attacker can determine the owners of open ports. This info can be used in a buffer overflow attack to gain access to the machine as that user. (i.e. a web server running as root). Also see the nmap output below:
Intent	Malicious, probing listeners for potential root access
Severity	(4+5)-(5+2)=2 Valuable info obtained from scan

```
# Log of: nmap -I -o identd-info.txt -v victim
Interesting ports on victim.home.com (172.16.1.200):
Port    State       Protocol  Service         Owner
```

```
21      open        tcp        ftp             root
23      open        tcp        telnet          root
25      open        tcp        smtp            root
37      open        tcp        time            root
53      open        tcp        domain          root
70      open        tcp        gopher          root
79      open        tcp        finger          root
80      open        tcp        http            nobody
98      open        tcp        linuxconf       root
109     open        tcp        pop-2           root
110     open        tcp        pop-3           root
111     open        tcp        sunrpc          bin
113     open        tcp        auth            root
139     open        tcp        netbios-ssn     root
143     open        tcp        imap2           root
513     open        tcp        login           root
514     open        tcp        shell           root
```

Detect 3 – Land Attack

```
22:55:58.961340 victim.ftp-data > victim.ftp-data: S 593718819:593718819(0) win
4096 (ttl 43, id 43718)
22:56:04.997431 victim.ftp > victim.ftp: S 4140239849:4140239849(0) win 4096
(ttl 43, id 16611)
22:56:11.037315 victim.ssh > victim.ssh: S 2387521472:2387521472(0) win 4096
(ttl 43, id 38864)
22:56:17.057293 victim.telnet > victim.telnet: S 593718819:593718819(0) win
4096 (ttl 43, id 49460)
```

Active Targeting?	Yes
Analysis	**Land Attack** A crafted packet (using ippacket in this case) was sent to victim with it's source address and source port spoofed to be the same as the destination address and port. Some IP stacks don't know how to handle packets such as this, since they cannot occur normally.
Intent	Malicious, Denial of Service attack
Severity	(4+4)-(5+2)=1 Low

Detect 4 – Queso scan

```
20:29:20.332978 badguy.7721 > victim.www: S 606281182:606281182
(0) win 4660 (ttl 240, id 39058)
20:29:20.333140 victim.www > badguy.7721: S 2092188174:20921881
74(0) ack 606281183 win 32736 <mss 536> (ttl 64, id 17381)
20:29:20.340290 badguy.7722 > victim.www: S 606281182:606281182
(0) ack 0 win 4660 (ttl 240, id 39059)
20:29:20.340378 victim.www > badguy.7722: R 0:0(0) win 0 (ttl 2
55, id 17382)
20:29:20.349799 badguy.7723 > victim.www: F 606281182:606281182
(0) win 4660 (ttl 240, id 39060)
20:29:20.358508 badguy.7724 > victim.www: F 606281182:606281182
(0) ack 0 win 4660 (ttl 240, id 39061)
20:29:20.358629 victim.www > badguy.7724: R 0:0(0) win 0 (ttl 2
55, id 17383)
20:29:20.365636 badguy.7725 > victim.www: SF 606281182:60628118
2(0) win 4660 (ttl 240, id 39062)
20:29:20.365742 victim.www > badguy.7725: SF 2029898772:2029898
772(0) ack 606281183 win 32736 <mss 536> (ttl 64, id 17384)
20:29:20.373542 badguy.7726 > victim.www: P win 4660 (ttl 240,
id 39063)
20:29:20.385035 badguy.7727 > victim.www: S 606281182:606281182
(0) win 4660 (ttl 240, id 39064)
20:29:20.385138 victim.www > badguy.7727: S 4288947413:42889474
13(0) ack 606281183 win 32736 <mss 536> (ttl 64, id 17385)
20:29:20.451655 badguy.7721 > victim.www: R 606281183:606281183
(0) win 0 (ttl 49, id 34220)
20:29:20.484768 badguy.7725 > victim.www: R 606281183:606281183
(0) win 0 (ttl 49, id 55808)
20:29:20.529088 badguy.7727 > victim.www: R 606281183:606281183
(0) win 0 (ttl 49, id 45481)
```

Active Targeting?	Yes
Analysis	**Queso OS Detection Scan** By sending a specific sequence of malformed packets, queso can determine the target's operating system. This info can then be used to target specific attacks against the machine. See queso output below:
Intent	Reconn
Severity	(4+2)-(3+2)=1 Low

```
# /usr/local/sbin/queso -d victim
Starting badguy:7721 -> 38.254.242.30:80
IN  #0 : 80->7721 S:1 A:+1 W:7FE0 U:0 F: SYN ACK
IN  #1 : 80->7722 S:0 A: 0 W:0000 U:0 F: RST
IN  #3 : 80->7724 S:0 A: 0 W:0000 U:0 F: RST
IN  #4 : 80->7725 S:1 A:+1 W:7FE0 U:0 F: SYN FIN ACK
IN  #6 : 80->7727 S:1 A:+1 W:7FE0 U:0 F: SYN ACK
38.254.242.30:80        * Linux 2.0.35 to 2.0.9999 :)
```

The above output shows the return flags from the victim to the badguy. It's OS determination was correct.

Detect 5 - Winnuke

```
21:30:01.886812 yoshi.3351 > victim-nt.139: S 946762713:946762713(0) win 32120
<mss 1460,sackOK,timestamp 22619476[|tcp]> (DF) (ttl 64, id 59437)
21:30:01.887080 victim-nt.139 > yoshi.3351: S 2662139176:2662139176(0) ack
946762714 win 32736 <mss 1460> (ttl 64, id 23260)
21:30:01.887329 yoshi.3351 > victim-nt.139: . ack 1 win 32120 (DF) (ttl 64, id
59438)
21:30:01.888332 yoshi.3351 > victim-nt.139: P 1:4(3) ack 1 win 32120 urg 3 (DF)
(ttl 64, id 59439)
21:30:01.888609 yoshi.3351 > victim-nt.139: F 4:4(0) ack 1 win 32120 (DF) (ttl
64, id 59440)
21:30:01.888803 victim-nt.139 > yoshi.3351: . ack 5 win 32732 (DF) (ttl 64, id
23261)
21:30:01.897281 victim-nt.139 > yoshi.3351: F 1:1(0) ack 5 win 32736 (ttl 64,
id 23264)
21:30:01.897543 yoshi.3351 > victim-nt.139: . ack 2 win 32120 (DF) (ttl 64, id
59441)
```

Active Targeting?	Yes
Analysis	Winnuke Winnuke takes advantage of NT's inability to handle unexpected data on port 139. In this case a perl script was used to initiate a connection then send a packet with the urgent flag set and the name "BILL" as data. This particular victim machine did not blue screen but the malformed packet is shown below. An indicator of this attack is the URG, ACK and PSH flags set with a destination port of 139.
Intent	Malicious, Denial of Service
Severity	(4+4)-(5+2)=1 Low

```
Packet 9
IP Header
       Version:                        4
       Header Length:                  20 bytes
       Service Type:             0x00
       Datagram Length:                43 bytes
       Identification:                 0xE82F
       Flags:                    MF=off, DF=on
       Fragment Offset:                0
       TTL:                            64
       Encapsulated Protocol:          TCP
       Header Checksum:                0xF7B1
       Source IP Address:        172.16.1.3 (yoshi)
       Destination IP Address:         172.16.1.200 (victim-nt)
TCP Header
       Source Port:              3351 (<unknown>)
       Destination Port:               139 (netbios-ssn)
       Sequence Number:                0946762714
       Acknowledgement Number:         2662139177
       Header Length:                  20 bytes (data=3)
       Flags:                    URG=on,  ACK=on,  PSH=on
                                       RST=off, SYN=off, FIN=off
       Window Advertisement:           32120 bytes
       Checksum:                       0xB207
       Urgent Pointer:                 3
```

```
TCP Data
       BILL
```

Detect 6 – ping-o-death

```
22:39:43.510349 yoshi > victim: icmp: echo request (frag 61760:1480@0+) (ttl
64)
22:39:43.511486 yoshi > victim: (frag 61760:1018@60680) (ttl 64)
22:39:43.513364 yoshi > victim: (frag 61760:1480@59200+) (ttl 64)
22:39:43.514862 yoshi > victim: (frag 61760:1480@57720+) (ttl 64)
22:39:43.516356 yoshi > victim: (frag 61760:1480@56240+) (ttl 64)
22:39:43.517852 yoshi > victim: (frag 61760:1480@54760+) (ttl 64)
22:39:43.519359 yoshi > victim: (frag 61760:1480@53280+) (ttl 64)
22:39:43.520855 yoshi > victim: (frag 61760:1480@51800+) (ttl 64)
22:39:43.522350 yoshi > victim: (frag 61760:1480@50320+) (ttl 64)

Many lines deleted

22:39:43.568854 yoshi > victim: (frag 61760:1480@4440+) (ttl 64)
22:39:43.570352 yoshi > victim: (frag 61760:1480@2960+) (ttl 64)
22:39:43.571851 yoshi > victim: (frag 61760:1480@1480+) (ttl 64)
```

Active Targeting?	Yes
Analysis	Ping-O-Death In this attack a large ping (65K ICMP echo request) packet was sent to the victim host. Many unpatched OS's can't handle pings of this size and will crash. This was attempted against an NT 4.0 SP5 machine and a RedHat 6.0 machine with no noticeable effect to either machine. A possible unfortunate side effect for the attacker is that the victim sends back a reply of the same size. So, the attacker could nuke himself in the attempt.
Intent	Malicious, Denial of Service
Severity	(4+4)-(5+2)=1 Low

Detect 7 – NT RPC Locator

```
21:46:34.339598 mario.64355 > victim-nt.135: S 2012494322:2012494322(0) win
32120 <mss 1460,sackOK,timestamp 22718721[|tcp]> (DF) (ttl 63, id 59969)
21:46:34.340546 victim-nt.135 > mario.64355: S 764048:764048(0) ack 2012494323
win 8760 <mss 1460> (DF) (ttl 128, id 39680)
21:46:34.340997 mario.64355 > victim-nt.135: . ack 1 win 32120 (DF) (ttl 63, id
59970)
21:46:41.699670 mario.64355 > victim-nt.135: P 1:13(12) ack 1 win 32120 (DF)
(ttl 63, id 59971)
21:46:41.853099 victim-nt.135 > mario.64355: . ack 13 win 8748 (DF) (ttl 128,
id 39936)
21:47:19.512016 mario.64355 > victim-nt.135: F 36:36(0) ack 1 win 32120 (DF)
(ttl 63, id 59978)
21:47:19.512487 victim-nt.135 > mario.64355: . ack 37 win 8725 (DF) (ttl 128,
id 41728)
```

Active Targeting?	Yes
Analysis	NT RPC Locator Using telnet to connect to a NT machine and sending a small amount of data will drive the victims CPU utilization to 100% - instantly. This attack was run against a NT4.0 SP5 machine and it immediately went to 100% utilization. Below is the actual packet carrying the data.
Intent	Malicious, Denial of Service
Severity	(4+4)-(3+2)=3 Attack succeeded

```
Packet 11
IP Header
       Version:                        4
       Header Length:                  20 bytes
       Service Type:             0x00
       Datagram Length:                52 bytes
       Identification:                 0xEA43
       Flags:                    MF=off, DF=on
       Fragment Offset:                0
       TTL:                            63
       Encapsulated Protocol:          TCP
       Header Checksum:                0x1F4C
       Source IP Address:        (mario)
       Destination IP Address:         (victim-nt)
TCP Header
       Source Port:              64355 (<unknown>)
       Destination Port:               135 (loc-srv)
       Sequence Number:                2012494323
       Acknowledgement Number:         0000764049
       Header Length:                  20 bytes (data=12)
       Flags:                    URG=off, ACK=on,  PSH=on
                                       RST=off, SYN=off, FIN=off
       Window Advertisement:           32120 bytes
       Checksum:                       0x9790
       Urgent Pointer:                 0
TCP Data
       0123456789.
```

Detect 8 – TCP port scan

```
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64449 to 207.238.186.18 on unserved port 426
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64450 to 207.238.186.18 on unserved port 159
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64451 to 207.238.186.18 on unserved port 112
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64452 to 207.238.186.18 on unserved port 1486
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64453 to 207.238.186.18 on unserved port 218
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64454 to 207.238.186.18 on unserved port 1462
Apr 10 01:28:55 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:64455 to 207.238.186.18 on unserved port 150


Many lines removed

Apr 10 01:29:05 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:61396 to 207.238.186.18 on unserved port 355
Apr 10 01:29:05 fw.victim.net unix: securityalert: tcp if=hme0 from
badguy:61397 to 207.238.186.18 on unserved port 518
```

Active Targeting?	Yes
Analysis	TCP Port Scan Simple nmap tcp port scan, looking for open ports. The nmap output (shown below) shows open ports, which are actually proxied ports. The ports marked filtered were actually filtered by the router before they hit the firewall.
Intent	Reconn
Severity	(5+2)-(5+4)=-2 Low

```
# Log of: nmap -sT -PT -F -o tcp-firewall.txt fw.victim.net
Interesting ports on fw.victim.net (10.1.2.3):
Port    State       Protocol  Service
21      open        tcp        ftp
23      open        tcp        telnet
25      open        tcp        smtp
53      open        tcp        domain
80      open        tcp        http
87      filtered    tcp        priv-term-l
111     filtered    tcp        sunrpc
113     open        tcp        auth
137     filtered    tcp        netbios-ns
443     open        tcp        https
512     filtered    tcp        exec
513     filtered    tcp        login
514     filtered    tcp        shell
515     filtered    tcp        printer
540     filtered    tcp        uucp
2000    filtered    tcp        callbook
6000    filtered    tcp        X11
```

Detect 9 – UDP port scan

```
04/10-02:12:04.860035 badguy:62527 -> fw.victim.net:1672
UDP TTL:29 TOS:0x0 ID:1758
Len: 8
04/10-02:12:04.864296 badguy:62527 -> fw.victim.net:510
UDP TTL:29 TOS:0x0 ID:34233
Len: 8
04/10-02:12:04.866012 badguy:62527 -> fw.victim.net:7006
UDP TTL:29 TOS:0x0 ID:29945
Len: 8
04/10-02:12:04.869934 badguy:62527 -> fw.victim.net:366
UDP TTL:29 TOS:0x0 ID:26864
Len: 8
04/10-02:12:04.880976 badguy:62527 -> fw.victim.net:2044
UDP TTL:29 TOS:0x0 ID:21896
Len: 8
04/10-02:12:04.884059 badguy:62527 -> fw.victim.net:146
UDP TTL:29 TOS:0x0 ID:18072
Len: 8
04/10-02:12:04.886532 badguy:62527 -> fw.victim.net:264
UDP TTL:29 TOS:0x0 ID:1603
Len: 8
04/10-02:12:04.890837 badguy:62527 -> fw.victim.net:280
UDP TTL:29 TOS:0x0 ID:5373
Len: 8
04/10-02:12:04.893049 badguy:62527 -> fw.victim.net:222
UDP TTL:29 TOS:0x0 ID:54472
Len: 8
04/10-02:12:05.207927 badguy:62528 -> fw.victim.net:1444
UDP TTL:29 TOS:0x0 ID:55583
Len: 8
04/10-02:12:05.210559 badguy:62528 -> fw.victim.net:1672
UDP TTL:29 TOS:0x0 ID:34685
Len: 8
```

Active Targeting?	Yes
Analysis	UDP Port Scan Simple nmap udp port scan, looking for open ports.
Intent	Reconn
Severity	(5+2)-(5+4)=-2 Low

Detect 10 – IMAPD attack

```
08:10:14.189375 yoshi.3217 > firewall.chazhome.com.imap2: S
3918918536:3918918536(0) win 32120 <mss 1460,sackOK,timestamp 11719125
0,nop,wscale 0> (DF) (ttl 64, id 21917)
08:10:14.189445 firewall.chazhome.com.imap2 > yoshi.3217: S
3356774784:3356774784(0) ack 3918918537 win 32120 <mss 1460,sackOK,timestamp
14171609 11719125,nop,wscale 0> (DF) (ttl 64, id 45337)
08:10:14.189826 yoshi.3217 > firewall.chazhome.com.imap2: . ack 1 win 32120
<nop,nop,timestamp 11719125 14171609> (DF) (ttl 64, id 21918)
08:10:14.210344 firewall.chazhome.com.imap2 > yoshi.3217: P 1:60(59) ack 1 win
32120 <nop,nop,timestamp 14171611 11719125> (DF) (ttl 64, id 45338)
08:10:14.210861 yoshi.3217 > firewall.chazhome.com.imap2: . ack 60 win 32120
<nop,nop,timestamp 11719127 14171611> (DF) (ttl 64, id 21919)
08:10:14.212498 yoshi.3217 > firewall.chazhome.com.imap2: P 1:23(22) ack 60 win
32120 <nop,nop,timestamp 11719128 14171611> (DF) (ttl 64, id 21920)
08:10:14.212532 firewall.chazhome.com.imap2 > yoshi.3217: . ack 23 win 32120
<nop,nop,timestamp 14171611 11719128> (DF) (ttl 64, id 45339)
08:10:14.212759 firewall.chazhome.com.imap2 > yoshi.3217: P 60:82(22) ack 23
win 32120 <nop,nop,timestamp 14171611 11719128> (DF) (ttl 64, id 45340)
08:10:14.214643 yoshi.3217 > firewall.chazhome.com.imap2: P 23:1057(1034) ack
60 win 32120 <nop,nop,timestamp 11719128 14171611> (DF) (ttl 64, id 21921)
08:10:14.221768 yoshi.3217 > firewall.chazhome.com.imap2: . ack 82 win 32120
<nop,nop,timestamp 11719129 14171611> (DF) (ttl 64, id 21922)
08:10:14.221832 firewall.chazhome.com.imap2 > yoshi.3217: P 82:189(107) ack
1057 win 32120 <nop,nop,timestamp 14171612 11719129> (DF) (ttl 64, id 45341)
08:10:14.231762 yoshi.3217 > firewall.chazhome.com.imap2: . ack 189 win 32120
<nop,nop,timestamp 11719130 14171612> (DF) (ttl 64, id 21923)
08:10:17.113510 yoshi.3217 > firewall.chazhome.com.imap2: P 1057:1058(1) ack
189 win 32120 <nop,nop,timestamp 11719418 14171612> (DF) (ttl 64, id 21924)
08:10:17.114095 firewall.chazhome.com.imap2 > yoshi.3217: P 189:209(20) ack
1058 win 32120 <nop,nop,timestamp 14171902 11719418> (DF) (ttl 64, id 45342)
08:10:17.131753 yoshi.3217 > firewall.chazhome.com.imap2: . ack 209 win 32120
<nop,nop,timestamp 11719420 14171902> (DF) (ttl 64, id 21925)
08:10:20.026470 yoshi.3217 > firewall.chazhome.com.imap2: P 1058:1059(1) ack
209 win 32120 <nop,nop,timestamp 11719709 14171902> (DF) (ttl 64, id 21926)
08:10:20.026864 firewall.chazhome.com.imap2 > yoshi.3217: P 209:229(20) ack
1059 win 32120 <nop,nop,timestamp 14172193 11719709> (DF) (ttl 64, id 45343)
08:10:20.041751 yoshi.3217 > firewall.chazhome.com.imap2: . ack 229 win 32120
<nop,nop,timestamp 11719711 14172193> (DF) (ttl 64, id 21927)
08:10:22.547173 yoshi.3217 > firewall.chazhome.com.imap2: P 1059:1060(1) ack
229 win 32120 <nop,nop,timestamp 11719961 14172193> (DF) (ttl 64, id 21928)
08:10:22.547552 firewall.chazhome.com.imap2 > yoshi.3217: P 229:249(20) ack
1060 win 32120 <nop,nop,timestamp 14172445 11719961> (DF) (ttl 64, id 45344)
08:10:22.561750 yoshi.3217 > firewall.chazhome.com.imap2: . ack 249 win 32120
<nop,nop,timestamp 11719963 14172445> (DF) (ttl 64, id 21929)
08:10:27.746869 yoshi.3217 > firewall.chazhome.com.imap2: F 1060:1060(0) ack
249 win 32120 <nop,nop,timestamp 11720481 14172445> (DF) (ttl 64, id 21930)
08:10:27.746906 firewall.chazhome.com.imap2 > yoshi.3217: . ack 1061 win 32120
<nop,nop,timestamp 14172965 11720481> (DF) (ttl 64, id 45345)
08:10:27.747635 firewall.chazhome.com.imap2 > yoshi.3217: F 249:249(0) ack 1061
win 32120 <nop,nop,timestamp 14172965 11720481> (DF) (ttl 64, id 45346)
```

Active Targeting?	Yes
Analysis	IMAPD Attack Using code obtained from packetstorm, the following packets were sent to firewall.chazhome.com with the intent of crashing the imap server via a buffer overflow and gaining root access to the machine. This attack has been successful before on Linux

	machines running the wu-imap server. It does not work however against this version of the server. The exploit is easily identified by the 'nops' sent to the target machine's imap port (143). Below is also a tcpshow of the relevant packets grabbed during the above tcpdump. It's lengthy, but shows the data sent to and from the imap server.
Intent	Malicious
Severity	(5+5)-(5+4)=1 Low

```
Packet 9
      Timestamp:                08:10:14.210344 (0.020518)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                111 bytes
      Identification:                 0xB11A
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x2F49
      Source IP Address:        172.16.1.2 (<unknown>)
      Destination IP Address:         172.16.1.3 (yoshi)
TCP Header
      Source Port:              143 (imap)
      Destination Port:               3217 (<unknown>)
      Sequence Number:                3356774785
      Acknowledgement Number:         3918918537
      Header Length:                  32 bytes (data=59)
      Flags:                    URG=off, ACK=on,  PSH=on
                                      RST=off, SYN=off, FIN=off
      Window Advertisement:           32120 bytes
      Checksum:                       0xFA49
      Urgent Pointer:                 0
      <Options not displayed>
TCP Data
      * OK firewall.chazhome.com IMAP4rev1 v12.250 server ready.

-----------------------------------------------------------------
Packet 11
      Timestamp:                08:10:14.212498 (0.001637)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                74 bytes
      Identification:                 0x55A0
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x8AE8
      Source IP Address:        172.16.1.3 (yoshi)
      Destination IP Address:         172.16.1.2 (<unknown>)
TCP Header
      Source Port:              3217 (<unknown>)
      Destination Port:               143 (imap)
```

```
      Sequence Number:                3918918537
      Acknowledgement Number:         3356774844
      Header Length:                  32 bytes (data=22)
      Flags:                    URG=off, ACK=on,  PSH=on
                                      RST=off, SYN=off, FIN=off
      Window Advertisement:           32120 bytes
      Checksum:                       0x96EE
      Urgent Pointer:                 0
      <Options not displayed>
TCP Data
      * AUTHENTICATE {1032}

-----------------------------------------------------------------------
Packet 13
      Timestamp:                08:10:14.212759 (0.000227)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                74 bytes
      Identification:                 0xB11C
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x2F6C
      Source IP Address:        172.16.1.2 (<unknown>)
      Destination IP Address:         172.16.1.3 (yoshi)
TCP Header
      Source Port:              143 (imap)
      Destination Port:               3217 (<unknown>)
      Sequence Number:                3356774844
      Acknowledgement Number:         3918918559
      Header Length:                  32 bytes (data=22)
      Flags:                    URG=off, ACK=on,  PSH=on
                                      RST=off, SYN=off, FIN=off
      Window Advertisement:           32120 bytes
      Checksum:                       0xA736
      Urgent Pointer:                 0
      <Options not displayed>
TCP Data
      + Ready for argument.

-----------------------------------------------------------------------
Packet 16
      Timestamp:                08:10:14.221832 (0.000064)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                159 bytes
      Identification:                 0xB11D
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x2F16
      Source IP Address:        172.16.1.2 (<unknown>)
      Destination IP Address:         172.16.1.3 (yoshi)
TCP Header
      Source Port:              143 (imap)
```

```
      Destination Port:               3217 (<unknown>)
      Sequence Number:                3356774866
      Acknowledgement Number:         3918919593
      Header Length:                  32 bytes (data=107)
      Flags:                    URG=off, ACK=on,  PSH=on
                                      RST=off, SYN=off, FIN=off
      Window Advertisement:           32120 bytes
      Checksum:                       0x3DF6
      Urgent Pointer:                 0
      <Options not displayed>
TCP Data
      * NO AUTHENTICATE ......................................
      ..................................... failed.

-----------------------------------------------------------------------
Packet 19
      Timestamp:                08:10:17.114095 (0.000585)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                72 bytes
      Identification:                 0xB11E
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x2F6C
      Source IP Address:        172.16.1.2 (<unknown>)
      Destination IP Address:         172.16.1.3 (yoshi)
TCP Header
      Source Port:              143 (imap)
      Destination Port:               3217 (<unknown>)
      Sequence Number:                3356774973
      Acknowledgement Number:         3918919594
      Header Length:                  32 bytes (data=20)
      Flags:                    URG=off, ACK=on,  PSH=on
                                      RST=off, SYN=off, FIN=off
      Window Advertisement:           32120 bytes
      Checksum:                       0x9EC9
      Urgent Pointer:                 0
      <Options not displayed>
TCP Data
      * BAD Null command.

-----------------------------------------------------------------------
Packet 22
      Timestamp:                08:10:20.026864 (0.000394)
      Encapsulated Protocol:          IP
IP Header
      Version:                        4
      Header Length:                  20 bytes
      Service Type:             0x00
      Datagram Length:                72 bytes
      Identification:                 0xB11F
      Flags:                    MF=off, DF=on
      Fragment Offset:                0
      TTL:                            64
      Encapsulated Protocol:          TCP
      Header Checksum:                0x2F6B
      Source IP Address:        172.16.1.2 (<unknown>)
      Destination IP Address:         172.16.1.3 (yoshi)
```

```
TCP Header
       Source Port:               143 (imap)
       Destination Port:                 3217 (<unknown>)
       Sequence Number:                  3356774993
       Acknowledgement Number:           3918919595
       Header Length:                    32 bytes (data=20)
       Flags:                     URG=off, ACK=on,  PSH=on
                                         RST=off, SYN=off, FIN=off
       Window Advertisement:             32120 bytes
       Checksum:                         0x9C6E
       Urgent Pointer:                   0
       <Options not displayed>
TCP Data
       * BAD Null command.

------------------------------------------------------------------------
Packet 25
       Timestamp:                 08:10:22.547552 (0.000379)
       Encapsulated Protocol:            IP
IP Header
       Version:                          4
       Header Length:                    20 bytes
       Service Type:              0x00
       Datagram Length:                  72 bytes
       Identification:                   0xB120
       Flags:                     MF=off, DF=on
       Fragment Offset:                  0
       TTL:                              64
       Encapsulated Protocol:            TCP
       Header Checksum:                  0x2F6A
       Source IP Address:         172.16.1.2 (<unknown>)
       Destination IP Address:           172.16.1.3 (yoshi)
TCP Header
       Source Port:               143 (imap)
       Destination Port:                 3217 (<unknown>)
       Sequence Number:                  3356775013
       Acknowledgement Number:           3918919596
       Header Length:                    32 bytes (data=20)
       Flags:                     URG=off, ACK=on,  PSH=on
                                         RST=off, SYN=off, FIN=off
       Window Advertisement:             32120 bytes
       Checksum:                         0x9A61
       Urgent Pointer:                   0
       <Options not displayed>
TCP Data
       * BAD Null command.
```

Detect 11 – SYN flood attack

```
01:34:08.317007 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317095 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317182 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317280 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317372 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317463 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.317555 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)

Many packets deleted

01:34:08.323430 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.323521 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.323613 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.323704 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
01:34:08.323796 1.2.3.4.telnet > victim.smtp: SFRP 0:25(25) ack 0 win 512 urg 0
(ttl 60, id 907)
```

Active Targeting?	Yes
Analysis	SYN Flood Attack Using ippacket, an anomalous packet (with a spoofed IP address) was created and sent repeatedly at a high rate to the victim machine's smtp port. While the attack showed little effect to the overall operation of the machine a potential denial of service against the email capabilities of this system exists. A tcpshow output of the packet is shown below.
Intent	Malicious
Severity	(4+4)-(5+4)=-1 Low

```
Packet 6
IP Header
       Version:                        4
       Header Length:                  20 bytes
       Service Type:             0x00
       Datagram Length:                65 bytes
       Identification:                 0x038B
       Flags:                    MF=off, DF=off
       Fragment Offset:                0
       TTL:                            60
       Encapsulated Protocol:          TCP
       Header Checksum:                0xC94E
       Source IP Address:        1.2.3.4 (<unknown>)
       Destination IP Address:         172.16.1.200 (victim)
TCP Header
       Source Port:              23 (telnet)
       Destination Port:               25 (smtp)
```

```
      Sequence Number:                0000000000
      Acknowledgement Number:         0000000000
      Header Length:                  20 bytes (data=25)
      Flags:                    URG=on,  ACK=on,  PSH=on
                                RST=on,  SYN=on,  FIN=on
      Window Advertisement:           512 bytes
      Checksum:                       0x6CE0
      Urgent Pointer:                 0
TCP Data
      syn flood pack
      <*** Rest of data missing from packet dump ***>
```

Detect 12 – time service

```
Apr 11 02:28:03 fw.victim.net unix: securityalert: udp if=qfe0 from
10.8.12.155:2009 to 10.1.224.2 on unserved port 37
Apr 11 03:28:20 fw.victim.net unix: securityalert: udp if=qfe0 from
10.8.12.155:3822 to 10.1.224.2 on unserved port 37
Apr 11 04:28:59 fw.victim.net unix: securityalert: udp if=qfe0 from
10.8.12.155:1680 to 10.1.224.2 on unserved port 37
```

Active Targeting?	No
Analysis	System trying to query the time service This was puzzling. Several things are wrong here: 1) Port 37 (time) tcp and udp were supposed to be blocked at the router. A quick check of the router's access-list shows that port 37 was not blocked (it is now). 2) Qfe0 is an external (internet) interface. RFC1918 addresses are blocked at the router and that does appear to be working. So where's 10.8.12.155 coming from? 3) 10.1.224.2 is an internal (local lan) interface and 10.8.12.155 would be a valid address on our internal lan, but its showing up on the wrong side of the firewall. 4) A review of the last week of logs shows this error has been occurring hourly for the last 4 days. After a few phone calls, I found that a traffic monitor had been placed on the same hub as the external interface of the firewall (by another team). This monitor had previously been used inside the firewall and was probably not reconfigured before plugging it in. It has been removed.
Intent	Not Malicious
Severity	(5+1)-(5+4)=-3 Low

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced