Global Information Assurance Certification Paper

*** Northcutt, wee oh, this is one of the best looking submissions we have seen yet! Solid analytical process, three might be more like a traceroute but Paul has submitted backup for his analysis, so I am willing to give that one full credit. We did 8 in class, is that a cablemodem? 10 is just a shade long. Doggone good job though, class act!! 94 ***

GCIA Certification Practical

Paul S. Sears

January 16, 2005

Background

These detects are from SHADOW logs that were analyzed from March 31, 2000 through April 07, 2000. Interesting events were extracted from the logs and discussed in this document

MySite.com has a Class C address space used for the DMZ of MySite and there are 5 devices that are members of that DMZ: a public Web server, a public FTP server, the primary border proxy firewall, the gateway router, and the system hosting the SHADOW NIDS.

The destination network address has been sanitized, but the source addresses have not. The firewall name was been replaced with proxy.mysite.com, the web server is www.mysite.com, and the ftp server changed to ftp.mysite.com.

The IP addresses for my site have been changed to 192.168.1.x

Severity is calculated using:

Severity = (Criticality + Lethality) – (system countermeasures + network countermeasures)

Where each aspect is rated on a scale of 0 – 5.

Threat Level:

- **Severity <= 0**
- **Severity = 1, 2**
- **Severity = 3, 4**
- **Severity = 5**

Detect 1 – Illegal flag combinations from Demon.net

```
Date: Apr03 - PDT: 08:00
194.217.242.89 > 192.168.1.3
08:30:22.682933 anchor-post-31.mail.demon.net.31510 > proxy.mysite.com.31501: SFR
8954981:8956445(1464) ack 2065694720 win 0 urg 4096 (DF)

194.217.242.91 > 192.168.1.3
08:22:10.134217 anchor-post-33.mail.demon.net.27045 > proxy.mysite.com.27005: SRP
10944190:10945650(1460) win 128 urg 25280 (DF)
08:26:30.577838 anchor-post-33.mail.demon.net.27035 > proxy.mysite.com.27005: SFRP
11519773:11521245(1472) win 0 urg 32768 (DF)

Date: Apr05 - PDT: 10:00
194.217.242.38 > 192.168.1.3
10:25:13.720179 finch-post-10.mail.demon.net.7766 > proxy.mysite.com.1077: SFR
2857770:2859210(1440) win 98 <[bad opt]> (DF)
```

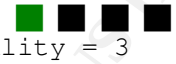
Description of detect
These packets were flagged as having illegal TCP flag combinations.

Active Targeting
No, normal email exchange.

Intent
Email exchange between Demon.net and mysite.com. No malicious intent stated by Demon.net.

History
Demon.net has stated they have a faulty router that creates packets with these illegal flag combinations.

Analysis
Syn-Reset-Push and Syn-Fin-Reset-Push are not legal combinations of TCP flags. It is actually kind of cool to see this after hearing about it at SANS2000. Of course, Demon.net really should fix that silly router...

Threat Level: 

Criticality = 3
Lethality = 1
System Countermeasures = 4
Network Countermeasures = 4
Severity =(3+1) – (4+4) = -4

Detect 2 - Illegal Flag combinations with source port 0

```
Date: Apr03 - PDT: 08:00
194.247.66.58 > 192.168.1.3
08:20:44.468715 194.247.66.58.0 > proxy.mysite.com.28434: SP
1332742656:1332743710(1054) win 1280 <[bad opt]> (DF)
08:20:53.653854 194.247.66.58.12551 > proxy.mysite.com.60797: SF
553952964:553954412(1448) win 34606 urg 64982 <[bad opt]> (DF)
```

Description of detect
These packets were flagged as having illegal TCP flag combinations.

Active Targeting
Yes.

Intent
Possible probe for Trojans.

History
This scan has only been seen once.

Analysis
Syn-Push and Syn-Fin are not legal combinations of TCP flags. The first packet was also sent from source port 0 which indicates that this packet was crafted. It is also significant that the first packet has a payload of 1054 octets. It could contain exploit code.

Threat Level: 
Criticality = 3
Lethality = 2 (System recon/fingerprinting)
System Countermeasures = 4 (Systems are patched and well maintained)
Network Countermeasures = 4 (Firewall rules in effect to block these ports)
Severity =(3+2) - (4+4) = -3

Detect 3 – UDP Port scanning

```
Date: Apr03 - PDT: 10:00
208.51.143.131 > 192.168.1.3
10:51:41.172023 fntn.com.39806 > proxy.mysite.com.33456: udp 12 [ttl 1]
10:51:46.174637 fntn.com.39806 > proxy.mysite.com.33457: udp 12 [ttl 1]
10:51:56.206520 fntn.com.39806 > proxy.mysite.com.33459: udp 12
10:52:04.242116 fntn.com.39806 > proxy.mysite.com.33460: udp 12
10:52:09.271056 fntn.com.39806 > proxy.mysite.com.33461: udp 12
10:52:14.209377 fntn.com.39806 > proxy.mysite.com.33462: udp 12
10:52:19.259046 fntn.com.39806 > proxy.mysite.com.33463: udp 12
10:52:24.221187 fntn.com.39806 > proxy.mysite.com.33464: udp 12
10:52:29.264669 fntn.com.39806 > proxy.mysite.com.33465: udp 12
10:52:34.217856 fntn.com.39806 > proxy.mysite.com.33466: udp 12
10:52:39.217741 fntn.com.39806 > proxy.mysite.com.33467: udp 12
10:52:44.217609 fntn.com.39806 > proxy.mysite.com.33468: udp 12
10:52:49.268144 fntn.com.39806 > proxy.mysite.com.33469: udp 12
10:52:54.257151 fntn.com.39806 > proxy.mysite.com.33470: udp 12
10:53:02.514708 fntn.com.39806 > proxy.mysite.com.33471: udp 12
10:53:12.544848 fntn.com.39806 > proxy.mysite.com.33473: udp 12
10:53:17.514579 fntn.com.39806 > proxy.mysite.com.33474: udp 12
10:53:27.564377 fntn.com.39806 > proxy.mysite.com.33476: udp 12
10:53:32.519471 fntn.com.39806 > proxy.mysite.com.33477: udp 12
10:53:37.518910 fntn.com.39806 > proxy.mysite.com.33478: udp 12
10:53:52.923986 fntn.com.39806 > proxy.mysite.com.33480: udp 12
10:53:57.957380 fntn.com.39806 > proxy.mysite.com.33481: udp 12
10:54:03.365734 fntn.com.39806 > proxy.mysite.com.33482: udp 12
10:54:13.545264 fntn.com.39806 > proxy.mysite.com.33484: udp 12
10:54:18.602871 fntn.com.39806 > proxy.mysite.com.33485: udp 12
10:54:23.697770 fntn.com.39806 > proxy.mysite.com.33486: udp 12
```

```
10:54:29.127943 fntn.com.39806 > proxy.mysite.com.33487: udp 12
10:54:39.529429 fntn.com.39806 > proxy.mysite.com.33489: udp 12
10:54:44.567136 fntn.com.39806 > proxy.mysite.com.33490: udp 12
10:55:00.011149 fntn.com.39806 > proxy.mysite.com.33493: udp 12
10:55:04.984294 fntn.com.39806 > proxy.mysite.com.33494: udp 12
10:55:15.122728 fntn.com.39806 > proxy.mysite.com.33496: udp 12
10:55:20.177731 fntn.com.39806 > proxy.mysite.com.33497: udp 12
10:55:25.229303 fntn.com.39806 > proxy.mysite.com.33498: udp 12
10:55:30.309156 fntn.com.39806 > proxy.mysite.com.33499: udp 12
```

Description of detect
A high UDP port scan of our firewall.

Active Targeting
Yes.

Intent
Probe for Trojans or mapping active high UDP ports.

History
This scan has only been seen once.

Analysis
In analyzing the logs over a week's period, it is fairly common to see traceroutes generated by loadbalancers and network mapping sites. Loadbalancers general send 3 or 4 traceroutes and the loadbalancers we have seen have a consistant signature of sending a UDP payload of 36 octets. Some examples of loadbalancer traces are shown here, with the start of each pattern highlited (*Note that these traces are different in pattern than the previous trace!*)

```
206.251.19.80 > 192.168.1.3
09:09:36.918845 206.251.19.80.2719 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:09:38.906996 206.251.19.80.2720 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:09:39.907763 206.251.19.80.2721 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:33:21.260896 206.251.19.80.2719 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:33:22.319357 206.251.19.80.2720 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:33:23.363397 206.251.19.80.2721 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:33:24.542210 206.251.19.80.2722 > proxy.mysite.com.33434: udp 36
09:35:16.894218 206.251.19.80.2719 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:35:17.934136 206.251.19.80.2720 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:35:19.242910 206.251.19.80.2721 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:35:20.479146 206.251.19.80.2722 > proxy.mysite.com.33434: udp 36
09:35:21.557384 206.251.19.80.2723 > proxy.mysite.com.33434: udp 36

206.251.19.88 > 192.168.1.3
09:32:07.821422 206.251.19.88.2819 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:32:09.076499 206.251.19.88.2820 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:32:10.216972 206.251.19.88.2821 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:32:11.460545 206.251.19.88.2822 > proxy.mysite.com.33434: udp 36

209.67.29.8 > 192.168.1.3
09:01:18.610941 209.67.29.8.2812 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:01:19.678933 209.67.29.8.2813 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:01:20.874803 209.67.29.8.2814 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:01:22.688886 209.67.29.8.2815 > proxy.mysite.com.33434: udp 36
09:02:27.691033 209.67.29.8.2812 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:02:28.694305 209.67.29.8.2813 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:02:29.920145 209.67.29.8.2814 > proxy.mysite.com.33434: udp 36 [ttl 1]
09:02:31.717909 209.67.29.8.2815 > proxy.mysite.com.33434: udp 36
```

Three things made this detect significant: 1) The source port remained constant; 2) the destination port was incrementing; and 3) the high rate of incoming packets.

Threat Level: ■ ■ ■ ■

Criticality = 5 (only targeting firewall)
Lethality = 4
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (firewall rules in effect to block these ports)
Severity =(5+4) - (4+4) = 1

Detect 4 - Scanning for SNMP

```
Site: MySite - Date: Apr02 - PDT: 21:00
205.210.134.73 > 192.168.1.3
21:41:27.678481 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
21:41:27.679307 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]

Site: MySite - Date: Apr02 - PDT: 22:00.
205.210.134.73 > 192.168.1.3
22:36:13.295664 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
22:36:18.203669 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
22:36:23.232361 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
22:36:28.061966 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
22:36:32.830398 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]

Site: MySite - Date: Apr03 - PDT: 20:00
205.210.134.73 > 192.168.1.3
20:19:43.186637 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
20:19:47.693044 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
20:19:52.247423 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
20:19:56.718735 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
20:20:01.208863 205.210.134.73.1030 > proxy.mysite.com.161:
GetNextRequest(11)[|snmp]
```

Description of detect
Scanning for SNMP in an attempt to get system configuration information.

Active Targeting
Yes.

Intent
The remote site is attempting to walk (GetNextRequest) through SNMP MIBS our firewall in an attempt to extract configuration information about the firewall.

History
This scan has only been seen once and the scan originated from a constant source IP address over the course of 2 days.

Analysis
The badguy performing the scan is attempting to gather system configuration information that could lead to a system exploit. Information about system type (OS level, patch level, etc.) sometimes can be extracted from SNMP MIBs.

Threat Level: ■ ■ ■ ■
Criticality = 5 (targeting only the firewall)
Lethality = 4 (can reveal information that can lead to a compromise)
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (Firewall does not run SNMP)
Severity =(5+4) - (4+4) = 1

Detect 5 - Scanning for Linuxconf

```
Site: MySite - Date: Apr02 - PDT: 22:00

216.5.194.100 > 192.168.1.4
22:13:19.336458 na.sdn.net.za.4195 > IDS.mysite.com.98: S 2866818756:2866818756(0)
win 32120  (DF)
22:13:19.361330 na.sdn.net.za.4211 > 20.mysite.com.98: S 2871026077:2871026077(0)
win 32120  (DF)
22:13:22.060477 na.sdn.net.za.4196 > www.mysite.com.98: S 2861468649:2861468649(0)
win 32120  (DF)
```

Description of detect
Scanning for Linuxconf to exploit a buffer overflow and compromise the system.

Active Targeting
Yes.

Intent
na.sdn.net.za is probing our class C address space looking for vulnerable linuxconf services to gain access to the system.

History
This scan was only seen once, however an assumption can be made that the badguy previously performed recon on the subnet (see analysis).

Analysis
What is interesting about this scan is that the badguy avoided the firewall and our public ftp server during the week the SHADOW logs were analyzed. The badguy's scan actually hit the SHADOW NIDS – the first time that any packets have been seen targeted at the NIDS system (IDS.mysite.com). Also, the scanner hit an unadvertised router (20.mysite.com) that performs VPN services to some remote sites. It looks like badguy had probed the subnet sometime before we set up the SHADOW NIDS...

Threat Level: ■ ■ ■ ■
Criticality = 5
Lethality = 5 (can result in a complete system compromise)
System Countermeasures = 4 (systems well maintained and patched)

Network Countermeasures = 2 (linuxconf is not dropped at the router)
Severity =(5+5) - (4+2) = 4

Detect 6 - Portmapper scan

```
Site: MySite - Date: Apr03 - PDT: 06:00
212.37.198.177 > 192.168.1.5
06:47:36.881198 212.37.198.177.1867 > www.mysite.com.111: S
1714644298:1714644298(0) win 32120  (DF)
06:47:36.893176 212.37.198.177.1866 > snoopy.mysite.com.111: S
1711713261:1711713261(0) win 32120  (DF)
06:47:36.898084 212.37.198.177.1869 > ftp.mysite.com.111: S
1708878615:1708878615(0) win 32120  (DF)
06:47:36.931387 212.37.198.177.1882 > 198-182-177-20.mysite.com.111: S
1699752839:1699752839(0) win 32120  (DF)
06:47:37.052795 212.37.198.177.1865 > proxy.mysite.com.111: S
1714037736:1714037736(0) win 32120  (DF)

Site: MySite - Date: Apr03 - PDT: 14:00
216.15.30.155 > 192.168.1.3
14:43:17.515964 dnai-216-15-30-155.cust.dnai.com.23601 > proxy.mysite.com.111: S
1300141340:1300141340(0) win 512
14:43:17.516282 dnai-216-15-30-155.cust.dnai.com.23602 > snoopy.mysite.com.111: S
2396594916:2396594916(0) win 512
14:43:17.518633 dnai-216-15-30-155.cust.dnai.com.23603 > www.mysite.com.111: S
2474789448:2474789448(0) win 512
14:43:17.542276 dnai-216-15-30-155.cust.dnai.com.23648 > ftp.mysite.com.111: S
224090953:224090953(0) win 512
14:43:18.851332 dnai-216-15-30-155.cust.dnai.com.26340 > 198-182-177-
20.mysite.com.111: S 2068679915:2068679915(0) win 512
14:43:27.776996 dnai-216-15-30-155.cust.dnai.com.837 > ftp.mysite.com.111: S
1454294161:1454294161(0) win 32120

Site: MySite - Date: Apr03 - PDT: 17:00
212.37.198.177 > 192.168.1.7
17:57:05.161896 212.37.198.177.807 > ftp.mysite.com.111: udp 56
```

Description of detect
Scanning for portmapper to exploit a buffer overflow and compromise the system.

Active Targeting
My site's entire class C address space.

Intent
Two sites (212.37.198.177 and dnai-216-15-30-155.cust.dnai.com) are probing our class C address space looking for vulnerable portmapper services to gain access to the system.

History
This scan was only seen once over a 1 week period and on the same day.

Analysis
This might be a coordinated portmapper scan and appears to be part of a larger, overall scan. Badguy A scans 8 hours before Badguy B does his scan. A few hours later, Badguy A tries it again.

Threat Level: ■ ■ ■ ■
Criticality = 2
Lethality = 5 (can result in a complete system compromise)
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 2 (portmapper is not dropped at the router)

Severity =(2+5) – (4+2) = 1

Detect 7 – Possible low and slow scan, or Why just one SFAU?

```
Site: MySite - Date: Apr04 - PDT: 11:00
194.70.34.241 > 192.168.1.3
11:30:12.935616 www.sti.healthcare.org.uk.1081 > proxy.mysite.com.1039: SF
2252104:2253584(1480) ack 268435903 win 8423 urg 28139 (DF)

Site: MySite - Date: Apr06 - PDT: 10:00
194.159.250.132 > 192.168.1.3
10:00:07.494291 194.159.250.132.7766 > proxy.mysite.com.1043: SF
4611514:4612974(1460) ack 3621173030 win 44673 urg 12476 (DF)
```

Description of detect
Low and slow port scan or anomalous packets.

Active Targeting
No.

Intent
Two sites (www.sti.healthcare.org.uk and 194.159.250.132) send TCP packets with SFAU flags set.

History
First time this type of scan was seen.

Analysis
This might be a low and slow scan as it happens once on April 4 and once on April 6, around the same time of the day. The packets have a similar signature in that the Syn, Fin, Ack and Urgent flags are set, and there is a full packet of payload in the packets (more than 1400 octets). These packets also could have been mangled by a router in transit and therefore be benign.

Threat Level: ■ ■ ■ ■

Criticality = 2
Lethality = 2
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (targeted ports are dropped at the firewall)
Severity =(2+2) – (4+4) = -4

Detect 8 - IP-proto-54

```
Site: MySite - Date: Apr04 - PDT: 14:00
146.203.19.25 > 192.168.1.5
14:56:34.424145 146.203.19.25 > www.mysite.com: ip-proto-54 44
14:57:58.457541 146.203.19.25 > www.mysite.com: ip-proto-54 44
14:58:08.668566 146.203.19.25 > www.mysite.com: ip-proto-54 44
```

Description of detect
Anomalous IP Protocol.

Active Targeting
Yes.

Intent
146.203.19.25 send packets with IP protocol 54 to our webserver.

History
First time this type of scan was seen.

Analysis
IP-Proto-54 is listed in IANA as NARP NBMA Address Resolution Protocol (NARP) [RFC1735] (from http://www.isi.edu/in-notes/iana/assignments/protocol-numbers)

It is unclear of the purpose of this scan. The NARP packets either escaped from an upstream site, maybe our ISP, or some Badguy is attempting to fingerprint our webserver by seeing how it responds to the NARP request.

Threat Level: ■ ■ ■ ■
Criticality = 2
Lethality = 2 (Recon)
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (targeted ports are dropped at the firewall)
Severity =(2+2) - (4+4) = -4

Detect 9 - Interesting connects attempts to our web server

```
Site: MySite - Date: Apr04 - PDT: 22:00
204.210.30.181 > 192.168.1.5
22:33:49.352300 dt0410nb5.san.rr.com.39444 > www.mysite.com.21: SFP
2819393729:2819393729(0) win 2048 urg 0
22:33:49.353885 dt0410nb5.san.rr.com.39446 > www.mysite.com.533: S
2819393729:2819393729(0) win 2048
```

Description of detect
Anomalous TCP Fragments and target of "netwall" port of webserver.

Active Targeting
Yes.

Intent
Probing for active ports, possibly looking for a trojan on port 533.

History
First time this type of scan was seen.

Analysis
Two packets were sent to www.mysite.com, one with SFP and no payload, the other a Syn packet with no payload to port 533. Badguy is probing for active ports and possibly trojans on the webserver. However, there are not any currently listed trojans that are on port 533.

Threat Level: ■ ■ ■ ■
Criticality = 2
Lethality = 2 (Recon)
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (targeted ports are dropped at the firewall)
Severity =(2+2) - (4+4) = -4

Detect 10 - Fragmented Pings

```
Site: MySite - Date: Apr05 - PDT: 03:00
128.93.11.73 > 192.168.1.3
03:15:54.493563 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50328:1480@0+)
03:15:54.493563 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50328:1480@0+)
03:15:54.501537 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50329:1480@0+)
03:15:54.501537 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50329:1480@0+)
03:15:54.510443 tif.inria.fr > proxy.mysite.com: (frag 50329:1480@1480+)
03:15:54.518409 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50330:1480@0+)
03:15:54.518409 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50330:1480@0+)
03:15:54.526391 tif.inria.fr > proxy.mysite.com: (frag 50330:1480@1480+)
03:15:54.540583 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50331:1480@0+)
03:15:54.540583 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50331:1480@0+)
03:15:54.548563 tif.inria.fr > proxy.mysite.com: (frag 50331:1480@1480+)
03:15:54.556541 tif.inria.fr > proxy.mysite.com: (frag 50331:1480@2960+)
03:15:54.568187 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50332:1480@0+)
03:15:54.568187 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50332:1480@0+)
03:15:54.576165 tif.inria.fr > proxy.mysite.com: (frag 50332:1480@1480+)
03:15:54.585305 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50333:1480@0+)
03:15:54.585305 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50333:1480@0+)
03:15:55.493170 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50340:1480@0+)
03:15:55.493170 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50340:1480@0+)
03:15:55.501136 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50341:1480@0+)
03:15:55.501136 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50341:1480@0+)
03:15:55.510043 tif.inria.fr > proxy.mysite.com: (frag 50341:1480@1480+)
03:15:55.518000 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50342:1480@0+)
03:15:55.518000 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50342:1480@0+)
03:15:55.525979 tif.inria.fr > proxy.mysite.com: (frag 50342:1480@1480+)
03:15:55.540174 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50343:1480@0+)
03:15:55.540174 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50343:1480@0+)
03:15:55.548153 tif.inria.fr > proxy.mysite.com: (frag 50343:1480@1480+)
03:15:55.559805 tif.inria.fr > proxy.mysite.com: (frag 50343:1480@2960+)
03:15:55.567787 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50345:1480@0+)
03:15:55.567787 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50345:1480@0+)
03:15:55.575754 tif.inria.fr > proxy.mysite.com: (frag 50345:1480@1480+)
03:15:55.583733 tif.inria.fr > proxy.mysite.com: (frag 50345:1480@2960+)
03:15:56.493342 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50500:1480@0+)
03:15:56.493342 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50500:1480@0+)
```

```
03:15:56.501323 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50511:1480@0+)
03:15:56.501323 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50511:1480@0+)
03:15:56.510222 tif.inria.fr > proxy.mysite.com: (frag 50511:1480@1480+)
03:15:56.518196 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50521:1480@0+)
03:15:56.518196 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50521:1480@0+)
03:15:56.526171 tif.inria.fr > proxy.mysite.com: (frag 50521:1480@1480+)
03:15:56.540375 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50539:1480@0+)
03:15:56.540375 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50539:1480@0+)
03:15:56.548343 tif.inria.fr > proxy.mysite.com: (frag 50539:1480@1480+)
03:15:56.559998 tif.inria.fr > proxy.mysite.com: (frag 50539:1480@2960+)
03:15:56.567965 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50567:1480@0+)
03:15:56.567965 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50567:1480@0+)
03:15:56.575946 tif.inria.fr > proxy.mysite.com: (frag 50567:1480@1480+)
03:15:56.583927 tif.inria.fr > proxy.mysite.com: (frag 50567:1480@2960+)
03:15:56.593049 tif.inria.fr > proxy.mysite.com: (frag 50571:1480@4440+)
03:15:57.493388 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50625:1480@0+)
03:15:57.493388 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50625:1480@0+)
03:15:57.509891 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50626:1480@0+)
03:15:57.509891 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50626:1480@0+)
03:15:57.518797 tif.inria.fr > proxy.mysite.com: (frag 50626:1480@1480+)
03:15:57.526769 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50627:1480@0+)
03:15:57.526769 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50627:1480@0+)
03:15:57.534747 tif.inria.fr > proxy.mysite.com: (frag 50627:1480@1480+)
03:15:57.548944 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50629:1480@0+)
03:15:57.548944 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50629:1480@0+)
03:15:57.556923 tif.inria.fr > proxy.mysite.com: (frag 50629:1480@1480+)
03:15:57.568575 tif.inria.fr > proxy.mysite.com: (frag 50629:1480@2960+)
03:15:57.576547 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50630:1480@0+)
03:15:57.576547 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50630:1480@0+)
03:15:57.584526 tif.inria.fr > proxy.mysite.com: (frag 50630:1480@1480+)
03:15:58.492919 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50638:1480@0+)
03:15:58.492919 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50638:1480@0+)
03:15:58.500892 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50639:1480@0+)
03:15:58.500892 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50639:1480@0+)
03:15:58.509799 tif.inria.fr > proxy.mysite.com: (frag 50639:1480@1480+)
03:15:58.517766 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50640:1480@0+)
03:15:58.517766 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50640:1480@0+)
03:15:58.525749 tif.inria.fr > proxy.mysite.com: (frag 50640:1480@1480+)
```

```
03:15:58.539943 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50641:1480@0+)
03:15:58.539943 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50641:1480@0+)
03:15:58.547925 tif.inria.fr > proxy.mysite.com: (frag 50641:1480@1480+)
03:15:58.559578 tif.inria.fr > proxy.mysite.com: (frag 50641:1480@2960+)
03:15:58.567929 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50642:1480@0+)
03:15:58.567929 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50642:1480@0+)
03:15:58.575898 tif.inria.fr > proxy.mysite.com: (frag 50642:1480@1480+)
03:15:58.583879 tif.inria.fr > proxy.mysite.com: (frag 50642:1480@2960+)
03:15:59.500814 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50661:1480@0+)
03:15:59.500814 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50661:1480@0+)
03:15:59.508773 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50662:1480@0+)
03:15:59.508773 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50662:1480@0+)
03:15:59.517679 tif.inria.fr > proxy.mysite.com: (frag 50662:1480@1480+)
03:15:59.526095 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50663:1480@0+)
03:15:59.526095 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50663:1480@0+)
03:15:59.534085 tif.inria.fr > proxy.mysite.com: (frag 50663:1480@1480+)
03:15:59.548271 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50664:1480@0+)
03:15:59.548271 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50664:1480@0+)
03:15:59.556264 tif.inria.fr > proxy.mysite.com: (frag 50664:1480@1480+)
03:15:59.567904 tif.inria.fr > proxy.mysite.com: (frag 50664:1480@2960+)
03:15:59.575876 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50665:1480@0+)
03:15:59.575876 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50665:1480@0+)
03:15:59.583856 tif.inria.fr > proxy.mysite.com: (frag 50665:1480@1480+)
03:15:59.728434 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50666:1480@0+)
03:15:59.728434 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50666:1480@0+)
03:16:00.501293 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50683:1480@0+)
03:16:00.501293 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50683:1480@0+)
03:16:00.509604 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50684:1480@0+)
03:16:00.509604 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50684:1480@0+)
03:16:00.518520 tif.inria.fr > proxy.mysite.com: (frag 50684:1480@1480+)
03:16:00.526486 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50685:1480@0+)
03:16:00.526486 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50685:1480@0+)
03:16:00.534459 tif.inria.fr > proxy.mysite.com: (frag 50685:1480@1480+)
03:16:00.548657 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50686:1480@0+)
03:16:00.548657 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50686:1480@0+)
03:16:00.556673 tif.inria.fr > proxy.mysite.com: (frag 50686:1480@1480+)
03:16:00.568294 tif.inria.fr > proxy.mysite.com: (frag 50686:1480@2960+)
03:16:00.576261 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50688:1480@0+)
```

```
03:16:00.576261 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50688:1480@0+)
03:16:01.500986 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50697:1480@0+)
03:16:01.500986 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50697:1480@0+)
03:16:01.508947 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50698:1480@0+)
03:16:01.508947 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50698:1480@0+)
03:16:01.517820 tif.inria.fr > proxy.mysite.com: (frag 50698:1480@1480+)
03:16:01.525788 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50699:1480@0+)
03:16:01.525788 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50699:1480@0+)
03:16:01.533775 tif.inria.fr > proxy.mysite.com: (frag 50699:1480@1480+)
03:16:01.547976 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50700:1480@0+)
03:16:01.547976 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50700:1480@0+)
03:16:01.555945 tif.inria.fr > proxy.mysite.com: (frag 50700:1480@1480+)
03:16:01.567608 tif.inria.fr > proxy.mysite.com: (frag 50700:1480@2960+)
03:16:01.575567 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50701:1480@0+)
03:16:01.575567 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50701:1480@0+)
03:16:01.583547 tif.inria.fr > proxy.mysite.com: (frag 50701:1480@1480+)
03:16:01.592646 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50702:1480@0+)
03:16:01.592646 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50702:1480@0+)
03:16:02.500846 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50711:1480@0+)
03:16:02.500846 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50711:1480@0+)
03:16:02.508815 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50712:1480@0+)
03:16:02.508815 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50712:1480@0+)
03:16:02.516796 tif.inria.fr > proxy.mysite.com: (frag 50712:1480@1480+)
03:16:02.525660 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50713:1480@0+)
03:16:02.525660 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50713:1480@0+)
03:16:02.533639 tif.inria.fr > proxy.mysite.com: (frag 50713:1480@1480+)
03:16:02.547833 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50714:1480@0+)
03:16:02.547833 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50714:1480@0+)
03:16:02.555818 tif.inria.fr > proxy.mysite.com: (frag 50714:1480@1480+)
03:16:02.567464 tif.inria.fr > proxy.mysite.com: (frag 50714:1480@2960+)
03:16:02.575444 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50715:1480@0+)
03:16:02.575444 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50715:1480@0+)
03:16:02.583413 tif.inria.fr > proxy.mysite.com: (frag 50715:1480@1480+)
03:16:02.592511 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50716:1480@0+)
03:16:02.592511 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50716:1480@0+)
03:16:03.497782 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50721:1480@0+)
```

```
03:16:03.497782 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50721:1480@0+)
03:16:03.509219 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50722:1480@0+)
03:16:03.509219 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50722:1480@0+)
03:16:03.518135 tif.inria.fr > proxy.mysite.com: (frag 50722:1480@1480+)
03:16:03.526473 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50723:1480@0+)
03:16:03.526473 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50723:1480@0+)
03:16:03.534456 tif.inria.fr > proxy.mysite.com: (frag 50723:1480@1480+)
03:16:03.548645 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50724:1480@0+)
03:16:03.548645 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50724:1480@0+)
03:16:03.556630 tif.inria.fr > proxy.mysite.com: (frag 50724:1480@1480+)
03:16:03.568312 tif.inria.fr > proxy.mysite.com: (frag 50724:1480@2960+)
03:16:03.576290 tif.inria.fr > proxy.mysite.com: (frag 50725:1480@1480+)
```

Description of detect
Fragmented ICMP Packets, no "last" frag packet.

Active Targeting
Yes.

Intent
tif.inria.fr (probably spoofed) sends fragmented ICMP packets to our firewall.

History
First time this type of scan was seen.

Analysis
This appears to be a DoS attempt as there are fragmented ICMP packets sent in rapid succession. From the packets in this trace, it only appears that we ever see the first few fragments of any packets and we never see the last fragment per frag ID. The assumption is being made that the Badguy is attempting to DoS the firewall by exploiting fragmentation weaknesses of Windows 9x and Windows NT. This could be an IceNewk/sPing/JOLT DoS (from http://www.indy.net/~sabronet/dos/spingjolt.html)

Threat Level: ■ ■ ■ ■

Criticality = 2
Lethality = 4 (Denial of Service!)
System Countermeasures = 4 (systems well maintained and patched)
Network Countermeasures = 4 (targeted ports are dropped at the firewall)
Severity =(2+4) - (4+4) = -2

Bonus Detect

This detect was logged by my NIDS after I had gathered my materials for this document. I felt that this was interesting enough to include it in this document, and it is a nice example of active targeting as this pattern was not seen going to any other system on this network, including the firewall.

Detect 11 - Portscan

```
Site: MySite - Date: Apr06 - PDT: 23:00
23:51:26.447977 cr31412-a.slnt1.on.wave.home.com.2324 > ftp.mysite.com.4: S
17209353:17209353(0) win 32120  (DF)
23:51:26.449484 cr31412-a.slnt1.on.wave.home.com.2325 > ftp.mysite.com.708: S
24554277:24554277(0) win 32120  (DF)
23:51:26.449918 cr31412-a.slnt1.on.wave.home.com.2326 > ftp.mysite.com.1080: S
11612054:11612054(0) win 32120  (DF)
23:51:26.450696 cr31412-a.slnt1.on.wave.home.com.2327 > ftp.mysite.com.635: S
11729565:11729565(0) win 32120  (DF)
23:51:29.973684 cr31412-a.slnt1.on.wave.home.com.3888 > ftp.mysite.com.103: S
19145168:19145168(0) win 32120  (DF)
23:51:29.974514 cr31412-a.slnt1.on.wave.home.com.3889 > ftp.mysite.com.303: S
16266214:16266214(0) win 32120  (DF)
23:51:29.976996 cr31412-a.slnt1.on.wave.home.com.3890 > ftp.mysite.com.893: S
13430816:13430816(0) win 32120  (DF)
23:51:29.977961 cr31412-a.slnt1.on.wave.home.com.3891 > ftp.mysite.com.588: S
20012933:20012933(0) win 32120  (DF)
23:51:29.979182 cr31412-a.slnt1.on.wave.home.com.3892 > ftp.mysite.com.523: S
13241598:13241598(0) win 32120  (DF)
23:51:29.980094 cr31412-a.slnt1.on.wave.home.com.3893 > ftp.mysite.com.610: S
24586451:24586451(0) win 32120  (DF)
23:51:29.981321 cr31412-a.slnt1.on.wave.home.com.3894 > ftp.mysite.com.173: S
25623211:25623211(0) win 32120  (DF)
23:51:29.982145 cr31412-a.slnt1.on.wave.home.com.3895 > ftp.mysite.com.4: S
18984878:18984878(0) win 32120  (DF)
23:51:30.043833 cr31412-a.slnt1.on.wave.home.com.3896 > ftp.mysite.com.916: S
16347279:16347279(0) win 32120  (DF)
23:54:12.062996 cr31412-a.slnt1.on.wave.home.com.50231 > ftp.mysite.com.21: SFP
2578782969:2578782969(0) win 1024 urg 0
23:54:12.064831 cr31412-a.slnt1.on.wave.home.com.50233 > ftp.mysite.com.43189: S
2578782969:2578782969(0) win 1024
23:54:12.882051 cr31412-a.slnt1.on.wave.home.com.50231 > ftp.mysite.com.21: SFP
2578782969:2578782969(0) win 1024 urg 0
```

Description of detect
Scan for active TCP ports, possibly trojans. Maybe trying to identify the system type.

Active Targeting
Yes.

Intent
cr31412-a.slnt1.on.wave.home.com is checking for open ports on our public ftp server.

History

First time this type of scan was seen.

Analysis
This might be a scan for trojans or the Badguy is looking for services running on non-standard ports. Most of the ports in this run are either unassigned or not commonly used. There was a hit to port 1080, which is used for SOCKS, so it is possible that the Badguy was looking for SOCKS and tried to hide it in the noise of a heavier scan. The scan takes place fairly rapidly, the scan is completed in 4 seconds. Additionally 2 packets with illegal TCP flag combinations are sent to port 21 of this server. Of all the ports scanned on this server, port 21 is the only open port so it seems likely that the Badguy determined this from the scan and then attempted to gather additional information about what is running on port 21, maybe trying to fingerprint the server.

Threat Level: ■ ■ ■ ■

Criticality = 2
Lethality = 3 (Recon, more lethal if trojan located)
System Countermeasures = 4 (system well maintained and patched)
Network Countermeasures = 0 (This system is not protected by the firewall)
Severity =(2+3) - (4+0) = 1

Last Updated: July 20th, 2017

Upcoming Training

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