Global Information Assurance Certification Paper

GIAC assignments for GCIDS by Donald.J.Smith

Assignment 1 Network Detects

Detect 1
1. Source of trace:
http://www.sans.org/y2k/020500.htm

2. Detect was generated by:
icmpdlogd and ipfw.

Explanation of fields in trace

3. Probability the source address was spoofed:
Low

216.32.68.10 is in an Exodus netblock. The contact for it is CompServ@Exodus.net

209.67.78.202 and 203 are in an Exodus netblock. The contact for it is CompServ@Exodus.net

Probably not spoofed. (Explanation in Attack Mechanism.)

4. Description of Attack:
First a few icmp 8/0 (pings) coming very fast from different addresses. Then some udp port 53 (dns) lookups.

5. Attack Mechanism:
This looks like the RoundTripTime probe used by several ContentDelieveryNetwork systems. Different CDN vendors are using different RTT probes but nearly all vendors are pinging some, then follow the ping with an nslookup to YOUR dns server if the ping goes unanswered. The high TTLs indicate it was a UNIX™ box. Most CDN systems are using UNIX™ for their content routers (locality content proxy servers). The distributed ping effect comes from trying to find out which of several content routers is closest" to the client.

This could be reconnaissance, in which case the DNS queries are certainly not spoofed addresses and the pings almost certainly not spoofed addresses.

This could be 3rd party effect. Someone could be spoofing a 195.89 address and exodus' CDN system could be trying to find the nearest content router by doing an RTT probe against a spoofed address.

6. Correlations:

Ryan.W.Maple wrote an analysis of CDN's pinging from several different addresses nearly simultanously, which sets off many IDS sensors. http://www.linuxsecurity.com/articles/firewalls_article-2064.html

Robert.Graham wrote "DoubleClick sends echos to people to redirect them to a nearer server for their advertising." http://www.csirt.wc.csirt.firewall-seen.htm

7. Evidence of active targeting:

The host is being targeted. The packets go to a specific address.

8. Severity:

(Criticality + Lethality) - (System + Net countermeasures) (5 + 0) - (5 + 0) = 0

9. Defensive recommendation:

Host defensives are fine. Ping should be blocked at the firewall and unless this is a dns server udp port 53 also.

Date	Time	Host	loggingsvc type	src addr
Feb 3	16:04:16	bishop-rock	icmplogd: ping from	[209.67.78.203]
Feb 3	16:04:47	bishop-rock	icmplogd: ping from	[209.67.78.203]
Feb 3	16:06:12	bishop-rock	icmplogd: ping from	[216.32.68.10]
Feb 3	16:06:50	bishop-rock	icmplogd: ping from	[209.67.78.203]
Feb 3	16:07:39	bishop-rock	icmplogd: ping from	[216.32.68.10]
Feb 3	16:10:32	bishop-rock	icmplogd: ping from	[209.67.78.203]

Date Time Host loggingsvc Protocal rule result interface SubProtocal SrcAddr:Port DestAddr:Port Length Flags ID TTL

Feb 3 16:18:01 bishop-rock kernel: IP fw-in rej eth0
UDP 209.67.78.202:2100 195.89.x.y:53 L=64 S=0x00 I=27056 F=0x0000 T=239
Feb 3 16:18:01 bishop-rock kernel: IP fw-in rej eth0
UDP 209.67.78.202:2101 195.89.x.y:53 L=64 S=0x00 I=27058 F=0x0000 T=239
Feb 3 16:18:01 bishop-rock kernel: IP fw-in rej eth0
UDP 209.67.78.202:2102 195.89.x.y:53 L=64 S=0x00 I=27060 F=0x0000 T=239

10. Why should ping be blocked at the firewall?

a. Ping can be used to map your network.

b. ICMP floods can be used in DDOS.

c. A single large ICMP packet can DOS some operating systems.

d. They might be controling a zombie/server via icmp.

Answer a, b, c and d.

Detect 2
1. Source of trace:
http://www.sans.org/y2k/010901-1300.htm (Joe Matusiewicz)

2. Detect was generated by:
Explanation of fields with trace.

3. Probability the source address was spoofed:
Low

209.67.50. is an Exodus netblock the contact for it is CompServ@Exodus.net

Probably not spoofed as I will explain in Attack Mechanism

The destination address is being spoofed causing 209.67.50.203 to reply to an incorrect address. The destination address will probably then send a reply to 209.67.50.203 if enough addresses are spoofed and they all reply to 209.67.50.203 a ddos can occur against 209.67.50.203.

4. Description of Attack:
Udp port 53 (dns) lookups MX lookups for aol.com.

5. Attack Mechanism:
This does not look like the RoundTripTime probe used by several ContentDelieveryNetwork systems. Notice the MX qwery, the lack of pings, and the single ip address.

This could be reconnaissance in which case the dns queries are certainly not spoofed addresses and the pings almost certainly not spoofed addresses.

This is could be a DDOS. A hacker could spoof 209.67.50.203 to a CDN Hosted name space. The CDN systems would then do a DNS qwery to the address of the name server of the address being spoofed. If the address being spoofed was also a CDN hosted system it could cause a pingpong effect. This could cause a DNS qwery amplification from each content router serving those addresses. This

is very simular to the smurf attack. HUGE results with a small number of initial packets. 100 packet per second against a site supported by 5 CRs spoofed from a site supported by 5 CRs could result in 2500 packets/sec.

6. Correlations:
No CVE for this particular attack. There are numerous CVE's for DNS lookups.

The CVE for smurf is **CVE-1999-0513 Description ICMP messages to broadcast addresses are allowed, allowing for a Smurf attack that can cause a denial of service.**

7. Evidence of active targeting:
A box is being targeted but I do not think it is the box/system that reported this attack. I believe it is the source address in this trace 209.67.50.203.

8. Severity:
(Criticality + Lethality) - (System + Net countermeasures) (5 + 4) - (5 + 4) = 0

9. Defensive recommendation:
None dns server need to be generally available for dns lookups..

(Joe Matusiewicz)
I'm was getting them at a rate of 29,000 an hour against 4 DNS servers. In the beginning they were bouncing off my firwall but now my border router just sends them to the bit bucket. I called Exodus.com and they told me that the register.com admins put an incoming filter on their border. Folks may want to check to see if some of the traffic is originating from their network.

DateTime srcAddr.portNum Dir localAddr.PortNum DNS_Qwery_type

2001/1/8 12:59:02.177788 209.67.50.203.6151 > my.dns.server1.53: 24585+ MX? **hostqweried flags**
aol.com. (25) (DF)

2001/1/8 12:59:02.311022 209.67.50.203.4894 > my.dns.server2.53: 3293+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.583484 209.67.50.203.24933 > my.dns.server3.53: 9234+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.617994 209.67.50.203.26315 > my.dns.server42.53: 39809+ MX?

aol.com. (25) (DF)
2001/1/8 12:59:02.747418 209.67.50.203.5737 > my.dns.server1.53: 38829+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.752486 209.67.50.203.27229 > my.dns.server3.53: 60955+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.774917 209.67.50.203.15825 > my.dns.server42.53: 13969+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.779536 209.67.50.203.28425 > my.dns.server4.53: 15191+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.947593 209.67.50.203.29238 > my.dns.server1.53: 37535+ MX?
aol.com. (25) (DF)
2001/1/8 12:59:02.948806 209.67.50.203.22744 > my.dns.server3.53: 12566+ MX?
aol.com. (25) (DF)

10. Why should internal dns servers be blocked at the firewall?

a. DNS can be used to map your network.
b. DNS servers are almost always vulnerable to some new attack.
c. DNS attacks have been used in several automated worms.
d. DNS has been redefined by Microsoft as the digital nervous system and is therefore a Microsoft trademark.

Answer A, B and C.

Detect 3
1. Source of trace:
http://www.sans.org/y2k/practical/mark_thyer.doc

2. Detect was generated by:
cisco acl logs

Explanation of fields with trace.

3. Probability the source address was spoofed:
Low

209.67.78.202 is in an Exodus netblock the contact for it is CompServ@Exodus.net

Probably not spoofed as I will explain in Attack Mechanism

4. Description of Attack:
First a few icmp 8/0 (pings). Then some udp port 53 (dns) lookups.

5. Attack Mechanism:
This looks like a little like the RoundTripTime probe used by several ContentDelieveryNetwork systems.

However I believe this is reconnaissance in which case the dns queries are certainly not spoofed addresses and the pings almost certainly not spoofed addresses because it is the same address for both. This is only coming from one address, packets are coming alot slower than expected, the pings contain more than one packet, therefore this does not match the CDN RTT pattern.

6. Correlations:
CERT, CIAC, GIAC all have alerts out for DNS probes and DNS problems.

7. Evidence of active targeting:
The host is being targeted. The packets go to a specific address.

8. Severity:
(Criticality + Lethality) - (System + Net countermeasures) (5 + 1) - (1 + 5) = 0

9. Defensive recommendation:
Network defensives are fine. Pings and NSLOOKUPS are being blocked at the router by acl 102.

Date Time LogHost loggingsvc ACL# Action "SubProtocol" src addr
Mar 31 00:05:06 rt1 1136: 07:46:42: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 ->
DestAddr (if SubProt=icmp ->type/code else DestPortNum) Num_packets
external.primary.dns (8/0), 5 packets

Mar 31 00:50:02 rt1 1223: 08:31:39: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 1 packet
Mar 31 00:50:35 rt1 1225: 08:32:11: %SEC-6-IPACCESSLOGP: list 102 denied tcp 209.67.78.202(3300) -> external.primary.dns(53), 1 packet
Mar 31 00:55:08 rt1 1235: 08:36:45: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 2 packets
Mar 31 02:48:04 rt1 1426: 10:29:41: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 1 packet
Mar 31 02:48:26 rt1 1429: 10:30:03: %SEC-6-IPACCESSLOGP: list 102 denied tcp 209.67.78.202(2900) -> external.primary.dns(53), 1 packet
Mar 31 02:52:42 rt1 1440: 10:34:19: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 2 packets
Mar 31 08:09:37 rt1 2264: 15:51:13: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 1 packet
Mar 31 08:09:57 rt1 2265: 15:51:33: %SEC-6-IPACCESSLOGP: list 102 denied tcp 209.67.78.202(2100) -> external.primary.dns(53), 1 packet
Mar 31 08:14:49 rt1 2275: 15:56:25: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 2 packets
Mar 31 08:24:45 rt1 2303: 16:06:20: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 1 packet
Mar 31 08:28:02 rt1 2313: 16:09:38: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 209.67.78.202 -> external.primary.dns (8/0), 2 packets
Mar 31 08:54:23 rt1 2397: 16:35:59: %SEC-6-IPACCESSLOGP: list 102 denied udp 209.67.78.202(3408) -> external.primary.dns(33434), 1 packet
Mar 31 13:55:07 rt1 3319: 21:36:44: %SEC-6-IPACCESSLOGP: list 102 denied udp 209.67.78.202(3408) -> external.primary.dns(33434), 1 packet

10. Why would rtt need to be computed from more then one source?
a. To get a more accurate rtt.

b. Because the internet is not reliable.

c. To use the additional cpu's on multiple hosts.

d. Because rtt's are used to decide which of several content engines should deliver the requested data.
Answer D.

Detect 4
1. Source of trace:
http://www.sans.org/y2k/032301-1900.htm *(Peter M Allan)*

2. Detect was generated by:
ipfw logging on Linux 2.0.26

Explanation of fields with trace.

3. Probability the source address was spoofed:
Not very likely. This type of scan requires a 3 way hand shake.

The address resolves to 207.71.92.221, which is a Verio netblock specifically shieldsup.grc.com. Shieldsup is a web based on request security scanner.

4. Description of Attack:
Port scan

5. Attack Mechanism:
Attacker first trys tcp port 80 (http) then trys tcp port 23 (telnet).

Uses the same source port for the entire http scan. This implies the packets are crafted. The chances of a system using a source port for an http request, followed by a 2nd and 3rd request with the same source port in this short of a time, is approximately 1/ ((63K) * (63K)). The http packets arrive 4 seconds apart implying an automated tool not a user. The ID's keep changing, implying a professional tool. It was coded a little better then some of the scriptkiddie tools that are written to use the same ID. The TTLs are all the same 114 which could be a windows 2K machine 14 hops away or could be part of the packet crafting. The length is the same on all of the packets more evidence of packet crafting. There are NO flags set this is the strongest indication of packet crafting yet. This is often called a NULL scan. TCP packets must always have some flags set (ack, syn, fin) depending on where in the TCP three way handshaking the session is.

6. Correlations:
A Null scan discussion is available at
http://www.linuxworld.com/linuxworld/lw-2001-03/lw-03-vcontrol_3.html

7. Evidence of active targeting:
Attack is to a specfic host. Yes this is targeted.

8. Severity:
(Criticality + Lethality) - (System + Net countermeasures) (3 + 1) - (5 + 0) = -2

9. Defensive recommendation:
Home pc with ipfw rejecting all packets in the scan and logging same. This system security is good.

In order to test the systems security the admin went to sheildsup.grc.com and started a scan against his machine.

10. Which of these is the best reason to believe that this packet is crafted?
a. The packets all arrive 4 seconds apart.

b. It uses the same source port for an entire service scan.

c. It has no flags set.

d. Because the packets came from a trusted address.

Answer c.

DTime Host Facility Protocal rule Status interface Protocal FromAddr:Port ToAddr:port Length Flags
Feb 17 08:43:18 notatla kernel: IP fw-in rej ppp0 TCP 207.71.92.221:1657 194.222.156.169:80 L=48 S=0x00 **ID InverseFLAG* TTL** I=52033 F=0x0040 T=114
Feb 17 08:43:22 notatla kernel: IP fw-in rej ppp0 TCP 207.71.92.221:1657 194.222.156.169:80 L=48 S=0x00 I=52406 F=0x0040 T=114
Feb 17 08:43:28 notatla kernel: IP fw-in rej ppp0 TCP 207.71.92.221:1657 194.222.156.169:80 L=48 S=0x00 I=53118 F=0x0040 T=114
Feb 17 08:47:35 notatla kernel: IP fw-in rej ppp0 TCP 207.71.92.221:1987 194.222.156.169:23 L=48 S=0x00 I=12146 F=0x0040 T=114

*InvFlag 40 invert the sense of the IP_FW_F_TCPSYN from ip_fw.h -> Check all but SYN bit of flags.

Detect 5
1. Source of trace:
http://www.sans.org/y2k/021301-1430.htm (Luis Mendoza)

2. Detect was generated by:
Snort.

3. Probability the source address was spoofed:
It is unlikely that the port is spoofed. This appears to be a login attempt which would imply that the source ip is not spoofed.

IP resolves to host028036.arnet.net.ar which is a rather DHCP like host name with the ip address encoded directly in the hostname.

A traceroute shows 200.45.x.x. to be in Argentina. The closest I can get is S3-7.mza-r1.arnet.net.ar 200.45.68.210

4. Description of Attack:
Zombi scan. Someone is looking for an mstream like server.

5. Attack Mechanism:
Host is scanning for a server.

UPD packets from port 31340 to 31320.

An attempt to login 2^passwordcahyna. Notice that spells anyhac backwards!

Looks a lot like mstream..

6. Correlations:
Trin00, TFN, TFN2k, Shaft … CVE 20010122.

Trin00's cert writeup
http://www.cert.org/incident_notes/IN-99-04.html

Certs distributed tool workshop writeup
http://www.cert.org/reports/dsit_workshop.pdf

Dittrich's ddos writeups
http://staff.washington.edu/dittrich/misc/ddos/

TFN2k writeup
http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt

Dittrich's mstream analysis.
http://packetstorm.securify.com/distributed/Mstream_Analysis.txt

7. Evidence of active targeting:
Not much. It is scanning a network "randomly" walking up the ip addresses.

8. Severity:
(Criticality + Lethality) - (System + Net countermeasures) (3 + 5) - (5 + 0) = 3.

9. Defensive recommendation:
Firewall/Router did not block packets. UDP should be blocked at the firewall via an ACL.

10. Why is this a scan not an attack?
a. Packets are traveling in both directions.

b. UDP is not used during at attack.

c. They only targeted some hosts on the network.

d. They appear to be sending a password in order to control a zombie/server.

Answer D

Date	Time	SrcAddr		DestAddr:Port	SubProtocol
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.70:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.75:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.80:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.84:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.87:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.93:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.97:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.101:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.103:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.104:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.114:31320	UDP
Feb 10	13:09:01	200.45.28.36:31340	->	a.b.c.118:31320	UDP

Frame 1 (64 on wire, 64 captured)
Arrival Time: Feb 10, 2001 13:08:59.2000
Time delta from previous packet: 0.000000 seconds
Frame Number: 1
Packet Length: 64 bytes
Capture Length: 64 bytes

Data (22 bytes)

Byte	HexData	AsciiData
0	00e0 b601 3a36 00d0 06d6 9c39 0800 4500	....:6.....9..E.
10	0032 a7ac 0000 6f11 2782 c82d 1c24 aabb	.2....o.'..-.$..
20	ccdd 7a6c 7a58 001e 551d 305e 7031 5e70	.FzlzX..U.0^p1^p
30	325e 7061 7373 776f 7264 6361 6879 6e61	2^passwordcahyna

Frame 2 (64 on wire, 64 captured)
Arrival Time: Feb 10, 2001 13:08:59.2047
Time delta from previous packet: 0.004726 seconds

```
    Frame Number: 2
    Packet Length: 64 bytes
    Capture Length: 64 bytes

Data (22 bytes)

  0  00e0 b601 3a36 00d0 06d6 9c39 0800 4500   ....:6.....9..E.
 10  0032 a9ac 0000 6f11 257d c82d 1c24 aabb   .2....o.%}.-.$..
 20  bf4b 7a6c 7a58 001e 5518 305e 7031 5e70   .KzlzX..U.0^p1^p
 30  325e 7061 7373 776f 7264 6361 6879 6e61   2^passwordcahyna

Frame 3 (64 on wire, 64 captured)
    Arrival Time: Feb 10, 2001 13:08:59.2273
    Time delta from previous packet: 0.022557 seconds
    Frame Number: 3
    Packet Length: 64 bytes
    Capture Length: 64 bytes
Data (22 bytes)

  0  00e0 b601 3a36 00d0 06d6 9c39 0800 4500   ....:6.....9..E.
 10  0032 abac 0000 6f11 2378 c82d 1c24 aabb   .2....o.#x.-.$..
 20  bf50 7a6c 7a58 001e 5513 305e 7031 5e70   .PzlzX..U.0^p1^p
 30  325e 7061 7373 776f 7264 6361 6879 6e61   2^passwordcahyna

Frame 4 (64 on wire, 64 captured)
    Arrival Time: Feb 10, 2001 13:08:59.2335
    Time delta from previous packet: 0.006264 seconds
    Frame Number: 4
    Packet Length: 64 bytes
    Capture Length: 64 bytes

Data (22 bytes)

  0  00e0 b601 3a36 00d0 06d6 9c39 0800 4500   ....:6.....9..E.
 10  0032 adac 0000 6f11 2174 c82d 1c24 aabb   .2....o.!t.-.$..
 20  bf54 7a6c 7a58 001e 550f 305e 7031 5e70   .TzlzX..U.0^p1^p
 30  325e 7061 7373 776f 7264 6361 6879 6e61   2^passwordcahyna
```

Assignment 2. Describe the state of Intrusion Detection.

Mscan, sscan and synscan the evolution of a worm enabling vulnerablitiy scanner that spans 2 milleniums.

By Donald.J.Smith 5/20/2001

These are very fast, simple and effective scanning and vulnerability detection tools. There are several versions of these tools being reported [20]. Starting with reports on mscan in 1998 [16], sscan report in 1999 [15] and synscan first reported in 2000 [5]. Synscan is the scanning and vulnerability testing engines for ramen [9], canserserver [11] and is included in some versions of the t0rn root kit as t0rnscan [7]. Because of its use in these worms and the current signature database [12] which matches all ID=39426 to synscan. Synscan is the most commonly reported version of this tool today.[20].

Tools used by these scanners.

Nsd From a comment in nsd.c "Written to pry some information out of a nameserver." [2] This tests for iquery and the bind version. This code exists in ramen, lpdW0rm and any worm that uses synscan as the vulnerability scanner. This appears to have a format string overflow vulnerability in its' named version.string printing. This code appears in all versions of mscan, synscan and sscan (renamed to binfo-udp.c in sscan2kpre-6.) It was rewritten and used in the AdmWorm as the overflow for named.

Z0ne Attempts to map a domain by doing an axfr against the dns server for a domain. This code is included with all versions of sscan.

Nat10 The netbois security kit version1.0. Based on code by Andrew Tridgell the author of samba. Andrew DID not write this but the author (unknown) used his code and did give him credit even including the gnu license files as required;-)

Upscan Has a hardcoded ip address in it 206.252.191.1. It appears to be vulnerable to shuting down the listener by spoofing either an icpm or igmp packet from this address to the address of the scanner. This code is included with synscan.c
hping -1 –a 206.252.191.1 ip.address,of.scanner should work.

Tcpsock is the "special" vulnerability scanner code used by synscan. It checks for vulnerabilities in finger, telnet, rpc, bind, and cgi scripts

Scanners

Mscan By JSBach is the granddaddy of them all. First reported in 1998 this scanner became the basis for all of these scanners. However even this code came from other code. Admtelnet from the ADMworm, Joshua Drake's nsd.c, and part of BiT's statd scanner were all used to help create this scanner [2].

Sscan 0.1 By JSBach has a signature that is similar to synscan. The current snort and Whitehats signatures for synscan will alert on sscan0.1 and report this as synscan. I suspect some of the synscan reports are actually sscan. It also has a queSO like fingerprinting scan. Which causes false queSO alerts.
Sscan was the predecessor to synscan. Pyschoid tore lots of code out of sscan to get it to do what he wanted and not much more. He reduced the capabilities but improved the functionality. JSBach the creator of Sscan put this in the readme for this scanner
"NOTE: WE TAKE FULL RESPONSIBILITY FOR EVERYTHING YOU DO ILLEGALLY WITH
THIS PROGRAM. WE CONDONE ILLEGAL AND MALICIOUS USE OF THIS PROGRAM."

Sscan also has documentation in the readme file on how to write an internet worm using sscan and it's modules ability. I suspect this became the blueprint for ramen. According to psychoid at the time of its' release sscan did not work correctly so someone probably used synscan1.6 and the scripting examples include in SSCAN.README to create ramen.

Synscan by psychoid is actually two vulnerability scanners and several support tools. The first is Upscan.c which uses igmp to find hosts that are "up" on a network. Then the attacker can use synscan with a list of ip addresses from a file. IGMP is often allowed through routers by default. Not many IDS systems will alert on IGMP packets. This probably accounts for some of the synscan detects that appear to have only gone to "live" hosts. However synscan can be used without Upscan by just scanning an entire class (a, b or c) network. Synscan.c is based on code from sscan. This scanner appears to have some flaws in it. Several of these have been documented in Joe Stewart's writeups [5]. It is vulnerable to having its' listener process shutdown by spoofing a syn packet from www.microsoft.com which kills the checkvuln function. Spoofing a syn packet from www.microsoft.de on 80 to the scanner's ip address on port 31337 kills the synport receive function which acts as the listener. This does not stop the scanning but the scanner machine will no longer be getting vulnerability information and therefore any worms using this version of synscan as their scanning engine will stop recording vulnerable machines and therefore should stop spreading of worms using this scanner. It also appears to have a remote root buffer overflow based on flaws in the nsd code.

"hping –p 31337 –s 80 –k –S –A –a 212.184.80.190 ip.address,of.scanner" JoeStewart[5]. Where 212.184.80.190 is the address of www.microsoft.de.
Synscan is the scanning and vulnerability testing engines for ramen, canserserver and included in some versions of the t0rn root kit as t0rnscan. Probably because of its use in these worms synscan1.6 is the most commonly reported version of this tool today. In versions 1.8 Dor and Tradegy fixed the nsd format overflow and the shutdown vulnerabilities. The id has been "randomized" and it uses mostly syn's.

I have reviewed publically available versions (1.5,1.6 and 2.1) of the synscan source code they have several flaws that I have not seen documented anywhere else so I will document them here.

1st the reason the sequence numbers and ack numbers don't change more often is because srand is called with unix time function as its seed. Under linux this returns the time to the nearest second. Then rand is called to provide the pseudo random numbers. "These random sequences are repeatable by calling srand with the same seed value." LinuxManpages others have noticed that these numbers appear to change around 50 hosts but it really depends on the speed of the scanning host and the speed of the scan. This tool allows for a delay factor which defaults to 1 tick but can be set to any valid short int.

2nd the network wildcard for loop goes up to 255 which of course is not a valid host id. So when using this tool to scan a classC network address such as 131.1.1 will cause SYNSCAN to scan every host in the 131.1.1 network plus the 255 "net address". A good general ids signature might be to look for address with a 255 in them this should never come from the outside to the inside or from the inside to the outside and is a fairly common mistake among network tool writers

3rd in versions 1.8 and later the id has been randomized however the random code is similar to the code in 1.5 for the randomized ID so it stays the same for 1 second then changes to a new random number.

Sscan2kpre6 is the current released version of sscan and is much more functional then the original sscan or synscan. It includes 170 vulnerability checks for ftp, imap, pop2, pop3, bind, lots of Trojan ports, lots of cgi vulnerabilities and other vulnerabilities.

It has an option for using nmap to guess os or it can do its own queso style os fingerprinting. This queso style fingerprinting has caused numerous incorrect detections. Sscan is much more dangerous then queso if detected as queso then some analysis might just right it off as "yet another scan". The queso style fingerprinting method in this scanner is flawed. It reported Solaris 2.x for a machine running linux 7.0.

This scanner was designed to support an internet worm. The comments in the SSCAN.README file "you could probably write a whole internet worm in the scripting language." is followed by an example of how to use sscan2kpre6 to write an internet worm. This scanner has checks for lots of well known Trojan ports but all but port 31337 is commented out. Uncommenting these would make this a very easily detected scanner.
This scanner trys to use a **POP2** buffer overflow and can use **POP2** banners to fingerprint the os. This might be the port 109 that we are seeing. Steven Northcutt mentioned at SANs2001 in NewOrleans. This scanner uses anonymous as the

username and guest@Microsoft.com as the anonymous ftp login password when checking for anonymous login.

This tools scans for wingates. This is so they can "hide" The default configuration for WinGate allows an intruder to use a WinGate server to conceal his or her true location without the need to forge packets [19].

There are so many versions of this scanner and supporting tools that I have tried to summerise the differences and features here in a table

Flags	Name	#	ID	Ttl	win	Ports	Default port scanned	author	Released reported	Vulnerabilitie
Syn	Mscan	1.0	Starts at 0 add one for every packet	64	32120	> 1024 to scanned port	25, 79, 110, 23,80,143, 53, 6000	Jsbach	6/1998	
Syn, During fingerprinting Queso Flags or nmap	Sscan	0.1	39426	42	1028	???	1,21, 22, 23 25, 53, 79, 110, 111, 139, 143, 1114, 6000, 2766, 31337	Jsbach	1/15/1999	
UDP	Nsd.c	???		64			53	Joshua James Drake	6/9/98	Format bug i statement tha provide remo overflow on t this scanner on.
	Z0ne	1.1					53	ADM	12/9/1999	.
SynFin	synscan	1.5	39426	42	1028	From=to	23, 80, 111, 1080	psychoid	1999	Uses nsd the shares the vu from it. Vulnerable to packets from www.microso scanner:3133
SynFin	Synscan	1.6	39426	42	1028	From=to	23, 80, 111, 1080	Pyschoic	1999	Uses nsd the shares the vu from it. Vulnerable to packets from www.microso scanner:3133
IGMP	Upscan	1.0	17664	255			Igmp type 2 Igmp code 31 Igmp_mtrac e?? Check rcf1112	Pyschoic	1999	
Syn	Synscan	1.8	Random	???	???	???	???	Pyschoic and Dor	???	Not released seen the sou According to

										vulnerable to shutdown an remote buffe was fixed.
SynFin	T0rnscan	?	39426	???	1028	During scan From=to During connection for vulnerability scan > 1024 to wellknown ports	???	???	???	???
Syn	Synscan	1.?	19104	2??	28	During scan From=to During connection for vulnerability scan > 1024 to wellknown ports	21 is all I saw in my detects.	???	???	I have not se but I did capt in the wild.
ACK	Synscan	2.0	Random	255	1028	During scan From=to During connection for vulnerability scan > 1024 to wellknown ports	23 80 111	Dor and Tragedy	????	Not vulnerab Microsoft pa known remot overflow has
Ack During vuln scan syn,ack	Scan2k-Pre6	Pre6	39426	42	1028	During scan From=to During connection for vulnerability scan > 1024 to wellknown ports	1, 21, 22,23,25,53 79, 80, 109, 110, 111, 113, 139, 143, 1114, 2766, 6000, 12345, 12346, 20034, 21544, 31337, 31789, 54320, 65533, , 65535	Eth0, mixter, axess	???	Uses guest@micro password to ftp.
Syn	RpCScaN	1.0	39426	42	1028	During scan From=to During connection for vulnerability scan > 1024 to wellknown ports	23, 25, 143, 110, 80,	Dor and Tragedy		Uses nsd so have the buff

Synscan detects in the wild

Packet capture of Tornscan from http://www.sans.org/y2k/011701-1500.htm
Note 9A02 base16 = 39426 base10.

```
------------------------------------------------------------
Packet 1
TIME:     09:51:55.037837
LINK:     00:02:B3:07:EE:ED -> 00:90:27:B8:B4:21 type=IP
  IP:     216.179.148.250 -> XXX.XXX.XX6.12 hlen=20 TOS=00 dgramlen=40 id=9A02
          MF/DF=0/0 frag=0 TTL=27 proto=TCP cksum=4893
 TCP:     port 9704 -> 9704 seq=0621232889 ack=0573123859
          hlen=20 (data=0) UAPRSF=000011 wnd=1028 cksum=EB95 urg=0
DATA:
------------------------------------------------------------
Packet 2
TIME:     09:51:55.038981 (0.001144)
LINK:     00:90:27:B8:B4:21 -> 00:02:B3:07:EE:ED type=IP
  IP:     XXX.XXX.XX6.12 -> 216.179.148.250 hlen=20 TOS=00 dgramlen=40 id=D109
          MF/DF=0/0 frag=0 TTL=128 proto=TCP cksum=AC8B
 TCP:     port 9704 -> 9704 seq=0000000000 ack=0621232891
          hlen=20 (data=0) UAPRSF=010100 wnd=0 cksum=3EC3 urg=0
DATA:
------------------------------------------------------------
Packet 3
TIME:     09:51:55.057821 (0.018840)
LINK:     00:02:B3:07:EE:ED -> 00:00:F8:1A:41:AF type=IP
  IP:     216.179.148.250 -> XXX.XXX.XX6.13 hlen=20 TOS=00 dgramlen=40 id=9A02
          MF/DF=0/0 frag=0 TTL=27 proto=TCP cksum=4892
 TCP:     port 9704 -> 9704 seq=0621232889 ack=0573123859
          hlen=20 (data=0) UAPRSF=000011 wnd=1028 cksum=EB94 urg=0
DATA:
------------------------------------------------------------
Packet 4
TIME:     09:51:55.058126 (0.000305)
LINK:     00:00:F8:1A:41:AF -> 00:02:B3:07:EE:ED type=IP
  IP:     XXX.XXX.XX6.13 -> 216.179.148.250 hlen=20 TOS=00 dgramlen=40 id=6C4B
          MF/DF=0/0 frag=0 TTL=64 proto=TCP cksum=5149
 TCP:     port 9704 -> 9704 seq=0000000000 ack=0621232890
          hlen=20 (data=0) UAPRSF=010100 wnd=0 cksum=3EC3 urg=0
DATA:
------------------------------------------------------------
Packet 5
TIME:     09:51:55.076996 (0.018870)
LINK:     00:02:B3:07:EE:ED -> 08:00:20:75:03:AA type=IP
  IP:     216.179.148.250 -> XXX.XXX.XX6.14 hlen=20 TOS=00 dgramlen=40 id=9A02
          MF/DF=0/0 frag=0 TTL=27 proto=TCP cksum=4891
 TCP:     port 9704 -> 9704 seq=0621232889 ack=0573123859
          hlen=20 (data=0) UAPRSF=000011 wnd=1028 cksum=EB93 urg=0
DATA:
------------------------------------------------------------
Packet 6
```

TIME: 09:51:55.077456 (0.000460)
LINK: 08:00:20:75:03:AA -> 00:02:B3:07:EE:ED type=IP
IP: XXX.XXX.XX6.14 -> 216.179.148.250 hlen=20 TOS=00 dgramlen=40 id=B14F
MF/DF=0/1 frag=0 TTL=27 proto=TCP cksum=F143
TCP: port 9704 -> 9704 seq=0000000000 ack=0621232890
hlen=20 (data=0) UAPRSF=010100 wnd=0 cksum=3EC2 urg=0
DATA:

Snort of synscan(1.7?) in the wild.
[**] IDS007 - MISC-Source Port Traffic 53 TCP [**]
04/30-12:53:47.751087 194.145.112.1:53 -> MY.NET.Classc.149:53
TCP TTL:26 TOS:0x0 ID:39426
S*** Seq: 0x1A99470A Ack: 0x27FCCF40 Win: 0x28

Snort of synscan(1.8 ??) with id = 19104 Syn only, ttl >= 237 in the wild.

[**] IDS007 - MISC-Source Port Traffic 53 TCP [**]
04/25-21:58:36.562856 210.102.28.200:53 -> MY.NET.CLASSC.5:53
TCP TTL:237 TOS:0x0 ID:19104
S*** Seq: 0x3CC0BC2B Ack: 0x133494B6 Win: 0x28

[**] IDS007 - MISC-Source Port Traffic 53 TCP [**]
04/25-21:58:36.563546 210.102.28.200:53 -> MY.NET.CLASSC.4:53
TCP TTL:237 TOS:0x0 ID:19104
S*** Seq: 0x3CC0BC2B Ack: 0x133494B6 Win: 0x28

[**] IDS007 - MISC-Source Port Traffic 53 TCP [**]
04/25-21:58:36.577969 210.102.28.200:53 -> MY.NET.CLASSC.12:53
TCP TTL:237 TOS:0x0 ID:19104
S*** Seq: 0x3CC0BC2B Ack: 0x133494B6 Win: 0x28

[**] IDS007 - MISC-Source Port Traffic 53 TCP [**]
04/25-21:58:36.599541 210.102.28.200:53 -> MY.NET.CLASSC.25:53
TCP TTL:237 TOS:0x0 ID:19104
S*** Seq: 0x3CC0BC2B Ack: 0x133494B6 Win: 0x28

My Synscan detects in the lab

#Note all lab detects 10.132.0.129 is the attacker (redhat6.1) and 10.132.0.131 is the victim (redhat 7.0).

Snort of upscan

06/03-22:51:30.247618 10.132.0.129 -> 10.132.0.131
IGMP TTL:255 TOS:0x0 ID:17664 IpLen:20 DgmLen:45
02 1F 00 00 0A 84 00 81 2A 2A 2A 2A 2A 2A 2A 2A .....********
2A 2A 2A 2A 2A 2A 2A 2A *********

+=+

Snort of sysscan1.5 showing syn, then full connect port 21.

06/03-22:54:00.342166 10.132.0.129:21 -> 10.132.0.131:21
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x454F6975 Ack: 0x5734CE73 Win: 0x404 TcpLen: 20

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.343661 10.132.0.131:21 -> 10.132.0.129:21
TCP TTL:64 TOS:0x0 ID:14 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62D20981  Ack: 0x454F6976  Win: 0x7FB8  TcpLen: 24
TCP Options (1) => MSS: 536
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.343732 10.132.0.129:21 -> 10.132.0.131:21
TCP TTL:255 TOS:0x0 ID:5 IpLen:20 DgmLen:40
*****R** Seq: 0x454F6976  Ack: 0x0  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.365025 10.132.0.129:1046 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:6 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCEC27F9F  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 5191434 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.365411 10.132.0.131:21 -> 10.132.0.129:1046
TCP TTL:64 TOS:0x0 ID:15 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x63AD6D89  Ack: 0xCEC27FA0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 138330 5191434 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.365472 10.132.0.129:1046 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:7 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCEC27FA0  Ack: 0x63AD6D8A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5191434 138330
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.427869 10.132.0.131:1025 -> 10.132.0.129:113
TCP TTL:64 TOS:0x0 ID:16 IpLen:20 DgmLen:60 DF
******S* Seq: 0x63A815F4  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 138336 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:00.427916 10.132.0.129:113 -> 10.132.0.131:1025
TCP TTL:255 TOS:0x0 ID:8 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x63A815F5  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:10.377262 10.132.0.129:1046 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:10 IpLen:20 DgmLen:52 DF
***A***F Seq: 0xCEC27FA0  Ack: 0x63AD6D8A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5192435 138330
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:10.377751 10.132.0.131:21 -> 10.132.0.129:1046
TCP TTL:64 TOS:0x10 ID:21 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x63AD6D8A  Ack: 0xCEC27FA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 139331 5192435
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

06/03-22:54:20.590643 10.132.0.131:21 -> 10.132.0.129:1046
TCP TTL:64 TOS:0x10 ID:26 IpLen:20 DgmLen:130 DF
```

```
***AP*** Seq: 0x63AD6D8A  Ack: 0xCEC27FA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 140352 5192435
32 32 30 20 70 31 36 36 20 46 54 50 20 73 65 72  220 p166 FTP ser
76 65 72 20 28 56 65 72 73 69 6F 6E 20 77 75 2D  ver (Version wu-
32 2E 36 2E 31 28 31 29 20 57 65 64 20 41 75 67  2.6.1(1) Wed Aug
20 39 20 30 35 3A 35 34 3A 35 30 20 45 44 54 20   9 05:54:50 EDT
32 30 30 30 29 20 72 65 61 64 79 2E 0D 0A        2000) ready...

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/03-22:54:20.590762 10.132.0.129:1046 -> 10.132.0.131:21
TCP TTL:255 TOS:0x10 ID:11 IpLen:20 DgmLen:40
*****R** Seq: 0xCEC27FA1  Ack: 0x0  Win: 0x0  TcpLen: 20

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Snort of synscan1.6 listener being shutdown with an hping.

```
05/08-17:34:06.227502 10.132.0.130:21 -> 10.132.0.131:21
TCP TTL:42 TOS:0x0 ID:39426
**SF**** Seq: 0x69C73A3B   Ack: 0x238FADA1   Win: 0x404
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
05/08-17:34:06.227680 10.132.0.131:21 -> 10.132.0.130:21
TCP TTL:64 TOS:0x0 ID:17912  DF
**S***A* Seq: 0xCEF3B779   Ack: 0x69C73A3C   Win: 0x7FB8
TCP Options => MSS: 536
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
05/08-17:34:06.228004 10.132.0.130:21 -> 10.132.0.131:21
TCP TTL:255 TOS:0x0 ID:14801
****R*** Seq: 0x69C73A3C   Ack: 0x0   Win: 0x0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

05/08-17:34:30.376707 10.132.0.253:80 -> 10.132.0.130:31337
TCP TTL:64 TOS:0x0 ID:57205
**S***A* Seq: 0x1C5B3617   Ack: 0x1C476939   Win: 0x200
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Snort of sscan2k-pre6

```
06/03-23:30:03.976648 10.132.0.129:23 -> 10.132.0.131:23
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x1C42187E  Ack: 0x1578081F  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+

06/03-23:30:03.977100 10.132.0.131:23 -> 10.132.0.129:23
TCP TTL:255 TOS:0x0 ID:109 IpLen:20 DgmLen:40
*****R** Seq: 0x1578081F  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+

06/03-23:30:03.987664 10.132.0.129:25 -> 10.132.0.131:25
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
```

A* Seq: 0x1C42187E Ack: 0x1578081F Win: 0x404 TcpLen: 20

=+
+

06/03-23:30:03.987977 10.132.0.131:25 -> 10.132.0.129:25
TCP TTL:255 TOS:0x0 ID:110 IpLen:20 DgmLen:40
*****R** Seq: 0x1578081F Ack: 0x0 Win: 0x0 TcpLen: 20

A "little while later" sscan comes back to check for vulnerabilities in "open" ports it found during it's ack sweep port 25 was open.

06/03-23:30:04.070935 10.132.0.129:1073 -> 10.132.0.131:25
TCP TTL:64 TOS:0x0 ID:75 IpLen:20 DgmLen:60 DF
******S* Seq: 0x5712F1E5 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 5407805 0 NOP WS: 0

=+
+

06/03-23:30:04.071219 10.132.0.129:1074 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:76 IpLen:20 DgmLen:60 DF
******S* Seq: 0x56866109 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 5407805 0 NOP WS: 0

=+
+

06/03-23:30:04.071360 10.132.0.131:25 -> 10.132.0.129:1073
TCP TTL:64 TOS:0x0 ID:117 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0xEB3976D3 Ack: 0x5712F1E6 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 354707 5407805 NOP WS: 0

=+
+

06/03-23:30:04.071422 10.132.0.129:1073 -> 10.132.0.131:25
TCP TTL:64 TOS:0x0 ID:77 IpLen:20 DgmLen:52 DF
A* Seq: 0x5712F1E6 Ack: 0xEB3976D4 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 5407805 354707

=+
+
A little while later it checks ftp using a null account.

=+
06/03-23:30:15.228130 10.132.0.131:21 -> 10.132.0.129:1087
TCP TTL:64 TOS:0x0 ID:150 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0xEC07E64A Ack: 0x5736D568 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 355823 5408921 NOP WS: 0

=+
06/03-23:30:15.228185 10.132.0.129:1087 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:106 IpLen:20 DgmLen:52 DF
A* Seq: 0x5736D568 Ack: 0xEC07E64B Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 5408921 355823

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:15.228570 10.132.0.129:1087 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:107 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x5736D568  Ack: 0xEC07E64B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5408921 355823
55 53 45 52 20 4E 55 4C 4C 0A                    USER NULL.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:15.228962 10.132.0.131:21 -> 10.132.0.129:1087
TCP TTL:64 TOS:0x0 ID:151 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEC07E64B  Ack: 0x5736D572  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 355823 5408921

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:15.228998 10.132.0.129:1087 -> 10.132.0.131:21
TCP TTL:64 TOS:0x0 ID:108 IpLen:20 DgmLen:64 DF
***AP*** Seq: 0x5736D572  Ack: 0xEC07E64B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5408921 355823
50 41 53 53 20 4E 55 4C 4C 0A 0A 0A              PASS NULL...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:15.232866 10.132.0.131:1035 -> 10.132.0.129:113
TCP TTL:64 TOS:0x0 ID:152 IpLen:20 DgmLen:60 DF
******S* Seq: 0xEB79461E  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 355823 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:15.232906 10.132.0.129:113 -> 10.132.0.131:1035
TCP TTL:255 TOS:0x0 ID:109 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0xEB79461F  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=0
06/03-23:30:15.238062 10.132.0.131:21 -> 10.132.0.129:1087
TCP TTL:64 TOS:0x0 ID:153 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEC07E64B  Ack: 0x5736D57E  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 355824 5408921

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
06/03-23:30:24.243713 10.132.0.131:21 -> 10.132.0.129:1074
TCP TTL:64 TOS:0x10 ID:165 IpLen:20 DgmLen:130 DF
***AP*** Seq: 0xEB6BB3EB  Ack: 0x5686610B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 356724 5407806
32 32 30 20 70 31 36 36 20 46 54 50 20 73 65 72  220 p166 FTP ser
76 65 72 20 28 56 65 72 73 69 6F 6E 20 77 75 2D  ver (Version wu-
32 2E 36 2E 31 28 31 29 20 57 65 64 20 41 75 67  2.6.1(1) Wed Aug
20 39 20 30 35 3A 35 34 3A 35 30 20 45 44 54 20   9 05:54:50 EDT
32 30 30 30 29 20 72 65 61 64 79 2E 0D 0A        2000) ready...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Mscan snort log

```
06/05-23:12:48.237823 10.132.0.129:1036 -> 10.132.0.131:25
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91F0C5AD  Ack: 0x0  Win: 0x7D78  TcpLen: 40
```

```
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.238913 10.132.0.131:25 -> 10.132.0.129:1036
TCP TTL:64 TOS:0x0 ID:14 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x25F70F24  Ack: 0x91F0C5AE  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 322123 89022 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.238978 10.132.0.129:1036 -> 10.132.0.131:25
TCP TTL:64 TOS:0x0 ID:1 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x91F0C5AE  Ack: 0x25F70F25  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 89022 322123

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.239071 10.132.0.129:1036 -> 10.132.0.131:25
TCP TTL:64 TOS:0x0 ID:2 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x91F0C5AE  Ack: 0x25F70F25  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 89022 322123

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.239195 10.132.0.129:1037 -> 10.132.0.131:79
TCP TTL:64 TOS:0x0 ID:3 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91A5C812  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.239491 10.132.0.131:25 -> 10.132.0.129:1036
TCP TTL:64 TOS:0x0 ID:15 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x25F70F25  Ack: 0x91F0C5AF  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 322123 89022

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.239589 10.132.0.131:79 -> 10.132.0.129:1037
TCP TTL:255 TOS:0x0 ID:16 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91A5C813  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.239672 10.132.0.129:1038 -> 10.132.0.131:110
TCP TTL:64 TOS:0x0 ID:4 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91D901E6  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240030 10.132.0.131:110 -> 10.132.0.129:1038
TCP TTL:255 TOS:0x0 ID:17 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91D901E7  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240104 10.132.0.129:1039 -> 10.132.0.131:23
TCP TTL:64 TOS:0x0 ID:5 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91DF865F  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240449 10.132.0.131:23 -> 10.132.0.129:1039
TCP TTL:255 TOS:0x0 ID:18 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91DF8660  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240520 10.132.0.129:1040 -> 10.132.0.131:80
TCP TTL:64 TOS:0x0 ID:6 IpLen:20 DgmLen:60 DF
******S* Seq: 0x9159E3B6  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240837 10.132.0.131:80 -> 10.132.0.129:1040
TCP TTL:255 TOS:0x0 ID:19 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x9159E3B7  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.240908 10.132.0.129:1041 -> 10.132.0.131:143
TCP TTL:64 TOS:0x0 ID:7 IpLen:20 DgmLen:60 DF
******S* Seq: 0x915F991B  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.241222 10.132.0.131:143 -> 10.132.0.129:1041
TCP TTL:255 TOS:0x0 ID:20 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x915F991C  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.241316 10.132.0.129:1042 -> 10.132.0.131:53
TCP TTL:64 TOS:0x0 ID:8 IpLen:20 DgmLen:60 DF
```

```
******S* Seq: 0x91B2F077  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.241629 10.132.0.131:53 -> 10.132.0.129:1042
TCP TTL:255 TOS:0x0 ID:21 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91B2F078  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.241699 10.132.0.129:1043 -> 10.132.0.131:110
TCP TTL:64 TOS:0x0 ID:9 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91175686  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242011 10.132.0.131:110 -> 10.132.0.129:1043
TCP TTL:255 TOS:0x0 ID:22 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91175687  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242081 10.132.0.129:1044 -> 10.132.0.131:110
TCP TTL:64 TOS:0x0 ID:10 IpLen:20 DgmLen:60 DF
******S* Seq: 0x91BA9526  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242396 10.132.0.131:110 -> 10.132.0.129:1044
TCP TTL:255 TOS:0x0 ID:23 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x91BA9527  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242466 10.132.0.129:1045 -> 10.132.0.131:6000
TCP TTL:64 TOS:0x0 ID:11 IpLen:20 DgmLen:60 DF
******S* Seq: 0x9146B4E6  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 89022 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242821 10.132.0.131:6000 -> 10.132.0.129:1045
TCP TTL:64 TOS:0x0 ID:24 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x25D44BA0  Ack: 0x9146B4E7  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 322123 89022 NOP WS: 0
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242846 10.132.0.129:1045 -> 10.132.0.131:6000
TCP TTL:64 TOS:0x0 ID:12 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x9146B4E7  Ack: 0x25D44BA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 89022 322123

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.242914 10.132.0.129:1045 -> 10.132.0.131:6000
TCP TTL:64 TOS:0x0 ID:13 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x9146B4E7  Ack: 0x25D44BA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 89022 322123

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.243264 10.132.0.131:6000 -> 10.132.0.129:1045
TCP TTL:64 TOS:0x0 ID:25 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x25D44BA1  Ack: 0x9146B4E8  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 322123 89022

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.243879 10.132.0.131:6000 -> 10.132.0.129:1045
TCP TTL:64 TOS:0x0 ID:26 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x25D44BA1  Ack: 0x9146B4E8  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 322123 89022

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.243918 10.132.0.129:1045 -> 10.132.0.131:6000
TCP TTL:64 TOS:0x0 ID:14 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x9146B4E8  Ack: 0x25D44BA2  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 89022 322123

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.457882 10.132.0.131:1025 -> 10.132.0.129:113
TCP TTL:64 TOS:0x0 ID:27 IpLen:20 DgmLen:60 DF
******S* Seq: 0x25D1273A  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 322145 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.457961 10.132.0.129:113 -> 10.132.0.131:1025
TCP TTL:255 TOS:0x0 ID:15 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x25D1273B  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+
```

```
06/05-23:12:48.941113 10.132.0.131:25 -> 10.132.0.129:1036
TCP TTL:64 TOS:0x0 ID:28 IpLen:20 DgmLen:128 DF
***AP*** Seq: 0x25F70F25  Ack: 0x91F0C5AF  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 322193 89022
32 32 30 20 72 65 64 68 61 74 37 2E 30 20 45 53  220 redhat7.0 ES
4D 54 50 20 53 65 6E 64 6D 61 69 6C 20 38 2E 31  MTP Sendmail 8.1
31 2E 30 2F 38 2E 31 31 2E 30 3B 20 54 75 65 2C  1.0/8.11.0; Tue,
20 35 20 4A 75 6E 20 32 30 30 31 20 31 37 3A 30   5 Jun 2001 17:0
35 3A 30 37 20 2D 30 36 30 30 0D 0A              5:07 -0600..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:12:48.941179 10.132.0.129:1036 -> 10.132.0.131:25
TCP TTL:255 TOS:0x0 ID:16 IpLen:20 DgmLen:40
*****R** Seq: 0x91F0C5AF  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Snort of rpcscan
Here it is just scanning for open ports.

```
06/05-23:43:12.814906 10.132.0.129:23 -> 10.132.0.131:23
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.815352 10.132.0.131:23 -> 10.132.0.129:23
TCP TTL:255 TOS:0x0 ID:29 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.826893 10.132.0.129:25 -> 10.132.0.131:25
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.827213 10.132.0.131:25 -> 10.132.0.129:25
TCP TTL:255 TOS:0x0 ID:30 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.847283 10.132.0.129:143 -> 10.132.0.131:143
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.847591 10.132.0.131:143 -> 10.132.0.129:143
TCP TTL:255 TOS:0x0 ID:31 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.866890 10.132.0.129:110 -> 10.132.0.131:110
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.867195 10.132.0.131:110 -> 10.132.0.129:110
TCP TTL:255 TOS:0x0 ID:32 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.886880 10.132.0.129:80 -> 10.132.0.131:80
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**** Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.887186 10.132.0.131:80 -> 10.132.0.129:80
TCP TTL:255 TOS:0x0 ID:33 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.913982 10.132.0.129:1046 -> 10.132.0.131:23
TCP TTL:64 TOS:0x0 ID:17 IpLen:20 DgmLen:60 DF
******S* Seq: 0x42AEB6F  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 271489 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.914307 10.132.0.131:23 -> 10.132.0.129:1046
TCP TTL:255 TOS:0x0 ID:34 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x42AEB70  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Here it starts getting the rpcportmapper information.

```
06/05-23:43:12.914652 10.132.0.129:1047 -> 10.132.0.131:111
TCP TTL:64 TOS:0x0 ID:18 IpLen:20 DgmLen:60 DF
******S* Seq: 0x470F312  Ack: 0x0  Win: 0x7D78  TcpLen: 40
```

```
TCP Options (5) => MSS: 1460 SackOK TS: 271489 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.915615 10.132.0.131:111 -> 10.132.0.129:1047
TCP TTL:64 TOS:0x0 ID:35 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x989A6B59  Ack: 0x470F313  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 504596 271489 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.915657 10.132.0.129:1047 -> 10.132.0.131:111
TCP TTL:64 TOS:0x0 ID:19 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x470F313  Ack: 0x989A6B5A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 271489 504596

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.915993 10.132.0.129:1047 -> 10.132.0.131:111
TCP TTL:64 TOS:0x0 ID:20 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x470F313  Ack: 0x989A6B5A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 271489 504596

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.916365 10.132.0.131:111 -> 10.132.0.129:1047
TCP TTL:64 TOS:0x0 ID:36 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x989A6B5A  Ack: 0x470F314  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 504596 271489

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.916646 10.132.0.131:111 -> 10.132.0.129:1047
TCP TTL:64 TOS:0x0 ID:37 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x989A6B5A  Ack: 0x470F314  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 504596 271489

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.916677 10.132.0.129:1047 -> 10.132.0.131:111
TCP TTL:64 TOS:0x0 ID:21 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x470F314  Ack: 0x989A6B5B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 271489 504596

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.942073 10.132.0.129:1048 -> 10.132.0.131:23
TCP TTL:64 TOS:0x0 ID:22 IpLen:20 DgmLen:60 DF
******S* Seq: 0x422E337  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 271492 0 NOP WS: 0
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.942410 10.132.0.131:23 -> 10.132.0.129:1048
TCP TTL:255 TOS:0x0 ID:38 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x422E338  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.942687 10.132.0.129:1 -> 10.132.0.131:111
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A**S* Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.942991 10.132.0.131:111 -> 10.132.0.129:1
TCP TTL:255 TOS:0x0 ID:39 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.956882 10.132.0.129:2 -> 10.132.0.131:111
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
*******F Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.976879 10.132.0.129:3 -> 10.132.0.131:111
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
***A***F Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.977178 10.132.0.131:111 -> 10.132.0.129:3
TCP TTL:255 TOS:0x0 ID:40 IpLen:20 DgmLen:40
*****R** Seq: 0x483344F6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.996879 10.132.0.129:4 -> 10.132.0.131:111
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x3EE924EE  Ack: 0x483344F6  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.997192 10.132.0.131:111 -> 10.132.0.129:4
TCP TTL:64 TOS:0x0 ID:41 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x98D9E7D7  Ack: 0x3EE924EF  Win: 0x7FB8  TcpLen: 24
TCP Options (1) => MSS: 536
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:12.997230 10.132.0.129:4 -> 10.132.0.131:111
TCP TTL:255 TOS:0x0 ID:23 IpLen:20 DgmLen:40
*****R** Seq: 0x3EE924EF  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

06/05-23:43:13.016882 10.132.0.129:5 -> 10.132.0.131:111
TCP TTL:42 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
****P*** Seq: 0x6D71C4E1  Ack: 0x3DAB13E1  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+
```

Assignment 3 "Analyze This"
Computer Security Report for GAIC.com
Definitions:
Compromised host: A host that is inside your network that is probably being controlled by someone outside your network without authorization. These are characterized by unusual activity such as port scanning other hosts or DDOS attacks.

Scanner: A host either internal or external that is performing some type of port scans on other hosts. These are characterized by the number of packets per second and by known scan signatures such as ACK=0, which implies an nmap, scan.

Gamer: A host either internal or external that appears to be running one of the network version of a game such as Unreal, Quake or Half-life. Ports and activity characterize these.

Network Anomalies: Any unusual event in the network. This includes, but is not limited to, bad packets such as illegal TCP flag combinations and packets not destined for the correct server such as a dns client that is misconfigured.

Number of Reports: This is not the number of packets. This is the number of lines in the logs that match this system for a specific type of incident.

This report is based on information contained in the zips received.
The logs start Nov-25-2000 and end Jan-19-2001

There are missing logs. Specifically in December there are no log entries for the 12th, 15th and the 19th. The snap length on the scans was 68 additional information could be obtained by capturing a full Ethernet packet. The reports should be generated in the same format to make parsing easier.

This network has several problems.
There are hosts that appear to have been compromised, game servers, game clients, misconfigured clients asking machines outside the network for information they should be getting internally.

These require immediate investigation these hosts may all be compromised.
These hosts are scanning external hosts.

Scans Reported	From
6290	MY.NET.217.150
4935	MY.NET.217.158
3009	MY.NET.100.230
2203	MY.NET.219.126
2002	MY.NET.253.24
1492	MY.NET.217.126
1328	MY.NET.217.182
498	MY.NET.140.21
330	MY.NET.1.3
301	MY.NET.1.5

These Hosts scanned this net numerous times. The Network administrators should be notified so they can stop these scans.

From address	Number of reports	Domain name and email address to notify.	Port/type of scan
212.64.74.169	22549	Casema Internet Knowledge Center address: Postbus / P.O. BOX 345 address: NL - 2600 AH Delft, Netherlands Network Operations Centre (NOC137-ORG) domain-tech@EURO.NET	21
24.7.86.215	2316	@Home Network abuse@HOME.COM	

24.113.198.51	1074	Rogers@Home abuse@HOME.COM	
216.99.200.242	10660	Secure design On demand port scanner herzogs@SDESIGN.COM	SYN and UDP including some Trojan ports
24.3.0.36	10007	@Home Network abuse@HOME.COM	
152.163.206.134	9697	America Online domains@aol.net	
63.78.39.192	679	192.dsl7839.rcsis.com UUNET Technologies dnsadmin@RCSIS.COM	Syn, queso
24.189.31.228	2446	Optimum Online (Cablevision Systems) hostmaster@CV.NET	
62.227.243.120	7991	Deutsche Telekom AG d.kaufmann@T-ONLINE.NET	
134.192.143.247	4892	U of Maryland Baltimore fsmith@umaryland.edu	
147.8.182.157	14368	University of Hong Kong kty@CC.HKU.HK	

62.158.93.109	21920	DeutcheTelecom abuse@t-ipnet.de	21 Syn not synscan.
24.3.29.129	257	md.home.com abuse@home.com	
128.244.27.166	66	jhvapl.edu (John Hopkins U) sfp@APLCOMM.JHUAPL.EDU	
24.23.62.234	48	md.home.com abuse@home.com	

Detailed report of hosts that scanned this network.
194.197.170.7 scanned your network over 1500 times on ports 21(ftp), 53(DNS), 109(POP2), and 9055. This was a very interesting scan. The ID was constant 39426 several others have reported the constant ID 39426 scans this was synscan.

Some of the hosts on your network appear to be compromised!

Detailed report of compromised host.

My.Net.60.8 began getting scanned on 11/24, this included OS fingerprinting, SYN-FIN, Port scans and finally on 12/13 on port 33715. On 12/16 My.net.60 started scanning outside hosts. At this point I believe it was compromised.

MY.NET.217.150 was scanned a few times for interesting ports Wingate, back orifice, and smb wildcard. On Jan 12th this machine kicked off the ids scanner while "scanning" for game server. Later that same day 151.23.32.23 sent MY.NET.217.150 some unusual udp packets. The sending port number incremented by 100 consistently. This machine scanned lots of outside hosts. This scan was picked up because of the flags that were set. Basically all combinations were tried. It sent lots of UDP packets to what appear to be game servers on the external network. On Jan 15th it appears this same machine was used in a DDOS it sent 3842 syns to a single host while scanning others. This other "scanning" was with weird flags this could have been some kind of communication channel like trinoo. The primary host it was DDOSing was 216.3.226.131 all to ports 1788 and 1789 alternating between these ports.

MY.NET.217.142 acted similar. Scanning and DDOSing on similar ports but it did not get involved in the SYN flood of 216.3.226.131.
MY.NET.217.158 was involved scanning with weird flags too. Udp packets to game servers on the udp port used to play starseige TRIBES this machine was used in DDOSing 207.172.3.55.

MY.NET.217.182 was scanned for ftp on Dec 9th then also started scanning with weird flags on Dec 16.

A group of your machines appear to have participated in a DDOS.

MY.NET.202.30
On Dec 21st around 2:30 24.191.63.215 sent 3 UDP packets to MY.NET.202.30 from port 4703 to port 21.
At 15:47 MY.NET.202.30 started sending UDP packets from ports ranging 1343 – 4992 to 100s of outside hosts on 5digit port numbers. This looks like a client server DDOS with MY.NET.202.30 being a zombie/server for 24.191.63.215.
MY.NET.202.30 did the same thing on 12/22, 01-04 sending out over a thousand packets.

MY.NET.100.230 sent 827 UDP packets to port 53 on 198.41.0.4. It appears that this and several other machines are being used in a DNS DDOS. Port 53 on the 198.41.0.4 machine was hit 827 times in 12 days by this one machine.
MY.NET.100.230 was also used for scanning there are 23670 reported scans. It scanned on SMTP (tcp port 25), DNS (udp port 53) , IDENT (tcp port 113), ftp (tcp port 21) and is almost certainly compromised or being used as a scanner of external hosts by its user.

MY.NET.1.8 sent 57 UDP packets to 198.41.0.4 in one day.
Several of these machines are VeriSign. I suspect the ones that did not resolve beyond the ISP might be Verisign hosts also since this attack appears to be aimed at Verisign at least the 198.41.0.101 address.

Host	Who is That
198.41.0.4	VeriSign Global Registry Services
198.41.0.101	Net-Internic
137.39.1.3	UUNET Technologies, Inc.
205.188.185.18	VeriSign

Note when looking up 205.188.185.18 I got the following message

Possible forgery - c.gtld-servers.net is claiming to be 205.188.185.18, but 205.188.185.18 isn't a valid address for c.gtld-servers.net
It would be a real problem if VeriSign certificate servers were DNS redirected to somewhere else.

My.net.71.38 seems to be a gamer server it has gotten a lot of 7777 and 7778 packets. This is a set of on line games known as Unreal.

Host	Who is that
147.8.182.157	Geographical domain of Hong Kong
151.200.22.41	Bell Atlantic Internet Solutions

194.251.249.32	Sonera Oyj
216.35.30.57	Mpath Interactive, Inc.
205.244.188.35	First Commerce Bank
212.185.240.190	Deutsche Telekom
62.158.55.36	Deutsche Telekom
216.99.200.242	Secure Design

MY.NET.217.182 and MY.NET.217.150 are scanning external hosts with “weird tcp options set” on port 2340. It looks like a buffer overflow attempt.

Host	Reports	Who is that
128.205.187.29	2	State University of New York at Buffalo
24.3.170.90	2050	ATHOME.com
24.188.12.238	2340	CSC Holdings, Inc.

External SMB Scans

From	Port	Who is That	To
64.230.24.78	137	BELLCANADA-5	MY.NET.206.134

Internal SMB Scans
MY.NET.101.160 scanned MY.NET.101.192 58 times.

Misconfigured dhcp clients SMB Scans

From	Port	To
169.254.140.158	137	MY.NET.206.134

Misconfigured dhcp client portscans
169.254.92.200
169.254.75.93

The address space 169.254.x.x is reserved for dhcp clients who did not get an ip address from their dhcp server.

A weird flags scan SFRP*U

From	Reports	Who is That
63.252.118.198	18245	SplitRock Services, Inc

REFERENCES:
Source:

1. A copy of the source for synscan1.6 is available here.
http://www.psychoid.lam3rz.de/synscan1.6.tar.gz

2. A copy of mscan can be obtained here.
http://digital-r00t.error32.com/Unix/mscan_tar[1].gz

3. A copy of tornscan cab be obtained here.
http://torn.kaapeli.net/junk/zip/

Writeups:

4. Writeup by jsbach about mscan
http://www.geek-girl.com/ids/1999/0020.html

5. Write up on syncan by Joe Stewart
http://archives.linuxbe.org/arch055/0017.html

6. Writeup on synscan by Daniel Martin
http://archives.linuxbe.org/arch055/0021.html

7. Writeup on T0rnScan by Chris Kuethe
http://www.sans.org/y2k/011701-1500.htm

8. Another T0rnScan write up
http://tfm.profm.ro/index.html

9. Writeup by Max Butler aka Max Vision on ramen including the scanning tool that was used SYNSCAN
http://whitehats.com/library/worms/ramen/index.html

10. Writeup on sscan-2k by George.Bakos
http://www.sans.org/y2k/practical/George_Bakos.html

11. Write up on cancerserver by dor.
http://archives.linuxbe.org/arch055/0654.html

Whitehats signatures

12. For incoming triggering on ID=39426 and SynFin
http://www.whitehats.com/info/IDS459

13. For outgoing triggers on source port 31337, dest port 80 and destination host of www.microsoft.de.
http://www.whitehats.com/info/IDS450

14. For incoming triggering on ID=19104 and Syn. I submitted this one based on detects I have seen in my snort logs.
http://www.whitehats.com/info/ID521

Cert
15. Cert advisory on Sscan in 1999
http://www.cert.org/incident_notes/IN-99-01.html

16. Cert advisory on mscan in 1998
http://www.cert.org/incident_notes/IN-98.02.html

17. Cert advisory for ramen.
http://www.cert.org/incident_notes/IN-2001-01.html

18. Cert advisory for rpc.statd, wu-ftpd discusses t0rnkit
http://www.cert.org/incident_notes/IN-2000-10.html

19. Wingate vulnerabiltiy
http://www.cert.org/vul_notes/VN-98.03.WinGate.html

20. **Global Incident Analysis Center: Detects**
Analyzed with 39426 as part of the detect. These are just from one page of a search on 39426 on the sans.org site! “Your search for 39426 resulted in 131 matches.”

http://www.sans.org/y2k/102400.htm
http://www.sans.org/y2k/011501-1500.htm
http://www.sans.org/y2k/061000.htm
http://www.sans.org/y2k/081600-1500.htm
http://www.sans.org/y2k/040400-000.htm
http://www.sans.org/y2k/091500.htm
http://www.sans.org/y2k/070100.htm
http://www.sans.org/y2k/080400.htm
http://www.sans.org/y2k/061200.htm
http://www.sans.org/y2k/021501-1200.htm
http://www.sans.org/y2k/110800.htm
http://www.sans.org/y2k/012001.htm
http://www.sans.org/y2k/091600.htm
http://www.sans.org/y2k/012301.htm
http://www.sans.org/y2k/021500.htm

http://www.sans.org/y2k/071600.htm
http://www.sans.org/y2k/061300.htm
http://www.sans.org/y2k/022900-1500.htm
http://www.sans.org/y2k/020101.htm
http://www.sans.org/y2k/112900-1500.htm
http://www.sans.org/y2k/111600.htm

GIAC practicals that include ID 39426.
http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm
http://www.sans.org/y2k/practical/Eric_Hacker.html
http://www.sans.org/sj00/learning.htm

Last Updated: January 19th, 2018

Upcoming Training

Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
Community SANS Baltimore SEC503	Baltimore, MD	Mar 12, 2018 - Mar 17, 2018	Community SANS
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, United Arab Emirates	Apr 07, 2018 - Apr 12, 2018	Live Event
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 14, 2018	vLive
Community SANS Virginia Beach SEC503	Virginia Beach, VA	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced