Global Information Assurance Certification Paper

***** Northcutt, 75 ***

Guillermo Palli

1) Port Scanning, a clasic port scanner tool.

```
16:40:56.526937 192.168.1.1.2075 > 192.168.1.2.tcpmux: S 5338936:5338936(0) win 8192 <mss 1460> (DF)
16:40:56.533432 192.168.1.1.2076 > 192.168.1.2.2: S 5338948:5338948(0) win 8192 <mss 1460> (DF)
16:40:56.544009 192.168.1.1.2077 > 192.168.1.2.3: S 5338996:5338996(0) win 8192 <mss 1460> (DF)
16:40:56.553699 192.168.1.1.2078 > 192.168.1.2.5: S 5338984:5338984(0) win 8192 <mss 1460> (DF)
16:40:56.564582 192.168.1.1.2079 > 192.168.1.2.echo: S 5338976:5338976(0) win 8192 <mss 1460> (DF)
16:40:56.573757 192.168.1.1.2080 > 192.168.1.2.discard: S 5339076:5339076(0) win 8192 <mss 1460> (DF)
16:40:56.584269 192.168.1.1.2081 > 192.168.1.2.systat: S 5339020:5339020(0) win 8192 <mss 1460> (DF)
16:40:56.593366 192.168.1.1.2082 > 192.168.1.2.daytime: S 5339160:5339160(0) win 8192 <mss 1460> (DF)
16:40:56.604565 192.168.1.1.2083 > 192.168.1.2.qotd: S 5339016:5339016(0) win 8192 <mss 1460> (DF)
16:40:56.614053 192.168.1.1.2084 > 192.168.1.2.msp: S 5339028:5339028(0) win 8192 <mss 1460> (DF)
16:40:56.626840 192.168.1.1.2085 > 192.168.1.2.chargen: S 5339156:5339156(0) win 8192 <mss 1460> (DF)
16:40:56.633868 192.168.1.1.2086 > 192.168.1.2.ftp-data: S 5339088:5339088(0) win 8192 <mss 1460> (DF)
```

2) Network Scanning using Legion program, this tool scans a network for shares through port netbios-ssn.

```
16:42:41.140735 192.168.1.1.2337 > 192.168.1.2.netbios-ssn: S 5443682:5443682(0) win 8192 <mss 1460> (DF)
16:42:41.140891 192.168.1.1.2338 > 192.168.1.3.netbios-ssn: S 5443682:5443682(0) win 8192 <mss 1460> (DF)
16:42:41.141230 192.168.1.1.2340 > vaio.localnet.netbios-ssn: S 5443682:5443682(0) win 8192 <mss 1460> (DF)
16:42:41.141601 192.168.1.1.2338 > 192.168.1.3.netbios-ssn: . ack 1 win 8760 (DF)
16:42:41.141694 192.168.1.1.2337 > 192.168.1.2.netbios-ssn: . ack 1 win 8760 (DF)
16:42:41.561478 192.168.1.1.2340 > vaio.localnet.netbios-ssn: S 5443682:5443682(0) win 8192 <mss 1460> (DF)
```

3) TCP/IP Printer Request Server DoS

```
16:52:01.391658 192.168.1.1.4948 > 192.168.1.3.printer: S 5875936:5875936(0) win 8192 <mss 1460> (DF)
16:52:01.881008 192.168.1.1.4948 > 192.168.1.3.printer: S 5875936:5875936(0) win 8192 <mss 1460> (DF)
16:52:02.381164 192.168.1.1.4948 > 192.168.1.3.printer: S 5875936:5875936(0) win 8192 <mss 1460> (DF)
16:52:02.881331 192.168.1.1.4948 > 192.168.1.3.printer: S 5875936:5875936(0) win 8192 <mss 1460> (DF)
...
16:52:05.897298 192.168.1.1.4951 > 192.168.1.3.printer: S 5880437:5880437(0) win 8192 <mss 1460> (DF)
16:52:06.382467 192.168.1.1.4951 > 192.168.1.3.printer: S 5880437:5880437(0) win 8192 <mss 1460> (DF)
16:52:06.890050 192.168.1.1.4951 > 192.168.1.3.printer: S 5880437:5880437(0) win 8192 <mss 1460> (DF)
```

4) Trin00 Telnet. The server is running in our machine in port 27665.

```
17:40:42.332527 192.168.1.1.1114 > 192.168.1.2.27665: S 8797451:8797451(0) win 8192 <mss 1460> (DF)
17:41:07.606971 192.168.1.1.1115 > 192.168.1.2.27665: S 8822700:8822700(0) win 8192 <mss 1460> (DF)
17:41:19.887228 192.168.1.1.1116 > 192.168.1.2.27665: S 8834942:8834942(0) win 8192 <mss 1460> (DF)
```

5) Ping of Death? No, someone is playing with 'Ping -l xxxx' (false positive!)

```
17:50:58.972433 192.168.1.1 > 192.168.1.3: icmp: echo reply (frag 56508:1480@0+)
```

```
17:50:58.973676 192.168.1.1 > 192.168.1.3: (frag 56508:1480@1480+)
17:50:58.974920 192.168.1.1 > 192.168.1.3: (frag 56508:1480@2960+)
17:50:58.976161 192.168.1.1 > 192.168.1.3: (frag 56508:1480@4440+)
...
17:50:58.976161 192.168.1.1 > 192.168.1.3: (frag 56508:1480@57720+)
17:50:58.983821 192.168.1.1 > 192.168.1.3: (frag 56508:808@59200)

6) IGMP packet, trying to nuke routers?

17:57:21.472821 192.168.1.1 > 192.168.1.3: igmp-0 [v0][|igmp] (frag 57282:1480@0+)
17:57:21.474062 192.168.1.1 > 192.168.1.3: (frag 57282:1480@1480+)
17:57:21.480650 192.168.1.1 > 192.168.1.3: (frag 57282:1480@2960+)
17:57:21.481878 192.168.1.1 > 192.168.1.3: (frag 57282:1480@4440+)
17:57:21.483117 192.168.1.1 > 192.168.1.3: (frag 57282:1480@5920+)
17:57:21.484355 192.168.1.1 > 192.168.1.3: (frag 57282:1480@7400+)
17:57:21.485597 192.168.1.1 > 192.168.1.3: (frag 57282:1480@8880+)
17:57:21.486836 192.168.1.1 > 192.168.1.3: (frag 57282:1480@10360+)
17:57:21.488078 192.168.1.1 > 192.168.1.3: (frag 57282:1480@11840+)
17:57:21.489317 192.168.1.1 > 192.168.1.3: (frag 57282:1480@13320+)
17:57:21.489518 192.168.1.1 > 192.168.1.3: (frag 57282:200@14800)
... (again and again...)

7) Ahh!, an NT Hunter scanning tool, have the same number(9825648), it probe for ports 135, 53, 1031 and 1040
   to discover NT boxes in a network.

17:55:42.451131 192.168.1.1.1150 > 192.168.1.3.135: S 9825648:9825648(0) win 8192 <mss 1460> (DF)
17:55:42.453751 192.168.1.1.1151 > 192.168.1.3.domain: S 9825648:9825648(0) win 8192 <mss 1460> (DF)
17:55:42.456085 192.168.1.1.1152 > 192.168.1.3.1031: S 9825648:9825648(0) win 8192 <mss 1460> (DF)
17:55:42.460506 192.168.1.1.1153 > 192.168.1.3.1040: S 9825648:9825648(0) win 8192 <mss 1460> (DF)

8) TearDrop exploit, someone spoof the source ip and try to nuke into sunrpc port

18:42:26.874856 123.123.123.123.sunrpc > 192.168.1.3.222: udp 28 (frag 242:36@0+)
18:42:26.874947 123.123.123.123 > 192.168.1.3: (frag 242:4@24)

The problem here is the second fragment, the computation of the offset is wrong (24 < 36!) and TCP/IP stack crash!.

9) Another well known back door, NetBus 2.0 Pro it uses port 20034 by default.

22:29:20.140391 192.168.1.1.1983 > 192.168.1.3.20034: S 13274342:13274342(0) win 8192 <mss 1460> (DF)
22:29:20.115487 192.168.1.1.1983 > 192.168.1.3.20034: . ack 1 win 8760 (DF)
22:29:20.117080 192.168.1.1.1983 > 192.168.1.3.20034: P 1:33(32) ack 1 win 8760 (DF)

10) UDP packet flooder, it uses well known port to create false positive.

22:54:59.670028 192.168.1.2.12345 > 192.168.1.3.12345: udp 10
22:54:59.670028 192.168.1.2.12345 > 192.168.1.3.12345: udp 10
22:54:59.670028 192.168.1.2.12345 > 192.168.1.3.12345: udp 10
22:54:59.670028 192.168.1.2.12345 > 192.168.1.3.12345: udp 10
22:54:59.670028 192.168.1.2.12345 > 192.168.1.3.12345: udp 10
```