SANS GCIA Certification

Practical Submission for Phillip Cherbaka

GCIA Practical Assignment v2.8a
Submitted May 5, 2001

Table of Contents

Section 1: Five Detects with Analysis

Background

Detects analyzed within this report were obtained from various systems on a client's network. The network itself utilizes a border router and a firewall which break up the network into three zones: Internal LAN, external (or Internet), and the "DMZ" where publicly accessible Domain Name Servers (DNS) and Web Servers are located. The Internal LAN, home to hosts and clients, uses strict private IP addresses and relies on the firewall's Network Address Translation rules to translate private IP addresses to a single public IP address for all outbound traffic (see below for further explanation). The DMZ zone contains publicly accessible DNS, Web, and Mail servers. Although the MY.NET.3.0 network also appears in the DMZ network, there are no active hosts on this network. Logs were obtained from only a few of the various security-related systems present on this network and were analyzed for suspicious activity:

1. **TCPDump / WinDump**
   A Windows NT Workstation with TCPDump 3.4a6 was placed in the external zone monitoring all traffic entering the network. Logs from this sensor, shown as **IDS1**, contain more detailed information used to further analyze detects other systems throughout the network find.

2. **Check Point Firewall-1 4.1**
   The firewall, denoted as **FW**, performs Network Address Translation (NAT) on Internal LAN IP addresses when they communicate with external hosts. All Internal LAN IP addresses are "hidden" and are seen by external hosts as the same IP address, "MY.NET.1.2".

   When an internal host attempts a connection with an external host, the firewall makes note of the source port of the packet and the internal hosts IP address. Then it substitutes a random high-numbered port for the source port and sends the packet on to the external host. Responses by the external host are sent back to the firewall using that same high-numbered port. The firewall then correlates this high-numbered port

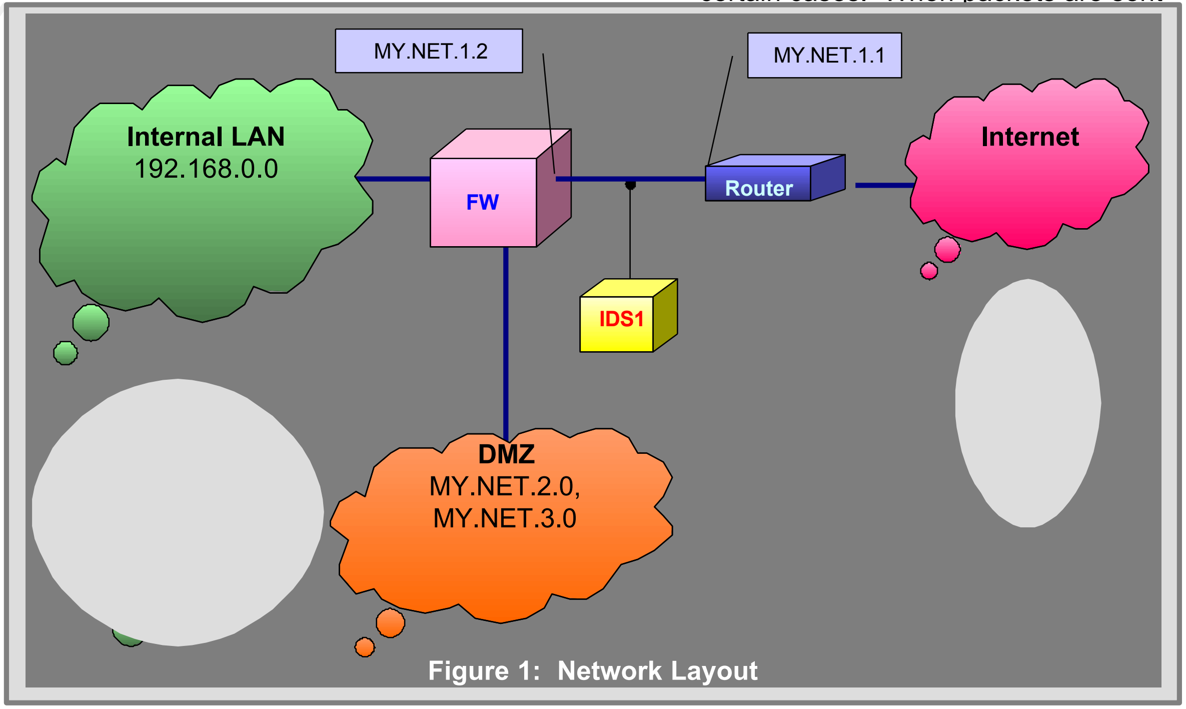


Figure 1: Network Layout

packet with the internal host that initiated the connection in the first place.

While NAT helps to protect internal hosts,

the preceding description shows that it also makes it very difficult to perform intrusion detection and analysis in certain cases. When packets are sent "stimulus" from the internal network. Furthermore, even when an internal host does indeed initiate a connection, IDS's placed outside the firewall cannot distinguish between valid traffic and malicious traffic. False positives are frequent with this setup and it requires careful and methodical analysis of multiple systems to insure proper interpretation of all data.

[redacted]

Trace Captured

TRACE

```
Time         Source           Dest           Protocol and Other Information
6:46:16 AM   213.167.203.26   MY.NET.2.8     icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.63    icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.64    icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.127   icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.128   icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.191   icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.192   icmp: echo request (ttl 232,id 1919)
6:46:16 AM   213.167.203.26   MY.NET.2.255   icmp: echo request (ttl 232,id 1919)
```

SOURCE IDS1 located outside the firewall on client network

GENERATED BY TCPDump v3.4a6 - Trace cleaned up, filtered, sanitized, and re-formatted for display.

Trace Description and Analysis

ATTACK DESCRIPTION This is a probe attempting to get responses from hosts on the target network. There are only five hosts in this network, none of which appear explicitly in the above trace. These broadcast echo requests are a reconnaissance sweep of the subnet trolling for any host that replies.

The timestamp allows us to determine that this is a scripted or automated scan, although not at all sophisticated or stealthy. There is no randomizing of the target addresses nor any attempt keep IDS systems from triggering. Very noisy scan.

What is a bit unusual here is the first destination address of MY.NET.2.8. If the attacker indeed wanted to scan this far down the “subnet food chain”, why don’t we see, for example, a correlating 2.7 to complete the pair as we see in the rest of the scan? In addition, while there is a 2.255, there is no 2.0. Can it be that the attacker mistyped (or miscoded) an 8 for a 0? If this is indeed a scripted scan it seems to require a little work.

ATTACK MECHANISM This probe utilizes icmp (echo) to try to get responses from hosts within a network by sending an echo request to broadcast addresses. In a class C subnet such as this it would require 254 echo requests to map the whole subnet. Instead, the attacker can send echo request to the broadcast address for a subnet. Any host within that subnet broadcast range that receives a packet would normally reply. In class C subnets, some systems respond to echo requests sent to MY.NET.2.0, while others would respond to MY.NET2.255. If the class C network is subnetted further the 63/64, 127/128, and 191/192 pairs function as broadcasts as well; so on and so forth as the network is subnetted even further down.

PROBABILITY SPOOFED SOURCE	HIGH The attacker is trolling for responses from hosts, so it is unlikely that the source IP address is spoofed. IP address registered to an Italian ISP; resolved thru RIPE.net. MED **LOW**

ACTIVE TARGETING	YES These hosts were not actively targeted. Rather, this is a blind scan attempting to find all hosts on a network or it's subnets.
	Trace Analysis

SEVERITY
=(C+L)-(H+N)

Metric
Notes
Rating

Total
Severity

Risk

Criticality (C)
Hosts on this network are DNS and Web servers

1
2
3
4

Risk
7
-2

Lethality (L)
This is only a probe and not an attack. However, it does an adequate job of quickly mapping a network.

1

3
4
5

Defense

Host (H)
The few hosts that are on these networks have hardened operating systems and have most patches installed. Some hosts may need most recent patches applied.

1
2
3
4
5

Defense
9

DEFENSIVE RECOMMENDS: At the border router and/or the firewall, reject or drop all inbound ICMP.

CORRELATION: This is a fairly common probe on the Internet.

Exam Question

QUESTION: The following trace is most probably indicative of what type of activity?

```
6:46:16 AM  213.167.203.26 > MY.NET.2.0:    icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.63:   icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.64:   icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.127:  icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.128:  icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.191:  icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.192:  icmp: echo request (ttl 232,id 1919)
6:46:16 AM  213.167.203.26 > MY.NET.2.255:  icmp: echo request (ttl 232,id 1919)
```

POSSIBLE ANSWERS:

a. Network mapping
b. Random host scan
c. Trace route being run
d. DNS lookup

CORRECT ANSWER

A

Trace Captured

TRACE

```
Time         Source            Prt    Dest            Port   Flags Seq#      Ack             Win     Other
 8:07:01 PM  195.47.94.239.80  >  MY.NET.2.114.1649  R     0:0(0)    ack 674711610   win 0   (ttl id 54923)
 9:02:11 PM  195.47.94.239.80  >  MY.NET.3.46 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 50580)
 9:12:07 PM  195.47.94.239.80  >  MY.NET.3.57 .1649  R     0:0(0)    ack 674711610   win 0   (ttl id 57715)
 9:14:43 PM  195.47.94.239.80  >  MY.NET.2.22 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 29601)
10:29:42 PM  195.47.94.239.80  >  MY.NET.3.104.1649  R     0:0(0)    ack 674711610   win 0   (ttl id 56626)
10:34:38 PM  195.47.94.239.80  >  MY.NET.2.69 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 40824)
11:37:29 PM  195.47.94.239.80  >  MY.NET.3.12 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 28933)
11:50:00 PM  195.47.94.239.80  >  MY.NET.2.116.1794  R     0:0(0)    ack 674711610   win 0   (ttl id 28890)
11:59:56 PM  195.47.94.239.80  >  MY.NET.2.127.1649  R     0:0(0)    ack 674711610   win 0   (ttl id 57192)
12:55:13 AM  195.47.94.239.80  >  MY.NET.3.59 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id  5164)
 1:05:08 AM  195.47.94.239.80  >  MY.NET.3.70 .1649  R     0:0(0)    ack 674711610   win 0   (ttl id 47903)
 1:07:44 AM  195.47.94.239.80  >  MY.NET.2.35 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 44337)
 1:17:41 AM  195.47.94.239.80  >  MY.NET.2.46 .1649  R     0:0(0)    ack 674711610   win 0   (ttl id 16531)
 2:12:57 AM  195.47.94.239.80  >  MY.NET.3.106.1794  R     0:0(0)    ack 674711610   win 0   (ttl id 16112)
 2:27:49 AM  195.47.94.239.80  >  MY.NET.2.82 .1794  R     0:0(0)    ack 674711610   win 0   (ttl id 49088)
....
```

SOURCE IDS1 located outside the firewall on client network

GENERATED BY TCPDump v3.4a6 - Trace cleaned up, filtered, sanitized, and re-formatted for display.

Trace Description and Analysis

ATTACK DESCRIPTION Most likely this trace is due to the use of a DDoS tool called "shaft" (see Correlations below). Based on the ack 674711610, we deduce that these RST ACK packets have been sent to our network in response to a Shaft attack on 195.47.94.239 with MY.NET addresses spoofed as the source.

ATTACK MECHANISM Shaft works very much like TFN or Trinoo in that it has masters, zombies, and targets. A link below under Correlation points to a detailed analysis of how "shaft" works.

PROBABILITY SPOOFED SOURCE The attacker usually uses spoofed addresses in operating this tool. It would seem that the above hosts on MY.NET are unwitting participants in the DoS attack on 195.47.94.239, with our IP addresses being spoofed.

MED

LOW

ACTIVE TARGETING	While hosts on MY.NET were not actively targeted, it would seem that the source is most definitely targeted. NO

Trace Analysis

SEVERITY
=(C+L)-(H+N)

Metric
Notes
Rating

Total
Severity

Risk

Criticality (C)
The few hosts on this network are external DNS and Web servers

1
2
3
4

Risk
7

-1

Lethality (L)
While this is a DoS on the target machine, hosts on MY.NET are seeing relatively little traffic

1

3
4
5

Defense

Host (H)
The few hosts that are on these networks have hardened operating systems and have most patches installed. Some hosts may need most recent patches applied.

1
2
3
4
5

Defense
8

DEFENSIVE RECOMMENDS

1. Configure border routers / firewall to deny all inbound traffic to .
2. Set IDS filters to look for the telltale RESET flag and abnormal ACK numbers.

CORRELATION

Sources discussing Shaft DDoS tool:

- http://www.whitehats.com/info/IDS252
- http://www.sans.org/infosecFAQ/threats/DDoS.htm
- http://www.sans.org/y2k/shaft.htm
- http://biocserver.bioc.cwru.edu/~jose/shaft_analysis/
- http://www.sans.org/y2k/041700.htm
- http://www.sans.org/y2k/032900.htm

Exam Question

QUESTION

The following trace is indicative of what type of activity?

```
245325    8:07:01 PM   195.47.94.239.80 >   MY.NET.2.114.1649    R  0:0(0) ack 674711610
256261    9:02:11 PM   195.47.94.239.80 >   MY.NET.3.46 .1794    R  0:0(0) ack 674711610
270813    9:12:07 PM   195.47.94.239.80 >   MY.NET.3.57 .1649    R  0:0(0) ack 674711610
```

POSSIBLE ANSWERS

a. Scanning for live hosts
b. Scanning for Subseven trojan
c. Shaft DDoS Tool – related Traffic
d. Normal traffic

CORRECT ANSWER

C

[redacted]

Trace Captured

```
TRACE Event   Date      Time      Actn    DstPort Source IP       Dest IP          TCP/UDP
      520665  8-Nov-00  12:13:45  drop    http    bres3.bora.net  MY.NET.1.2       tcp
      520667  8-Nov-00  12:13:45  drop    http    bres3.bora.net  MY.NET.1.10      tcp
      520678  8-Nov-00  12:13:47  drop    http    bres3.bora.net  MY.NET.1.1       tcp
      520694  8-Nov-00  12:13:53  accept  http    bres3.bora.net  MY.NET.2.3       tcp
      520695  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.7       tcp
      520696  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.4       tcp
      520697  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.5       tcp
      520698  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.10      tcp
      520699  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.11      tcp
      520700  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.1       tcp
      520701  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.6       tcp
      520702  8-Nov-00  12:13:53  drop    http    bres3.bora.net  MY.NET.2.8       tcp
      Additional traces: lines deleted for brevity...
      520760  8-Nov-00  12:13:55  drop    http    bres3.bora.net  MY.NET.2.44      tcp
      520761  8-Nov-00  12:13:55  accept  http    bres3.bora.net  MY.NET.2.46      tcp
      520762  8-Nov-00  12:13:55  drop    http    bres3.bora.net  MY.NET.2.45      tcp
      Additional traces: lines deleted for brevity...
      520996  8-Nov-00  12:13:58  drop    http    bres3.bora.net  MY.NET.2.201     tcp
      520997  8-Nov-00  12:13:58  accept  http    bres3.bora.net  MY.NET.2.203     tcp
      520998  8-Nov-00  12:13:58  drop    http    bres3.bora.net  MY.NET.2.207     tcp
      Additional traces: lines deleted for brevity...
      521096  8-Nov-00  12:14:00  drop    http    bres3.bora.net  MY.NET.2.241     tcp
      521097  8-Nov-00  12:14:00  drop    http    bres3.bora.net  MY.NET.2.247     tcp
      521098  8-Nov-00  12:14:00  drop    http    bres3.bora.net  MY.NET.2.245     tcp
      Additional traces: lines deleted for brevity...
      First probe of ports shown completely...
      521406  8-Nov-00  12:15:59  drop    32773   bres3.bora.net  MY.NET.1.10      tcp
      521407  8-Nov-00  12:15:59  drop    32778   bres3.bora.net  MY.NET.1.10      tcp
      521408  8-Nov-00  12:15:59  drop    32776   bres3.bora.net  MY.NET.1.10      tcp
      521409  8-Nov-00  12:15:59  drop    32771   bres3.bora.net  MY.NET.1.10      tcp
      521410  8-Nov-00  12:15:59  drop    ftp     bres3.bora.net  MY.NET.1.10      tcp
      521411  8-Nov-00  12:15:59  drop    32772   bres3.bora.net  MY.NET.1.10      tcp
      521412  8-Nov-00  12:15:59  drop    32774   bres3.bora.net  MY.NET.1.10      tcp
      521413  8-Nov-00  12:15:59  drop    32775   bres3.bora.net  MY.NET.1.10      tcp
      521414  8-Nov-00  12:15:59  drop    telnet  bres3.bora.net  MY.NET.1.10      tcp
      521423  8-Nov-00  12:16:01  drop    32773   bres3.bora.net  MY.NET.1.10      tcp
      521424  8-Nov-00  12:16:01  drop    32778   bres3.bora.net  MY.NET.1.10      tcp
      521425  8-Nov-00  12:16:01  drop    32776   bres3.bora.net  MY.NET.1.10      tcp
      521426  8-Nov-00  12:16:01  drop    32775   bres3.bora.net  MY.NET.1.10      tcp
      521427  8-Nov-00  12:16:01  drop    32779   bres3.bora.net  MY.NET.1.10      tcp
      521428  8-Nov-00  12:16:01  drop    ftp     bres3.bora.net  MY.NET.1.10      tcp
      521429  8-Nov-00  12:16:01  drop    32772   bres3.bora.net  MY.NET.1.10      tcp
      521430  8-Nov-00  12:16:01  drop    32774   bres3.bora.net  MY.NET.1.10      tcp
      521431  8-Nov-00  12:16:01  drop    telnet  bres3.bora.net  MY.NET.1.10      tcp
      521432  8-Nov-00  12:16:01  drop    32777   bres3.bora.net  MY.NET.1.10      tcp
      521439  8-Nov-00  12:16:02  drop    32778   bres3.bora.net  MY.NET.1.10      tcp
      521440  8-Nov-00  12:16:02  drop    32776   bres3.bora.net  MY.NET.1.10      tcp
```

```
TRACE  (continued from previous page)
(cont) Event   Date     Time     Actn   DstPort Source IP      Dest IP        TCP/UDP
       521441  8-Nov-00 12:16:02 drop   32775   bres3.bora.net MY.NET.1.10    tcp
       521442  8-Nov-00 12:16:02 drop   ftp     bres3.bora.net MY.NET.1.10    tcp
       521443  8-Nov-00 12:16:02 drop   32773   bres3.bora.net MY.NET.1.10    tcp
       521444  8-Nov-00 12:16:02 drop   telnet  bres3.bora.net MY.NET.1.10    tcp
       521445  8-Nov-00 12:16:02 drop   32772   bres3.bora.net MY.NET.1.10    tcp
       521446  8-Nov-00 12:16:02 drop   32774   bres3.bora.net MY.NET.1.10    tcp
       521447  8-Nov-00 12:16:02 drop   32779   bres3.bora.net MY.NET.1.10    tcp
       521448  8-Nov-00 12:16:02 drop   32777   bres3.bora.net MY.NET.1.10    tcp
       521460  8-Nov-00 12:16:03 drop   32779   bres3.bora.net MY.NET.1.10    tcp
       521461  8-Nov-00 12:16:03 drop   32777   bres3.bora.net MY.NET.1.10    tcp
       521468  8-Nov-00 12:16:05 drop   32779   bres3.bora.net MY.NET.1.10    tcp
       521469  8-Nov-00 12:16:05 drop   32772   bres3.bora.net MY.NET.1.10    tcp
       521470  8-Nov-00 12:16:05 drop   32775   bres3.bora.net MY.NET.1.10    tcp
       521471  8-Nov-00 12:16:05 drop   32778   bres3.bora.net MY.NET.1.10    tcp
       521472  8-Nov-00 12:16:05 drop   32773   bres3.bora.net MY.NET.1.10    tcp
       521473  8-Nov-00 12:16:05 drop   ftp     bres3.bora.net MY.NET.1.10    tcp
       521474  8-Nov-00 12:16:05 drop   32777   bres3.bora.net MY.NET.1.10    tcp
       521475  8-Nov-00 12:16:05 drop   23      bres3.bora.net MY.NET.1.10    tcp
       521476  8-Nov-00 12:16:05 drop   32774   bres3.bora.net MY.NET.1.10    tcp
       521477  8-Nov-00 12:16:05 drop   32776   bres3.bora.net MY.NET.1.10    tcp
       521478  8-Nov-00 12:16:07 drop   32777   bres3.bora.net MY.NET.1.10    tcp
       521479  8-Nov-00 12:16:07 drop   telnet  bres3.bora.net MY.NET.1.10    tcp
       521480  8-Nov-00 12:16:07 drop   32776   bres3.bora.net MY.NET.1.10    tcp
       521481  8-Nov-00 12:16:07 drop   ftp     bres3.bora.net MY.NET.1.10    tcp
       521482  8-Nov-00 12:16:07 drop   32779   bres3.bora.net MY.NET.1.10    tcp
       521483  8-Nov-00 12:16:07 drop   32774   bres3.bora.net MY.NET.1.10    tcp
       521484  8-Nov-00 12:16:07 drop   32775   bres3.bora.net MY.NET.1.10    tcp
       521485  8-Nov-00 12:16:07 drop   32772   bres3.bora.net MY.NET.1.10    tcp
       521486  8-Nov-00 12:16:07 drop   32778   bres3.bora.net MY.NET.1.10    tcp
       521487  8-Nov-00 12:16:07 drop   32773   bres3.bora.net MY.NET.1.10    tcp
       521493  8-Nov-00 12:16:08 drop   32777   bres3.bora.net MY.NET.1.10    tcp
       521494  8-Nov-00 12:16:08 drop   telnet  bres3.bora.net MY.NET.1.10    tcp
       521495  8-Nov-00 12:16:08 drop   32772   bres3.bora.net MY.NET.1.10    tcp
       521496  8-Nov-00 12:16:08 drop   ftp     bres3.bora.net MY.NET.1.10    tcp
       521497  8-Nov-00 12:16:08 drop   32779   bres3.bora.net MY.NET.1.10    tcp
       521498  8-Nov-00 12:16:08 drop   32775   bres3.bora.net MY.NET.1.10    tcp
       521499  8-Nov-00 12:16:08 drop   32774   bres3.bora.net MY.NET.1.10    tcp
       521500  8-Nov-00 12:16:08 drop   32776   bres3.bora.net MY.NET.1.10    tcp
       521501  8-Nov-00 12:16:08 drop   32778   bres3.bora.net MY.NET.1.10    tcp
       521502  8-Nov-00 12:16:08 drop   32773   bres3.bora.net MY.NET.1.10    tcp
       Additional traces: only first packet and other interesting traffic shown...
       521975  8-Nov-00 12:18:25 drop   32773   bres3.bora.net MY.NET.2.2     tcp
       522064  8-Nov-00 12:18:31 drop   43008   bres3.bora.net MY.NET.2.2     tcp
       522065  8-Nov-00 12:18:31 drop   43008   bres3.bora.net MY.NET.2.2     tcp
       522066  8-Nov-00 12:18:31 drop   43008   bres3.bora.net MY.NET.2.2     tcp
       522067  8-Nov-00 12:18:31 drop   43008   bres3.bora.net MY.NET.2.2     udp
```

TRACE (cont)

```
(continued from previous page)
Event    Date      Time      Actn    DstPort Source IP        Dest IP          TCP/UDP
Additional traces: only first packet and other interesting traffic shown...
522111   8-Nov-00  12:18:47  drop    32778   bres3.bora.net   MY.NET.2.3       tcp
522188   8-Nov-00  12:18:53  drop    39115   bres3.bora.net   MY.NET.2.3       tcp
522189   8-Nov-00  12:18:53  drop    39115   bres3.bora.net   MY.NET.2.3       tcp
522190   8-Nov-00  12:18:53  drop    39115   bres3.bora.net   MY.NET.2.3       tcp
522191   8-Nov-00  12:18:53  drop    39115   bres3.bora.net   MY.NET.2.3       udp
Additional traces: only first packet and other interesting traffic shown...
522417   8-Nov-00  12:19:44  drop    32773   bres3.bora.net   MY.NET.2.46      tcp
522506   8-Nov-00  12:19:49  drop    38717   bres3.bora.net   MY.NET.2.46      tcp
522507   8-Nov-00  12:19:49  drop    38717   bres3.bora.net   MY.NET.2.46      tcp
522508   8-Nov-00  12:19:49  drop    38717   bres3.bora.net   MY.NET.2.46      udp
522509   8-Nov-00  12:19:49  drop    38717   bres3.bora.net   MY.NET.2.46      tcp
Additional traces: only first packet and other interesting traffic shown...
522572   8-Nov-00  12:20:00  drop    ftp     bres3.bora.net   MY.NET.2.203     tcp
522671   8-Nov-00  12:20:06  drop    41852   bres3.bora.net   MY.NET.2.203     tcp
522672   8-Nov-00  12:20:06  drop    41852   bres3.bora.net   MY.NET.2.203     udp
522673   8-Nov-00  12:20:06  drop    41852   bres3.bora.net   MY.NET.2.203     tcp
522674   8-Nov-00  12:20:06  drop    41852   bres3.bora.net   MY.NET.2.203     tcp
522743   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.251     tcp
522744   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.249     tcp
522745   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.253     tcp
522746   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.250     tcp
522747   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.252     tcp
522748   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.254     tcp
522749   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.2.0       tcp
522750   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.3.0       tcp
522751   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.3.1       tcp
522752   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.3.11      tcp
522753   8-Nov-00  12:20:17  drop    http    bres3.bora.net   MY.NET.3.16      tcp
Additional traces: lines deleted for brevity...
523004   8-Nov-00  12:20:20  drop    http    bres3.bora.net   MY.NET.3.239     tcp
523005   8-Nov-00  12:20:20  drop    http    bres3.bora.net   MY.NET.3.247     tcp
523006    8-Nov-00 12:20:20  drop    http    bres3.bora.net   MY.NET.3.254     tcp
```

SOURCE FW on client network

GENERATED BY Check Point FireWall-1: Trace cleaned up, filtered, sanitized, and re-formatted for display

Trace Description and Analysis

ATTACK DESCRIPTION

This extremely noisy probe seems to encompass various techniques and scans. The attacker, resolved to a Korean company, initially scans for web servers (and possibly other services not logged by firewall – details below) in a somewhat random order. Upon getting responses from servers on the networks, a targeted scan of each host that responded is run in search of vulnerabilities. Timestamps indicate an automated attack. The targeted ports in the port scans include **FTP**, **Telnet**, vulnerable **Solaris RPC ports** (32771-32779), and other **unknown ports** (38717, 39115, 41852 and 43008).

It is important to note that while only **three** hosts responded to the initial HTTP probe (2.3, 2.46, and 2.203 responded), **five** total hosts were targeted for further port scans (1.10 and 2.2 in addition to the aforementioned three). The only port 1.10 listens to is SMTP (mail relay) and the only port 2.2 listens to is DNS-UDP (DNS server). Why did the attacker port-scan these two hosts if they did not respond to the HTTP scan? There must be something else the attacker is using to illicit responses that were not captured in the firewall logs. A careful review of firewall logging policies showed that both SMTP and DNS-UDP traffic were NOT BEING LOGGED due to the sheer volume of SMTP and DNS-UDP traffic on the network. So it is possible that the attacker's initial scan also searched for listening SMTP and DNS ports. On the other hand, both of these hosts are listed in the organizations DNS records; anyone can easily determine which server is the mail relay (using the MX record) and which servers are the DNSs (using the NS records) from these entries. So it is also possible that the attacker used this public information for his attack list. However, if he did then he didn't need to also probe 2.3, 2.46, and 2.203 since these three are also listed in the DNS records. Therefore, one must conclude that the attacker was also probing for SMTP and DNS ports, both of which were not in the trace since the firewall was not logging this type of traffic.

There are other peculiarities in the traces. For each host that was port scanned (except one), seemingly random and unknown ports were also scanned with both TCP and UDP protocols. These random target ports were 38717, 39115, 41852 and 43008. There are no known trojans or correlations for these ports on SANS or various other security web sites searched. Are these anomalies of or bugs in the automated attacker program, or are these scans for new trojans or new ports used for existing trojans? A search of the SANS GIAC and many other security-related web sites failed to turn up any meaningful information on these scans.

IDS1, running TCPDump, was offline and was not capturing data during the period this attack was logged; surely the highly detailed logs from TCPDump would have been instrumental in ascertaining the nature of these probes. Lesson learned from this experience is to always have a backup IDS system online to insure network coverage in case the primary IDS needs to be serviced.

ATTACK MECHANISM

First, an HTTP probe (and probably other ports) is performed to each IP address on a network. Next, any host that responded to the initial probe is then scanned for open FTP, Telnet, or vulnerable Solaris rpc services (32771-32779). The initial HTTP probe does not complete before the host probes begin. The HTTP probe was more than half complete before it was stopped and port scans were performed on five hosts that responded to the initial probes. This could signify an automated scan giving the attacker live feedback of which hosts responded, data which he then used to manually or automatically launch further targeted port scans.

1. **First host** probed for FTP, Telnet and vulnerable Solaris RPC ports (32771-32779). All ports were probed multiple times for some reason. It is possible the attacker was using an application to initiate a connection? Applications are usually ambivalent to the risks of retrying connections numerous times. Or is the automated attack tool's author the one who's ambivalent?
2. **Second host** probed for the above ports multiple times as well as 43008. 43008/TCP 3 times followed by a single 43008/UDP probe.
3. **Third host** probed for the above ports multiple times as well as 39115. 39115/TCP 3 times followed by a single 39115/UDP probe.
4. **Fourth host** probed for the above ports multiple times as well as 38717. 38717/TCP 3 times followed by a single 38717/UDP probe.
5. **Fifth host** probed for the above ports multiple times as well as 41852. 41852/TCP 3 times followed by a single 41852/UDP probe.

After these port scans were completed, an HTTP scan continued for the remaining hosts in the 2.0 and 3.0 networks. Unclear why ports 38717, 39115, 41852 and 43008 TCP and UDP were probed.

PROBABILITY SPOOFED SOURCE

HIGH

Since the attacker needs responses from hosts for later attack, it is unlikely that the source IP address is spoofed. IP address registered to a Korean company; resolved via ARIN.net. Probes and attacks from Korean networks are apparently historically prevalent.

MED

LOW

ACTIVE TARGETING	While scans of the subnets was not targeted, subsequent targeted port scans were performed on hosts that responded to the initial network scans. NO

Trace Analysis

SEVERITY
=(C+L)-(H+N)

Metric
Notes
Rating

Total
Severity

Risk

Criticality (C)
The few hosts on this network are external DNS and Web servers
1
2
3
4

Risk
8
-1

Lethality (L)
This is a general network scan as well as a highly targeted probe.
1
2

4
5

Defense

Host (H)
The hosts that were targeted have hardened operating systems and have patched services. However, some of the most recent patches may still need to be applied.
1
2
3
4
5

Defense
9

DEFENSIVE RECOMMENDATION

1. At the firewall, block access to ports 32771-32779.
2. Unless utilized, block access to FTP and Telnet at the firewall or border router.
3. Regularly review security logs for signs of probes.

CORRELATION

No correlations found for this particular network probe and subsequent host probes. Some correlations for possible vulnerabilities the port scans were searching for:

- GIAC Detects Analyzed: 16 Feb 2000: http://www.sans.org/y2k/021600.htm
- GIAC Detects Analyzed: 18 Feb 2000: http://www.sans.org/y2k/021800-1600.htm
- GIAC Detects Analyzed: 23 Feb 2000: http://www.sans.org/y2k/022300.htm
- GIAC Detects Analyzed: 23 Jun 2000: http://www.sans.org/y2k/062300.htm
- GIAC Detects Analyzed: 15 Sep 2000: http://www.sans.org/y2k/091500.htm
- CVE (cve.mitre.org): CVE-1999-0003, CVE-1999-0003, CAN-1999-0631, CAN-1999-0632

Exam Question

QUESTION

In the following trace, what vulnerable services are being scanned for?

```
Event   Date      Time     Action DstPrt Source          Dest            Proto
521406  8-Nov-00  12:15:59 drop   32773  bres3.bora.net  MY.NET.1.10     tcp
521407  8-Nov-00  12:15:59 drop   32778  bres3.bora.net  MY.NET.1.10     tcp
521408  8-Nov-00  12:15:59 drop   32776  bres3.bora.net  MY.NET.1.10     tcp
521409  8-Nov-00  12:15:59 drop   32771  bres3.bora.net  MY.NET.1.10     tcp
521411   8-Nov-00 12:15:59 drop   32772  bres3.bora.net  MY.NET.1.10     tcp
```

CORRECT ANSWER

B

POSSIBLE ANSWERS

a. Back Orifice default ports
b. Possible rpc service ports
c. Trinoo DDoS default ports
d. None of the above

Trace Captured

Note that only **1.2** and **1.10** were scanned, then the whole **2.0** network, and finally only the first 40 IP addresses in the **3.0** network.

```
TRACE Event   Date       Time     Actn    DestPort     Source IP                Dest IP       TCP/UDP
      248981  5-Nov-00   3:27:49  drop    smtp         203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248983  5-Nov-00   3:27:49  drop    name         203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248984  5-Nov-00   3:27:49  drop    time-tcp     203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248986  5-Nov-00   3:27:49  drop    telnet       203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248987  5-Nov-00   3:27:49  drop    ftp          203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248988  5-Nov-00   3:27:49  drop    netstat      203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248993  5-Nov-00   3:27:52  drop    daytime-tcp  203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248994  5-Nov-00   3:27:52  drop    systat       203-109-163-24.ihug.net  MY.NET.1.2    tcp
      248995  5-Nov-00   3:27:52  drop    discard-tcp  203-109-163-24.ihug.net  MY.NET.1.2    tcp
      249003  5-Nov-00   3:28:17  drop    smtp         203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249006  5-Nov-00   3:28:19  drop    name         203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249007  5-Nov-00   3:28:19  drop    time-tcp     203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249010  5-Nov-00   3:28:20  drop    telnet       203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249011  5-Nov-00   3:28:20  drop    ftp          203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249012  5-Nov-00   3:28:20  drop    netstat      203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249013  5-Nov-00   3:28:20  drop    daytime-tcp  203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249014  5-Nov-00   3:28:20  drop    systat       203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249015  5-Nov-00   3:28:20  drop    discard-tcp  203-109-163-24.ihug.net  MY.NET.1.10   tcp
      249281  5-Nov-00   3:39:59  drop    smtp         203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249282  5-Nov-00   3:39:59  drop    whois        203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249283  5-Nov-00   3:39:59  drop    name         203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249284  5-Nov-00   3:39:59  drop    time-tcp     203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249286  5-Nov-00   3:40:00  drop    telnet       203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249287  5-Nov-00   3:40:00  drop    ftp          203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249288  5-Nov-00   3:40:01  drop    netstat      203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249289  5-Nov-00   3:40:01  drop    daytime-tcp  203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249290  5-Nov-00   3:40:01  drop    systat       203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249292  5-Nov-00   3:40:02  drop    discard-tcp  203-109-163-24.ihug.net  MY.NET.2.1    tcp
      249293  5-Nov-00   3:40:02  drop    smtp         203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249298  5-Nov-00   3:40:03  drop    name         203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249299  5-Nov-00   3:40:03  drop    time-tcp     203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249301  5-Nov-00   3:40:04  drop    telnet       203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249302  5-Nov-00   3:40:04  drop    ftp          203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249303  5-Nov-00   3:40:04  drop    netstat      203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249304  5-Nov-00   3:40:05  accept  daytime-tcp  203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249305  5-Nov-00   3:40:05  drop    systat       203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249306  5-Nov-00   3:40:05  drop    discard-tcp  203-109-163-24.ihug.net  MY.NET.2.2    tcp
      249307  5-Nov-00   3:40:06  drop    smtp         203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249310  5-Nov-00   3:40:07  drop    name         203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249311  5-Nov-00   3:40:07  drop    time-tcp     203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249313  5-Nov-00   3:40:07  drop    telnet       203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249314  5-Nov-00   3:40:08  drop    ftp          203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249315  5-Nov-00   3:40:08  drop    netstat      203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249316  5-Nov-00   3:40:08  accept  daytime-tcp  203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249317  5-Nov-00   3:40:08  drop    systat       203-109-163-24.ihug.net  MY.NET.2.3    tcp
      249318  5-Nov-00   3:40:09  drop    discard-tcp  203-109-163-24.ihug.net  MY.NET.2.3    tcp
```

(continued next page)

TRACE (continued from previous page)

(cont)

```
Event   Date      Time     Actn  DestPort     Source IP                 Dest IP      TCP/UDP
249319  5-Nov-00  3:40:10  drop  smtp         203-109-163-24.ihug.net  MY.NET.2.4   tcp
249320  5-Nov-00  3:40:10  drop  whois        203-109-163-24.ihug.net  MY.NET.2.4   tcp
249321  5-Nov-00  3:40:10  drop  name         203-109-163-24.ihug.net  MY.NET.2.4   tcp
249322  5-Nov-00  3:40:10  drop  time-tcp     203-109-163-24.ihug.net  MY.NET.2.4   tcp
249326  5-Nov-00  3:40:11  drop  telnet       203-109-163-24.ihug.net  MY.NET.2.4   tcp
249327  5-Nov-00  3:40:11  drop  ftp          203-109-163-24.ihug.net  MY.NET.2.4   tcp
249328  5-Nov-00  3:40:11  drop  netstat      203-109-163-24.ihug.net  MY.NET.2.4   tcp
249330  5-Nov-00  3:40:12  drop  daytime-tcp  203-109-163-24.ihug.net  MY.NET.2.4   tcp
249331  5-Nov-00  3:40:12  drop  systat       203-109-163-24.ihug.net  MY.NET.2.4   tcp
249333  5-Nov-00  3:40:13  drop  discard-tcp  203-109-163-24.ihug.net  MY.NET.2.4   tcp
Additional traces: lines deleted for brevity...
251528  5-Nov-00  3:51:24  drop  smtp         203-109-163-24.ihug.net  MY.NET.3.40  tcp
251529  5-Nov-00  3:51:24  drop  whois        203-109-163-24.ihug.net  MY.NET.3.40  tcp
251530  5-Nov-00  3:51:25  drop  name         203-109-163-24.ihug.net  MY.NET.3.40  tcp
251531  5-Nov-00  3:51:26  drop  time-tcp     203-109-163-24.ihug.net  MY.NET.3.40  tcp
251533  5-Nov-00  3:51:26  drop  telnet       203-109-163-24.ihug.net  MY.NET.3.40  tcp
251534  5-Nov-00  3:51:26  drop  ftp          203-109-163-24.ihug.net  MY.NET.3.40  tcp
251535  5-Nov-00  3:51:27  drop  netstat      203-109-163-24.ihug.net  MY.NET.3.40  tcp
251536  5-Nov-00  3:51:27  drop  daytime-tcp  203-109-163-24.ihug.net  MY.NET.3.40  tcp
251537  5-Nov-00  3:51:27  drop  systat       203-109-163-24.ihug.net  MY.NET.3.40  tcp
251538  5-Nov-00  3:51:27  drop  discard-tcp  203-109-163-24.ihug.net  MY.NET.3.40  tcp
```

SOURCE FW on client network

GENERATED BY Check Point FireWall-1: Trace cleaned up, filtered, sanitized, and re-formatted for display

Trace Description and Analysis

ATTACK DESCRIPTION

This noisy probe is attempting to get responses from any host on the target networks for various services. Vulnerable services searched for are:

Service	Port	Service	Port
DISCARD-TCP	9	NAME	53
SYSTAT	11	NETSTAT	15
FTP	21	TIME-TCP	37
TELNET	23	DAYTIME-TCP	13
SMTP	25	WHOIS	513?

Note that the firewall dropped all packets except for two daytime-tcp packets which were responded to by the hosts. An examination of the firewall rules showed this port was open on these two hosts, apparently from past tests performed after which the ports were not closed.

ATTACK MECHANISM

This probe seems to be an unsophisticated attempt at locating open ports within a list of ten. It is extremely fast and steps through every host on the networks sequentially without any attempt to randomize or otherwise obfuscate it's presence. Very noisy scans are sometimes precursors to more sophisticated attacks, or simply deceptive exercises.

PROBABILITY SPOOFED SOURCE	HIGH The attacker is looking for responses from hosts, so it is unlikely that the source IP address is spoofed. IP address registered to an ISP in New Zealand; resolved thru APNIC.net MED **LOW**
ACTIVE TARGETING	YES These hosts were not actively targeted. This is a blind scan attempting to find specific vulnerable services on all hosts on the network.
	Trace Analysis

SEVERITY
=(C+L)-(H+N)

Metric
Notes
Rating

Total
Severity

Risk

Criticality (C)
The few hosts on this network are external DNS and Web servers

1
2
3
4

8

-1

Lethality (L)
While few of these services probed for are allowed in, a couple hosts did apparently respond to some exploitable services.

1
2

4
5

Defense

Host Countrmsr (H)
The few hosts that are on this network have hardened operating systems and are up-to-date with patches. Some hotfixes may still need to be applied.

1
2
3
4
5

9

DEFENSIVE RECOMMENDATION	1. At the firewall, block access to any port not used. 2. Regularly review security logs for signs of probes.	
CORRELATION	These types of “shotgun” probes are fairly common on the Internet.	
	Exam Question	
QUESTION	A rapid stream of packets from a single external address bound for multiple hosts in succession (.1, .2, .3, .4, etc) to the FTP, DNS, SMTP and Telnet ports signifies:	CORRECT ANSWER
POSSIBLE ANSWERS	a. Typical host scan b. Back Orifice communication with internal hosts c. SubSeven probe of hosts d. IRC traffic	**A**

Trace Captured

TRACE

```
Date        Time      Message-Type   User-Name   Caller-ID           Authen-Failure-Code
3/6/2001    1:24:18   Authen failed  ` L         7035552850          External DB user invalid or bad passsword
3/6/2001    1:24:43   Authen failed  ` L         7035552850          External DB user invalid or bad passsword
3/12/2001   23:13:23  Authen failed  ` L         4105553219          External DB user invalid or bad passsword
3/12/2001   23:13:34  Authen failed  ` L         4105553219          External DB user invalid or bad passsword
3/30/2001   11:17:48  Authen failed  ` L         7035556030          External DB user invalid or bad passsword
3/30/2001   11:17:51  Authen failed  ~?~?~?~?~?  7035556030          Unknown
4/4/2001    2:59:29   Authen failed  ` L         6195553861          External DB user invalid or bad passsword
4/4/2001    3:00:43   Authen failed  ` L         6195553861          External DB user invalid or bad passsword
4/8/2001    0:10:31   Authen failed  ]|r)F{i     2065552000          External DB user invalid or bad passsword
```

SOURCE Logs from RAS located inside the firewall on client network

GENERATED BY Cisco AS5300 - Trace cleaned up, filtered, sanitized, and re-formatted for display (and to protect the innocent).

Trace Description and Analysis

ATTACK DESCRIPTION The above trace is from the logs of a Cisco AS5300, a Remote Access Server (RAS), which allows network users to dial in using POTS or ISDN and use network resources while on travel. The RAS box forces users to authenticate using a username and password. It is unclear at this time if the above is an attack or simply a user misdialing, mistyping, or using an incorrect front-end to dial. However, it seems a bit suspicious given that the calls usually happen around midnight, have a certain user-name signature, and never try more than twice per session. Phone numbers which weren't unlisted were traced back to hotels in Washington state and San Diego, (using Switchboard.com).

ATTACK MECHANISM This seems to be a slow methodical attempt to log in to a network via dial-in systems. It does not appear to be scripted based on the date/time signatures, although it could be.

PROBABILITY HIGH

SPOOFED SOURCE Since this system uses Caller ID to list the originating phone number, it is unlikely that the originating phone numbers can be spoofed or faked.

MED

LOW

Trace Analysis

SEVERITY
=(C+L)-(H+N)

Metric
Notes
Rating

Total
Severity

Risk

Criticality (C)
This RAS device gives access to network resources upon authentication
1
2
3
4

Risk
7
-1

Lethality (L)
This seems to be a slow search for dial-in username with weak passwords
1

3
4
5

Defense

Host (H)
The RAS device is regularly patched and employs various methods of authenticating usernames
1
2
3
4
5

Defense
8

DEFENSIVE RECOMMENDS	1. Tighten firewall rules from RAS to internal network 2. Review logs for and track failed authentications. 3. Employ token-based authentication for RAS access	
CORRELATION	The RAS logs have not been reviewed until recently, and these are the only entries. No external correlations were found.	
	Exam Question	
QUESTION	Dial-in servers (or Remote Access Servers) are never targets of probes or attacks?	CORRECT ANSWER **F**
POSSIBLE ANSWERS	T. True F. False	

Section 2: Detailed Evaluation of an Attack: Data Synchronization Sites

Background
What is an attack? What is an exploit tool? Reading most analysts' practicals on the GIAC site, one would be led to believe that attacks are usually launched from outside the network, and exploit tools are generally those that look for or exploit vulnerabilities.

However, according to many studies the majority of "attacks" occur from within a network. Furthermore, the majority of corporate data loss is NOT from hackers or the use of hacker tools, but from internal sources either electronically or physically stealing information or sabotaging data / systems. Our job as information security professionals is ultimately to allow our organizations to do business. And we do that within our scope by focusing on mainly three things:

1. Preventing the loss or divulgence of sensitive/private corporate information,
2. Preventing a denial of service for our employees or our customers, and
3. Prevent network resource from being unwitting attackers against others.

It is my experience that we in information security should worry just as much about someone purposely or inadvertently disseminating sensitive corporate information as we do about the latest and greatest attack tool or vulnerability that comes in vogue.

While many analysts are watching traffic entering and leaving their networks, scouring logs looking for suspicious traffic from external sources, very few watch non-suspicious traffic such as HTTP leaving their networks. In fact, most corporations' firewall rules allow all internal clients to use HTTP (80) and HTTPS (443) unfettered to any and every Internet site.

The Tools
With the above in mind, I decided to evaluate something completely different. Besides, most of the fun stuff had already been analyzed. I want to analyze one method that corporate data can be lost – the operation of *Personal Data Synchronization* applications from within corporate networks. Many people use these tools in conducting day-to-day business. They allow the synchronization of data on a work computer, home computer, laptop, PDA, mobile phone, etc. via a **web site** that can be reached from anywhere Internet access is available. There are numerous such sites, but I will concentrate on one called *FusionOne* found at http://www.fusionone.com. This is a very convenient and powerful tool, allowing one to synchronize email, contacts, to-do lists, calendar, bookmarks, etc AND data files from a variety of sources such as Microsoft Outlook and other applications and sources.

So What's the Problem?
So what's potentially dangerous in running these tools? There are a couple of concerns that I will highlight:

1. Danger of the synchronization web sites getting hacked. Within the last 18 months many web sites, including those run by very reputable companies with big security staffs, have been hacked. It would seem that if someone hacked the FusionOne web site it would be a treasure trove of corporate information. After all, each individual's data is protected only by a username and password.

2. Maybe more importantly (and what I will concentrate on in this report) is the potential for sensitive data to leave the corporate network under common conditions, bypassing security controls.

3. Possibility of similar tools with malicious intent distributed to unsuspecting users, working in the background and using HTTP/HTTPS for all

communications.

These tools make it really easy for the loss of corporate data to occur; the **MASS** transfer of corporate information out of the corporate network and onto individual's personal computers and laptops on a regular and automatic basis where it is easier for that data to be compromised.

But Data Already Leaves the Network

While data can leave the corporate network via laptop, ZIP disks, email, printouts, etc those methods usually:

a. Take some form of direct intervention by the user (for example copying files to a ZIP disk)
b. Are not usually conducive for the transfer of LARGE amounts of data (for example, 10GB of corporate accounting data).
c. Require frequent work by the individual to keep data updated.

These data synchronization tools allow the automatic and frequent transfer of large amounts of data out of the corporate network on a regular basis is facilitated. This data usually is transferred to various individual's home computers and laptops, continuously and automatically with little if any notice by the individual or the security staff. With a corporate T-3 and a user's DSL, both always on, and the use of these tools running on HTTP/HTTPS, it is a rather simple and unobtrusive task for a user (such as an accountant who likes to work at home) to continuously synchronize the corporate accounting network drive and have that 10GB of CURRENT data reside on his home computer. Once that data is on a user's home computer/laptop it is vulnerable to disclosure since that user most probably does not employ even a fraction of the security controls usually found on corporate networks. Furthermore, that individual may have allowed some other programs (such as Napster) with known vulnerabilities to operate unfettered on the same computer. The types of data that most people synchronize (mail inboxes, data on corporate computers, data on corporate drives, etc) means that a lot of sensitive data is available outside any security controls that the corporation may have set up to protect that data in the first place.

Give Me A Scenario

Let’s evaluate two possibly common scenarios with the use of these tools (FusionOne used as example):

Scenario 1

a. Joe Shmoe just got DSL installed at home and his Internet access is now magnitudes faster than his 56k modem. However, the corporate network does not allow access to resources over the Internet, but rather forces users to dial in (usually over 56k modem lines). They are working on installing VPNs that will give users secure remote access to the corporate network from the Internet, but it’s still months away.
b. Joe’s not too happy about waiting months in order to work at home, nor does he relish the idea of dialing in over a 56k line. So he uses FusionOne at work to get his Outlook information, including emails in his Inbox, and a few work directories synchronized so that he can access them at home.
c. Joe’s home computer, always connected to the Internet via DSL, doesn’t have a personal firewall installed.
d. In addition, his son is a frequent user of Napster and Gnutella and has shared out dad’s hard drive at the root level. While at this point Joe’s personal data is also at risk, the risk to corporate sensitive information is really what concerns us.

Scenario 2

a. Jane Shmoe is frequently on the road due on business. She found out about FusionOne from her husband and also installed it at work and on her work laptop, sync’ing all sorts of data.
b. On one of her business trips to Seattle where she was to give a briefing to a corporation her company may be partnering with, her laptop somehow got rained on and was no longer functional.
c. Not panicking, she utilizes one of that company’s desktop computers to sync back to FusionOne. The sync is successful and she

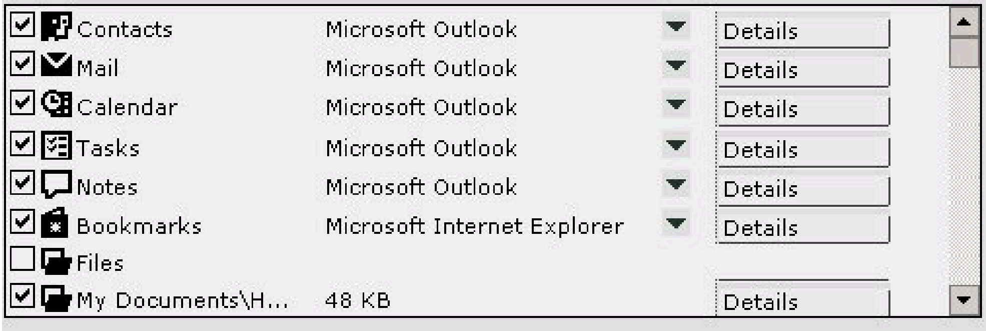
retrieves the briefing and asks it to be placed on the Presentation computer in the conference room.

d. In her haste she forgets to uninstall FusionOne. At this point, her company's data that was sync'ed is at risk of being shared out and will always be automatically updated.

FusionOne Capabilities

The FusionOne application can be downloaded from the FusionOne web site and installed locally. Most corporations either use versions of Windows that have little control to prohibit users from installing applications without authorization, or choose not to use those features in versions of Windows that do have those controls.

There are various settings within FusionOne that can be manipulated as needed by the user. Figure 2 is a snapshot of the various types of data that can be synchronized. Note that any number of file directories, local or networked, can also be synchronized. Various other options are available such as scheduling transactions, automating the login process, and setting up proxy use. Note that the application does not ask for passwords to access data in such applications as Microsoft Outlook. While there are password capabilities in the application, it seems only to control access to the FusionOne web site. Even so, the AutoSync feature allows a user to enter a password one time and all future syncs need no intervention.



☑ Contacts	Microsoft Outlook	Details
☑ Mail	Microsoft Outlook	Details
☑ Calendar	Microsoft Outlook	Details
☑ Tasks	Microsoft Outlook	Details
☑ Notes	Microsoft Outlook	Details
☑ Bookmarks	Microsoft Internet Explorer	Details
□ Files		
☑ My Documents\H...	48 KB	Details

Figure 2: FusionOne Sync options

Traffic Traces

A test computer was set up with Microsoft Windows 2000 and Outlook 2000, and the FusionOne application was installed. A firewall rule was placed tracking all traffic from the test computer to any destination. In addition, the test computer and a TCPDump host were placed on a shared hub in order to get packet traces from the test computer. Multiple FusionOne syncs were initiated on the test computer and snippets from the resultant traces from a couple of those syncs are listed below.

The first trace from the firewall shows that all traffic occurred over a combination of http and https, ports 80 and 443, that are generally allowed out of corporate networks unmolested and normally unmonitored. Even with stateful firewalls or proxy servers, this traffic usually leaves corporate networks without serious monitoring since the traffic appears to be normal web surfing activity.

```
Event    Date       Time      Actn      DstPort  Source IP     Dest IP            TCP/UDP
411066   2-Dec-00   12:19:28  accept    http     MY.NET.10.254 fms.fusionone.com  tcp
411067   2-Dec-00   12:19:28  accept    http     MY.NET.10.254 fms.fusionone.com  tcp
411074   2-Dec-00   12:19:30  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411081   2-Dec-00   12:19:31  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411082   2-Dec-00   12:19:32  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411083   2-Dec-00   12:19:32  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411085   2-Dec-00   12:19:32  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411086   2-Dec-00   12:19:33  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
411088   2-Dec-00   12:19:34  accept    http     MY.NET.10.254 fms01.fusionone.com tcp
411121   2-Dec-00   12:20:29  accept    http     MY.NET.10.254 fms01.fusionone.com tcp
411122   2-Dec-00   12:20:30  accept    https    MY.NET.10.254 fms01.fusionone.com tcp
```

The following sampling from the second trace, obtained from TCPDump, shows the three way handshakes on both ports 80 and 443, with the rest of the trace appearing to be fairly normal web activity.

```
13:26:26.643391 MY.NET.10.254.4009 > fms.FUSIONONE.COM.80: S 3952218141:3952218141(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
13:26:26.738830 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: S 708477933:708477933(0) ack 3952218142 win 17520 <nop,nop,sackOK,mss 1460>
```

```
            (DF)
13:26:26.738962 MY.NET.10.254.4009 > fms.FUSIONONE.COM.80: . ack 1 win 17520 (DF)
(Continued on next page)
(Continued from previous page)

13:26:26.739484 MY.NET.10.254.4009 > fms.FUSIONONE.COM.80: P 1:275(274) ack 1 win 17520 (DF)
13:26:26.739717 MY.NET.10.254.4009 > fms.FUSIONONE.COM.80: P 275:389(114) ack 1 win 17520 (DF)
13:26:26.828554 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: . ack 275 win 17246 (DF)
13:26:26.875666 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: . ack 389 win 17520 (DF)
13:26:26.960163 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: P 1:320(319) ack 389 win 17520 (DF)
13:26:27.006868 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: P 320:925(605) ack 389 win 17520 (DF)
13:26:27.006876 fms.FUSIONONE.COM.80 > MY.NET.10.254.4009: F 925:925(0) ack 389 win 17520 (DF)
...
13:26:27.375279 MY.NET.10.254.4011 > fms04.FUSIONONE.COM.443: S 3952465935:3952465935(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
13:26:27.464349 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4011: S 709984427:709984427(0) ack 3952465936 win 17520 <nop,nop,sackOK,mss 1460>
            (DF)
13:26:27.464469 MY.NET.10.254.4011 > fms04.FUSIONONE.COM.443: . ack 1 win 17520 (DF)
13:26:27.552582 MY.NET.10.254.4011 > fms04.FUSIONONE.COM.443: P 1:79(78) ack 1 win 17520 (DF)
13:26:27.641284 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4011: . ack 79 win 17520 (DF)
13:26:27.643018 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4011: P 1:705(704) ack 79 win 17520 (DF)
13:26:27.647582 MY.NET.10.254.4011 > fms04.FUSIONONE.COM.443: P 79:283(204) ack 705 win 16816 (DF)
...
13:26:28.920973 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4012: P 1:147(146) ack 103 win 17520 (DF)
13:26:28.923031 MY.NET.10.254.4012 > fms04.FUSIONONE.COM.443: P 103:170(67) ack 147 win 17374 (DF)
13:26:28.925121 MY.NET.10.254.4012 > fms04.FUSIONONE.COM.443: P 170:733(563) ack 147 win 17374 (DF)
13:26:28.925577 MY.NET.10.254.4012 > fms04.FUSIONONE.COM.443: P 733:895(162) ack 147 win 17374 (DF)
13:26:29.015686 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4012: . ack 733 win 17520 (DF)
13:26:29.018269 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4012: P 147:582(435) ack 895 win 17520 (DF)
13:26:29.018276 fms04.FUSIONONE.COM.443 > MY.NET.10.254.4012: F 582:582(0) ack 895 win 17520 (DF)
13:26:29.018432 MY.NET.10.254.4012 > fms04.FUSIONONE.COM.443: . ack 583 win 16939 (DF)
13:26:29.029824 MY.NET.10.254.4012 > fms04.FUSIONONE.COM.443: F 895:895(0) ack 583 win 16939 (DF)
```

Observations

While the tool itself is not an exploit tool nor it's use deemed an attack per se, the use of tools such as FusionOne by corporate employees should give corporate management and information security professionals reason to pause and evaluate corporate network usage policies as well as technical ways of controlling these types of activities. Sites with similar capabilities exist, such as Xdrive.com, iDrive.com, MySpace.com, Blink.com, and others.

More sinister scenarios that may be just on the horizon (if not here already) involve persons with malicious intent writing such tools with some or all of the additional capabilities:

- Silent install and operation utilizing normally unwatched ports such as 80 and 443; can be launched via a number of established methods.
- ActiveX or Java applets that can gather additional data such as network addresses, available services, etc. There appears to be some tools already in use commercially with these capabilities (Ecora, for example, can gather NT domain, Exchange, Cisco router, and other information; especially if run by an Administrator).

Remedies

There are both social and technical remedies to these potential problem areas.

1. Corporations need to properly define and publicize their *Acceptable Use* policies since other technologies such as wireless PDA's and cell phones that can sync to desktops will be taxing current technical solutions.

2. Blocking access to these sites at the perimeter, while cumbersome, may be necessary. The use of URL filtering software/hardware (such as 8e6's XStop or SurfWatch) may be used to block access to all *Personal Data Synchronization* sites.
3. The security staff need to be watchful of outbound *http* traffic a little more than is currently the norm at most corporations.