Global Information Assurance Certification Paper

THE SCOPE OF INTRUSION DETECTION IN A TACTICAL RESPONSE STRATEGY

by

Stan Hoffman, CCNP

A paper submitted in partial fulfillment of the requirements for the certification of

GIAC Certified Intrusion Analyst

GIAC

2001

Program Authorized
to Offer Certification: GIAC Certified Intrusion Analyst Online V3.0

Date: October 28, 2001

GIAC Intrusion Analyst V3.0

Abstract

THE ROLE OF OUT-OF-BAND DATA IN A TACTICAL RESPONSE SCENARIO

by Stan Hoffman, CCNP

The purpose of this paper is to demonstrate that a variety of out-of-band data sources can support intrusion detection in a tactical response paradigm. By tactical response, the reference is to an in-time attempt to mitigate the effects of an ongoing, or imminent, attack on the target systems. This is in contrast to a forensic, or strategic, analysis, which, while offering a deeper understanding of the tools and methods used in the attack, demands time and resources that are often unavailable during an online response scenario. As will be seen, however, correlation with available forensic data during the response decision phase is often a critical component in choosing the course most likely to produce a positive result.

The tactical response model that will be followed consists of the steps (1) Monitoring, (2) Alerting, (3) Analysis, (4) Planning, and (5) Response. Strategic, or long-term, planning, while vitally necessary, will be considered outside the scope of this examination.

Examples will be used from the real world experience that was gained in dealing with the recent (Sept 2001) W32.nimda worm outbreak.

SANS GIAC INTRUSION DETECTION IN DEPTH

ONLINE TRAINING 2001

V3.0

Assignment 1 – Describe the State of Intrusion Detection (30 points possible)

THE ROLE OF OUT-OF-BAND DATA IN A TACTICAL RESPONSE SCENARIO

BY *STAN HOFFMAN, CCNP*

Stephen Northcutt makes the observation that "Intrusion detection is not a specific tool, but a capability, a blending of tools and techniques".[1] The NSA glossary defines intrusion detection as, "Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data."[2]. By including in our detection horizon the many sources of information available to the intrusion analyst, we can open our "window of detection" orders of magnitude beyond that of even the best IDS product operating as a stand-alone detection source.

The focus of this paper is an examination of the roles played by Out-of-band data sources in a tactical response scenario. The impetus for this study came about as a direct result of the experience gained during the recent W32.nimda worm outbreak (Sep 2001). Examples will be drawn from the actual response to that incident.

Tactical Response – a framework

Tactical response can be as basic as the system admin sending a notice to the corporate CIRT and awaiting instructions. Or, it can be the more challenging situation of a lone network engineer, system admin, or user-support person alone in the data center at 2AM staring at indicators that tell them that "all is not well" with their network. The common factor in this situation is the need for local decision making in an online environment. Let's start by examining a definition of the conditions for tactical decision-making.

"There are Four major aspects of tactical decision making:

[1] Northcutt & Novak, Network Intrusion Detection, An Analyst's Handbook *2e* New Riders Publishing, 2001, Page 118

[2] NSA Glossary of Terms Used in Security and Intrusion Detection
URL: http://www.sans.org/newlook/resources/glossary.htm

- **Real-time** -- in tactical domains, data arrive and must be processed in real-time, so decisions have temporal constraints. Making the right decision too late is as bad (or worse!) than making the wrong decision in a timely manner
- **Opportunistic and uncertain** -- while the tactical decision maker will have clear goals, the external events to be faced will typically be unpredictable. This means that it will be unclear exactly what decisions may be required until the situation unfolds. Moreover, the results of actions taken by the person are uncertain (i.e., they may or may not have the desired result). The decision maker thus must adapt both to the unfolding situation and to the results of actions taken..
- **Multi-tasking** -- the pace of events and the uncertain nature of the process require the decision maker to be prepared to interrupt any cognitive activity to address a more critical decision at any time. This will typically result in a weakly-concurrent multi-tasking, in which the decision maker may have several decision processes underway at a time (with one processing and the others suspended).
- **Situated in computer-based and verbal interactions** -- the majority of information available to the tactical decision maker comes not from direct sensation of the problem environment, but rather through information displayed at computer-based workstations and verbal messages from teammates. Similarly, decisions are implemented not through direct action, but as interactions with the computer workstation or verbal messages to other persons. "[3]

As you can see, the goals of tactical decision making align closely with the experience of daily operations in Intrusion Detection and Incident Handling. The same need to be aware of the immediate issues, peripheral signals and possible consequences, informs both models.

The goal of tactical response, as used in this study, is that of responding to an online threat situation in such a way as to contain, or negate, the perceived risk to protected systems with minimal impact to the normal function of those systems. The approach that will be used consists of a five-phase model:

1) **Monitoring** – The collection and analysis of network and host data (in-band data), listserv notices, vendor alerts, Internet Storm Center reports, GIAC postings, etc. (out-of-band data).
2) **Alerting** – Through the assessment of gathered data a determination is made that one, or more, potential threats to protected systems are present, or imminent, in the environment. An IDS expert system or an intrusion detection analyst may generate alerts.
3) **Analysis** – A determination of what specific points of entry, system vulnerabilities, exploit methods are most likely to be used to compromise protected systems at the current threat level.
4) **Planning** – Developing a response that minimizes the target cross-section, and ideally neutralizes the perceived threat, while having the least impact on normal system operations.

---

3 Wayne W. Zachary, Joan M. Ryder, and James H. Hicinbothom, COGNITIVE TASK ANALYSIS AND MODELING OF DECISION MAKING IN COMPLEX ENVIRONMENTS, Lower Gwynedd, 1999
http://www.manningaffordability.com/S&tweb/PUBS/CHI_TADMUS/CHI_TADMUS_CHAPTER.htm

5) **Response** – Implementation of the planned response. This will be aided by the observation of the impact to the protected systems and the effectiveness of the risk reduction measures. General categories of response might be:

   a. Take action against the intruder

   b. Amend the environment

   c. Collect more information[4]

Nimda, A Day in the Life of a Worm

(the worm reference is to Nimda, comments from the peanut gallery notwithstanding…)

Phase 1 – Monitoring

The sun rises, the coffee perks, and all is well with the network. The normal morning routine of digesting the SHADOW and SNORT logs, Firewall logs, assorted amulets, and the ever-present crystal ball shows nothing more disturbing that good ole CodeRedX and RPC probes. All are Condition Green and present only outside the firewall. Bandwidth usage is within 1 standard deviation of the mean for the time of day, all systems show green on the board, connections to our business partners are up and passing data. In-band data tells me that life is good.

I open the priority e-mail in my inbox. The usual mix of vendor alerts, security bulletins, and listserv postings. One posting that I notice is from Russ Cooper at TruSecure/NTBugTraq. In his posting Russ expresses concern regarding a new worm[5] that appears to be making the rounds. This little guy apparently can be pulled in from an infected web server by a client browser. Needless to say, this causes me some concern, as my users do make use of IE to browse the web. Russ promises to keep us posted as he obtains more information.

Being in the CDT time zone, I actually finish the first of many cups of coffee for the day before the phone rings. It is a call from my ISP's net admin asking if I have any information on a new worm/virus that may be actively making the rounds. I forward a copy of Russ's email and open a tcpdump session on one of my probes looking at port 80 traffic to my clients. Phone call number two is from a net admin at one of our sister companies, bad, evil things are infesting their servers, and do I have any idea what they might be? Again, I forward the email and initiate a web search from my secure box to find any new information.

---

[4] Bace, Rebecca Gurley, Intrusion Detection
Macmillan Technical Publishing, 2000, 5.2.1 Active Responses

[5] "worms are automated probes that identify and exploit vulnerable systems, exponentially replicating themselves. "
Lance Spitzner, Know Your Enemy, Worms at War,
URL: http://project.honeynet.org/papers/worm/ , 2000

Phase 2 – Alerting

Many of us think of correlation as an after-the-fact, flesh-out-the-data type of activity. And, while that is one aspect of correlation, this sequence of events just tripped my Distant Early Warning system. An email from a respected source, two frantic sightings close to home,….. " It waddles like a duck, it quacks like a duck…" [6]. I'm not waiting until there are duck droppings on my hat to call this a duck.

Alert conditions –

- Red – Penetration of secure perimeter. System and/or data compromised, or functionally impacted.
- Yellow – Active, or directed, threat to protected systems. No detectable breach has occurred.
- Green – No directed threats detected, all defenses operational. Systems nominal.

We just went to Condition Yellow status, high probability of threat to systems. This issue is now priority, until it is resolved.

Phase 3 – Analysis

I receive a new email from the NTBugTraq list, an update on the new worm. Not looking good. Russ has a sample and it is looks like a mean one - forks for different operating systems, multiple methods of infection, etc. A call to our sister operation turns up a high rate of propagation once it gets in. No antiviral vendors have word out yet. What we know so far:

- It can be downloaded through a client browsing an infected web page
- Transmission occurs through shares, Code Red Trojans, and IIS vulnerabilities
- Email transmission is likely
- It eats Windows systems for lunch

This should be enough data for a severity assessment.[7]

- Criticality is penciled in at **4**, this puppy seems to move around inside of a network once it gets in.
- Lethality, make that a **5**, if it can jump shares, user access is the least that it has.
- Network Countermeasures… we'll call that **2**. We allow web access from workstations; however, we block all active attachments through our Email server.

---

[6] Northcutt, et al., Intrusion Signatures and Analysis.
New Riders Publishing, 2001, The Duck Principle, Page 29

[7] Network Intrusion Detection, An Analyst's Handbook *2e*, ibid, Calculating Severity, Page 153

- System Countermeasures, a **1**, we use Win NT and Outlook, and there is no evidence that our AV solution can handle this worm.

((4+5)-(2+1))=6. A 6 is about like cholera for us. We are an e-commerce firm. Time to go to plan B. Just wish that I knew what plan B was. And, that takes us to…

Phase 4 – Planning

Planning consists of listing the known data, implied data, and possible responses. Assessing the cost/benefit of each, and making an informed judgment call. OK, so what do we know at the moment?

1) We have a bug with a Severity rating of 6
2) We have verified that our web servers are patched to current level and that they are uninfected
3) No sign that the worm is present in our system
4) Our Exchange Server blocks all active attachments
5) Internet browsing remains an avenue of infection
6) Internet browsing is not critical to our operations

Conferring with our CIO, we agree that terminating outgoing requests and incoming datastreams on ports 80 and 443 is an acceptable risk reduction measure that will close one known avenue of infection, at least until we receive an update for our AV solution that we can test in our lab. We will keep one stand-alone box online, with a modem dialed in to our ISP, to research updates. Our regular email service should be allowed to continue without any additional measures. Batten the hatches, but keep sailing. We feel we can weather this one.

Phase 5 – Response

Adjustments are made to our firewalls and router ACLs to close down http/https requests from internal clients. Connectivity is tested at various points to insure that there are no unexpected side-effects. Business operations continue. The servers, HTTP and FTP, are monitored closely for any aberrant activity. Nimda, as we learn the worm is named, comes knocking on our IDS door. SNORT shows IIS traversals and .ida alerts. SHADOW confirms the level of activity on affected ports, including tftp. Two of our business partners are offline for the duration. Cleanup is apparently a slow, painful process. I continue passing along updates to anyone that has requested data.

Once the signature is determined, we update SNORT to gather more detailed data the worm's activity. We have obtained a sample from one of the infected machines at our sister company. When we receive an update from our AV vendor, we deploy the patch in our lab. It does indeed catch and kill the current variant. A plan is made to deploy the update, and open outgoing web connectivity, on a machine-by-machine basis the next morning.

Current Severity Assessment

- Criticality **4**
- Lethality **5**
- Network Countermeasures **5**, after the firewall ports are reopened we will call it **3**
- System Countermeasures (no browser access) **4**, after patch it will be **4** with browser access

((4+5)-(5+4))=0, down from a 6. I can at least feel that we are holding until morning.

((4+5)-(3+4))=2, not ideal. It means that we keep an eye out for AV updates and any unusual activity within our system. Approval already exists to cut the HTTP filters back in if any unusual activity is detected.

Distant Early Warning – Out-of-band data

As you can see from the above scenario, intrusion detection has increased effectiveness when you extend your "sensor horizon" with out-of-band data. Had we waited until our IDS detected the presence of the worm, and possibly from within our network, it may well have been very costly for our business unit. Had we not monitored the information sources available to us during the incident, we might not have been able to restore web connectivity at the earliest possible time, decreasing unit productivity.

Intelligence gathering that can be performed on an ongoing basis can aid the analyst in assessing, and in reacting to, the ever-changing threat landscape. These "First-strike" whiskers come in many forms, some of which are:

- SANS GIAC, NTBugTraq, Internet Storm Center, and other lists
- Vendor Alerts – Symantec, NAI
- Security Organizations – Infragard, MIS, SANS
- Security Subscription services – Trusecure, Versign, ISS, CA
- Your peers in the Intrusion Detection community
- The ever growing Body of Knowledge in the Intrusion Detection community[8]

The further out that your window-of-detection extends, the more time you will have to prepare, and update, contingency plans as things develop. Strategic planning help to put in place the tools that we will need to fight the individual battles. The firewalls, router ACLs, IDS nodes, system logs, etc. Tactical response is about making the best use of those tools. Keeping your knowledge level current, records updated, and your lines of communication open.

Intrusion detection is the synthesis of alerts, logs, news, and your own perception and judgment. When that web server shows a traffic load that just doesn't "feel right", when a client calls to complain about "slow response" on your website, when you read about a new worm or virus surfacing

[8] Some examples:
http://www.sans.org/infosecFAQ/index.htm
http://www.whitehats.com
http://www.sans.org/giac.htm

on the net, your whiskers should twitch just like when you see that SYN-FIN packet hit your IDS box. As so many have said, "real-time" response just isn't a practical reality in intrusion detection. But, "in-time" response is possible when have enough warning.

"Know Your Enemy, Know Yourself" – Being Prepared

If you know the enemy and know yourself,
You need not fear the outcome of a hundred battles.
If you know yourself but not the enemy,
For every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself,
You will succumb in every battle.
Sun Tzu, The Art of War

Sun Tzu's advice regarding intelligence and preparedness apply very well to intrusion detection. Knowledge of the tools and exploits available, the virii and worms, the incidence of attacks, all serves to prepare you for what you may face. Knowledge of your network, IDS tools, security policies, will help to prepare you for how to respond.

Sure, the plethora of exploits and scripts, worms and virii, is growing daily. For every intrusion analyst there are probably several hundred people worldwide that would like to compromise your systems. But, you have one major advantage over your opponent. You control the firewalls through which his packets must pass. You set the ACLs on the router that deliver those packets to the hosts that he would compromise. You patch the OS and set the permissions that allow him to work.

Whether you opponent is a script-kiddie, an elite hacker, or an Internet worm, he is crossing your territory to accomplish his task. And, that should be territory that is more familiar to you than to your opponent. Deny him what intelligence you can. Use your intrusion detection system and logs to learn what he must reveal in order to pass your walls. And, most importantly, know well the arsenal at your disposal to respond when he does intrude. Possible tools include:

- **Firewall filters** – Have a good working knowledge of the granularity of the firewall filter language. It can be useful to have contingency rulesets prepared for quick upload depending on the threat.
- **Router ACL's** – Knowing the path traffic must take in your network, you can construct router scripts to contain various types of traffic within your network, or isolate critical pieces of infrastructure.
- **Host Services** – When you know the vulnerability being targeted, the detailed knowledge of which hosts are running what services can allow you to focus your efforts, and if necessary, to disable those services rapidly.
- **Intrusion Detection Systems** – These are your eyes and ears. Know how to tune them, and what they may be trying to tell you. Make them an active tool in your defense. Be able to focus their potential quickly upon need.

Of course, this is just a small list of the many possible tools available. And, whether or not any particular tool is ready to hand at the time, it is important that you know how to best use the tools that might be available. Practice constructing firewall and router rulesets. Build IDS filters for obscure and complex signature patterns. Exchange insights and ideas with other analysts, and on mailing lists.

Tactical response in intrusion detection is about integrating all the relevant data available to you at the time. It means making the best use of the tools that you have to reduce the risks to your systems.

-SMH

Glossary

CIRT - (Acronym) Computer Incident Response Team. Person(s) designated to respond to detected intrusion attempts.

Forensic analysis - Analysis of recorded data and affected systems to determine, after the fact, in what manner a system compromise occurred. Also referred to as post mortem, or after-action analysis.

In-band data - Data collected and analyzed through system logs, IDS alerts and logs, system monitors, etc. relating to traffic and interaction through a protected network

Out-of-band data - Data acquired from newsgroups, fellow analysts, system admin, users, listservs, etc. touching on any activity that may impact on protected systems, the Internet in general, World/National security, Business, etc.

Standard Deviation - The standard deviation of a collection of numbers is the square root of (the difference between the mean of the squares of the numbers and the square of the mean of the numbers). Used in statistical analysis, the standard deviation of a set of measurements represents the dispersion (spread) of the values around their mean (average) value.

Strategy - The art and science of developing and using political, economic, psychological, and military forces during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat. (Joint Chiefs of Staff, "Dictionary of Military and Associated Terms," *JCS Pub. 1*, Department of Defense, June 1, 1987.)

Strategic response - (As used in this paper) The assessment of data, and the associated planning, relating to systems and network operations defensive posture (e.g., Systems architecture decisions, firewall ruleset design, IDS deployment, etc.).

Tactical Warning - A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. (Joint Chiefs of Staff, "Dictionary of Military and Associated Terms," *JCS Pub. 1*, Department of Defense, June 1, 1987.)

Tactical response - (As used in this paper) The activity initiated by a CIRT intended to mitigate an ongoing, or imminent, attack on the system(s) being protected. This is distinct from an active response, or “counter-attack”, strategy (e.g., Shutting down server/services, tightening firewall rulesets, blocking hostile source addresses, etc.).

BIBLIOGRAPHY

Amoroso, Edward.
Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traceback, Traps, and Response
Intrusion.Net Books, 1999.

Nichols, Randall K.
Ryan, Daniel J.
Ryan, Julie J.C.H.
Defending Your Digital Assets,
McGraw Hill, 2000.

Northcutt, Stephen
Cooper, Mark
Fearnow, Matt
Fredrick, Karen
Intrusion Signatures and Analysis.
New Riders Publishing, 2001.

Skoudis, Ed.
Counter Hack, a Step-by-Step guide to Computer Attacks and Effective Defenses,
Prentice Hall, 2002

Bace, Rebecca Gurley.
Intrusion Detection,
Macmillan Technical Publishing, 2000.

Northcutt, Stephen
Novak, Judy.
Intrusion Detection, An Analysts Handbook, 2nd ed.,
New Riders Publishing, 2001.

Proctor, Paul E..
The Practical Intrusion Detection Handbook.
Prentice Hall, 2001.

Assignment 2 – Network Detects (40 points possible)

Detect 1 – LPRng scan followed by identd version probe

SNORT ALERT LOG

Sep 26 00:26:51 194.109.199.253:1471 -> X.Y.Z.225:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1472 -> X.Y.Z.226:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1494 -> X.Y.Z.248:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1500 -> X.Y.Z.254:515 SYN ******S*
09/26-00:28:29.626238 [**] [1:616:1] SCAN ident version [**] [Classification: Attempted Information Leak] [Priority: 3] {TCP} 194.109.199.253:2071 -> X.Y.Z.17:113 [Snort log]
09/26-00:30:29.375454 [**] [1:616:1] SCAN ident version [**] [Classification: Attempted Information Leak] [Priority: 3] {TCP} 194.109.199.253:2071 -> X.Y.Z.17:113 [Snort log]

```
[**] SCAN ident version [**]
09/26-00:28:29.626238 194.109.199.253:2071 -> X.Y.Z.17:113
TCP TTL:48 TOS:0x0 ID:42157 IpLen:20 DgmLen:48 DF
***AP**F Seq: 0x9C80A9AA  Ack: 0x4E27BA36  Win: 0x7FB8  TcpLen: 20
56 45 52 53 49 4F 4E 0A                          VERSION.

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

1. **Source of trace**

Sensor outside the DMZ Firewall. Time is CST. Offending host ID values not modified.

2. **Detect was generated by:**

SNORT v1.8 running on RH Linux v7.1 with current (09/01) ruleset. The rules that generated these detects were:

-TCP portscan settings of 5 addresses in 5 seconds for the port 515 catch.

SCAN ident version
[arachNIDS:303]
Rules with message "SCAN ident version":
alert tcp $EXTERNAL_NET any -> $HOME_NET 113 (msg:"SCAN ident version"; flags: A+;

content: "VERSION|0A|"; depth: 16;reference:arachnids,303; classtype:attempted-recon; sid:616; rev:1;) (from *scan.rules*)

3. Probability the source address was spoofed

LOW to Negligible - The scan on Port 515 was followed by an attempted connection on tcp port 113 on the LaBrea box. The same source address appears in both cases. Since the 3-way TCP handshake was completed in at least one case of identd probing, it would appear most unlikely that the source address was spoofed. The following WHOIS indicates that this attempt is from the Netherlands.

Server used for this query: [whois.ripe.net]
Query: [194.109.199.253]

```
inetnum:      194.109.196.0 - 194.109.199.255
netname:      XS4ALL-ADSL
descr:        XS4ALL Internet BV
descr:        ADSL Static IP numbers
country:      NL
admin-c:      CB127
admin-c:      OD45
tech-c:       OD45
tech-c:       CB127
status:       ASSIGNED PA
notify:       netmaster@xs4all.nl
mnt-by:       XS4ALL-MNT
changed:      oliver@xs4all.nl 20000501
source:       RIPE

route:        194.109.0.0/16
descr:        XS4ALL Networking
origin:       AS3265
notify:       as-guardian@xs4all.nl
mnt-by:       XS4ALL-MNT
changed:      cor@xs4all.nl 19960519
source:       RIPE
```

4. Description of attack:

This was an attempt to locate an open server on TCP Port 515 (spooler). If successful, a remote user may be able to execute arbitrary code with elevated privileges. In addition, the printing service may be disrupted or disabled entirely. This was followed by a successful connection to TCP port 113 (authentication) on the LaBrea box. The speed of connection argues scripting. The failure to attempt connection addresses 85, 96, 238 may well be caused by LaBrea “holding” a connection open. This would indicate a single threaded application, most likely the retries, which occurred over a 20-minute span, caused the user to abort.

5. Attack mechanism:

"LPRng, now being packaged in several open-source operating system distributions, has a missing format string argument in at least two calls to the syslog() function.

Missing format strings in function calls allow user-supplied arguments to be passed to a susceptible *snprintf() function call. Remote users with access to the printer port (port 515/tcp) may be able to pass format-string parameters that can overwrite arbitrary addresses in the printing service's address space. Such overwriting can cause segmentation violations leading to denial of printing services or to the execution of arbitrary code injected through other means into the memory segments of the printer service. "

From: http://www.cert.org/advisories/CA-2000-22.html - CERT® Advisory CA-2000-22 Input Validation Problems in LPRng

---

I believe that the subject was most likely trying to collect data through IDENTD version query. Though this could well be reconnaissance for an attack on a vulnerable version of identd. However, certain vulnerabilities do exist in identd.

6. Correlation:

SHADOW LOGS from a sensor on the same segment: (Highlighted portions indicate conversation with the LaBrea box.)

Blue – 515 probe

Green – 515 answered with SYN-ACK handshake

Violet – Identd Probe

```
00:26:57.403702 < agitogroup-rotterdam1.xs4all.nl.1260 > X.Y.Z.17.printer: S
2614468883:2614468883(0) win 32120  (DF)
00:26:57.403748 < X.Y.Z.17.printer > agitogroup-rotterdam1.xs4all.nl.1260: S
2759185426:2759185426(0) ack 2614468884 win 5
00:26:57.427131 < agitogroup-rotterdam1.xs4all.nl.1329 > X.Y.Z.85.printer: S
2617795507:2617795507(0) win 32120  (DF)
00:26:57.427180 < X.Y.Z.85.printer > agitogroup-rotterdam1.xs4all.nl.1329: S
376851798:376851798(0) ack 2617795508 win 5
00:26:57.430572 < agitogroup-rotterdam1.xs4all.nl.1342 > X.Y.Z.96.printer: S
2614581593:2614581593(0) win 32120  (DF)
00:26:57.430621 < X.Y.Z.96.printer > agitogroup-rotterdam1.xs4all.nl.1342: S
2771583059:2771583059(0) ack 2614581594 win 5
00:26:57.453715 < agitogroup-rotterdam1.xs4all.nl.1409 >
zbc108.dbltpa.com.printer: S 2622925031:2622925031(0) win 32120  (DF)
```

```
00:26:57.453762 < zbc108.dbltpa.com.printer > agitogroup-
rotterdam1.xs4all.nl.1409: S 2923620627:2923620627(0) ack 2622925032 win 5
00:26:57.470060 < agitogroup-rotterdam1.xs4all.nl.1458 >
test.realec.com.printer: S 2624602170:2624602170(0) win 32120  (DF)
00:26:57.474155 < agitogroup-rotterdam1.xs4all.nl.1465 > X.Y.Z.219.printer: S
2611164210:2611164210(0) win 32120  (DF)
00:26:57.476818 < agitogroup-rotterdam1.xs4all.nl.1466 > X.Y.Z.220.printer: S
2618105630:2618105630(0) win 32120  (DF)
00:26:57.480381 < agitogroup-rotterdam1.xs4all.nl.1467 > X.Y.Z.221.printer: S
2617281491:2617281491(0) win 32120  (DF)
00:26:57.483494 < agitogroup-rotterdam1.xs4all.nl.1474 > X.Y.Z.228.printer: S
2610374507:2610374507(0) win 32120  (DF)
00:26:57.486648 < agitogroup-rotterdam1.xs4all.nl.1484 > X.Y.Z.238.printer: S
2623562868:2623562868(0) win 32120  (DF)
00:26:57.486695 < X.Y.Z.238.printer > agitogroup-rotterdam1.xs4all.nl.1484: S
568129853:568129853(0) ack 2623562869 win 5
00:26:57.490417 < agitogroup-rotterdam1.xs4all.nl.1494 > X.Y.Z.248.printer: S
2626043081:2626043081(0) win 32120  (DF)
00:26:58.334383 < agitogroup-rotterdam1.xs4all.nl.1260 > X.Y.Z.17.printer: .
2614468884:2614468884(0) ack 2759185427 win 32120 (DF)
00:26:58.344664 < agitogroup-rotterdam1.xs4all.nl.1329 > X.Y.Z.85.printer: .
2617795508:2617795508(0) ack 376851799 win 32120 (DF)
00:26:58.348104 < agitogroup-rotterdam1.xs4all.nl.1342 > X.Y.Z.96.printer: .
2614581594:2614581594(0) ack 2771583060 win 32120 (DF)
00:26:58.353675 < agitogroup-rotterdam1.xs4all.nl.1409 >
zbc108.dbltpa.com.printer: . 2622925032:2622925032(0) ack 2923620628 win
32120 (DF)
00:26:58.358303 < agitogroup-rotterdam1.xs4all.nl.1484 > X.Y.Z.238.printer: .
2623562869:2623562869(0) ack 568129854 win 32120 (DF)
00:26:58.663674 < agitogroup-rotterdam1.xs4all.nl.2071 > X.Y.Z.17.auth: S
2625677737:2625677737(0) win 32120  (DF)
00:26:58.663722 < X.Y.Z.17.auth > agitogroup-rotterdam1.xs4all.nl.2071: S
1311226421:1311226421(0) ack 2625677738 win 5
00:26:58.816211 < agitogroup-rotterdam1.xs4all.nl.2071 > X.Y.Z.17.auth: .
2625677738:2625677738(0) ack 1311226422 win 32120 (DF)
00:26:58.819653 < agitogroup-rotterdam1.xs4all.nl.2071 > X.Y.Z.17.auth: P
2625677738:2625677743(5) ack 1311226422 win 32696 (DF)
```

Potential IDENTD Vulnerabilities

CVE-1999-0746	A default configuration of in.identd in SuSE Linux waits 120 seconds between requests, allowing a remote attacker to conduct a denial of service.
CVE-2000-0369	The IDENT server in Caldera Linux 2.3 creates multiple threads for each IDENT request, which allows remote attackers to cause a denial of service.
CVE-2000-1107	in.identd ident server in SuSE Linux 6.x and 7.0 allows remote attackers to cause a denial of service via a long request, which causes the server to access a NULL pointer and crash.
CVE-	Format string vulnerability in stunnel 3.8 and earlier allows

2001-0060	attackers to execute arbitrary commands via a malformed ident username.
CVE-2001-0196	inetd ident server in FreeBSD 4.x and earlier does not properly set group permissions, which allows remote attackers to read the first 16 bytes of files that are accessible by the wheel group.
CAN-1999-0629	** CANDIDATE (under review) ** The ident/identd service is running.
CAN-1999-1176	** CANDIDATE (under review) ** Buffer overflow in cidentd ident daemon allows local users to gain root privileges via a long line in the .authlie script.
CAN-2001-0609	** CANDIDATE (under review) ** Format string vulnerability in Infodrom cfingerd 1.4.3 and earlier allows a remote attacker to gain additional privileges via a malformed ident reply that is passed to the syslog function.

7. Evidence of active targeting:

Active targeting is unlikely on the LPRng scan. The attacker does appear to be trying different methods of access. It is likely that the response on the earlier 515 attempts was the driver in selecting the addresses for the identd probe.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(4 + 4) - (5 + 5) = - 2

System criticality: **4** – All exposed systems are production servers on the Net. However, no Core servers are on this subnet.

Attack lethality: **4** - The goal is to probably create a buffer overflow to gain access

System Countermeasures: **5** – No vulnerable services are running on the servers on this subnet.

Network Countermeasures: **5** – Restrictive firewall prevented traffic from passing into DMZ.

9. Defensive recommendation:

System defense is adequate. All systems are behind a restrictive firewall. Additionally, all production systems are Windows–based. The attack was successfully blocked by the firewall.

10. Write a question that is based on the trace and your analysis with your answer.

```
Sep 26 00:26:51 194.109.199.253:1471 -> X.Y.Z.225:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1472 -> X.Y.Z.226:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1494 -> X.Y.Z.248:515 SYN ******S*
Sep 26 00:26:51 194.109.199.253:1500 -> X.Y.Z.254:515 SYN ******S*
```

Using the above trace, what is the service most likely being probed for?

a) Windows print spooler service
b) Linux LPRng print spooler service
c) SUN OS print spooler service
d) Windows SMB service

Answer: b

Detect 2 – RPC statd

SNORT ALERT LOG

```
Sep 26 03:35:32 202.159.99.135:2973 -> X.Y.Z.92:111 SYN ******S*
Sep 26 03:35:39 202.159.99.135:955 -> X.Y.Z.92:111 UDP
09/26-03:35:39.893768 [**] [1:583:1] RPC portmap request rstatd [**] [Classification: Attempted Information Leak] [Priority: 3] {UDP} 202.159.99.135:955 -> X.Y.Z.92:111
```

[Snort log]

09/26-03:35:44.905001 [**] [1:583:1] RPC portmap request rstatd [**] [Classification: Attempted Information Leak] [Priority: 3] {UDP} 202.159.99.135:955 -> X.Y.Z.92:111 [Snort log]
Sep 26 03:35:49 202.159.99.135:955 -> X.Y.Z.92:111 UDP
09/26-03:35:49.914103 [**] [1:583:1] RPC portmap request rstatd [**] [Classification: Attempted Information Leak] [Priority: 3] {UDP} 202.159.99.135:955 -> X.Y.Z.92:111 [Snort log]

```
[**] RPC portmap request rstatd [**]
09/26-03:35:39.893768 202.159.99.135:955 -> X.Y.Z.92:111
UDP TTL:48 TOS:0x0 ID:7602 IpLen:20 DgmLen:84
Len: 64
33 4E 8E E2 00 00 00 00 00 00 00 02 00 01 86 A0  3N..............
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01  ................
00 00 00 11 00 00 00 00                          ........

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

1. Source of trace

Sensors outside the DMZ Firewall. Time is CST. Offending host ID values not modified.

2. Detect was generated by:

SNORT v1.8 running on RH Linux v7.1 with current (09/01) ruleset. The rules that generated these detects were:

RPC portmap request rstatd	6 sources	7 destinations
[arachNIDS:10]		
Rules with message "RPC portmap request rstatd":		
alert udp $EXTERNAL_NET any -> $HOME_NET 111 (msg:"RPC portmap request rstatd"; content: "|01 86 A0 00 00|"; reference:arachnids,10;classtype:attempted-recon; sid:583; rev:1;) (from *rpc.rules*)		
alert tcp $EXTERNAL_NET any -> $HOME_NET 111 (msg:"RPC portmap request rstatd"; content: "|01 86 A0 00 00|"; reference:arachnids,10;classtype:attempted-recon; flags:A+; sid:1270; rev:1;) (from *rpc.rules*)		

3. Probability the source address was spoofed

Unlikely to LOW – The scan was UDP scan was followed by a TCP RPC statd request. This would only be useful if the data were retrieved by the host. Additionally the 3-way TCP handshake was completed. Source is indicated to be in Indonesia, and appears to

be a nameserver. Most likely the host is compromised. Possible cache poisoning, or farmed DNS servers, would seem to be indicated by the two nslookup responses.

nslookup 202.159.99.135

Canonical name: ns1.starko.co.id

Addresses:

202.159.99.135

Recursive queries supported by this server

Query for ns1.starko.co.id type=255 class=1

ns1.starko.co.id A (Address) 202.149.129.246

Dig ns1.starko.co.id@ns1.starko.co.id (202.149.129.246) ...

Authoritative Answer

Server used for this query: [whois.apnic.net]
Query: [202.159.99.135]

```
% Rights restricted by copyright. See
http://www.apnic.net/db/dbcopyright.html
% (whois7.apnic.net)

inetnum:      202.159.96.0 - 202.159.99.255
netname:      SIGNET-INDONET-ID
descr:        PT. Sigma Pratama
country:      ID
admin-c:      RN39-AP
tech-c:       RN39-AP
mnt-by:       MAINT-INDONET-ID
changed:      ratmin@indo.net.id 20010613
source:       APNIC

person:       Rhadmin Nasution
address:      Grha Citra Caraka Lt.M
address:      Jl. jend. Gatot Subroto Kav 52
address:      Jakarta 12710
country:      ID
phone:        +62-21-5268164
fax-no:       +62-21-5271850
e-mail:       ratmin@indo.net.id
nic-hdl:      RN39-AP
mnt-by:       MAINT-INDONET-ID
changed:      ratmin@indo.net.id 20010307
source:       APNIC
```

3. **Description of attack:**
   This was listed in the:

SANS - How To Eliminate The Ten Most Critical Internet Security Threats

Threat #3 - Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely-used to access network services such as shared files in NFS. Multiple vulnerabilities caused by flaws in RPC, are being actively exploited. There is compelling evidence that the vast majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems.

http://www.sans.org/infosecFAQ/threats/development.htm
CVE-1999-0018, CVE-1999-0019

Analysis of packet:

```
[**] RPC portmap request rstatd [**]
09/26-03:35:39.893768 202.159.99.135:955 -> X.Y.Z.92:111
UDP TTL:48 TOS:0x0 ID:7602 IpLen:20 DgmLen:84
Len: 64
33 4E 8E E2 00 00 00 00 00 00 00 02 00 01 86 A0  3N..............
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01  ................
00 00 00 11 00 00 00 00                          ........
```

The data portion of the packet shows the following:

Transaction ID = 0

Message Type = CALL

RPC Version = 0

RPC Program = STATUS

Program Version = 1

Procedure Number = 17

Authentication = 0

4. Attack mechanism:

Although Vulnerabilities exist in abundance for portmapper, this would appear to be a probe to retrieve data from RPCinfo by using a status call. The speed of connections, and the incidence of TCP sequence numbers and source ports, argues for an automated process of at least 3 threads.

5. Correlation:

SHADOW LOGS from a sensor on the same segment:

UDP Portmapper probe

```
03:37:19.623343 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:24.634717 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:29.643963 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:34.653046 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
```

TCP Portmapper attempt

```
03:37:13.367058 < ns1.starko.co.id.2954 > X.Y.Z.73.sunrpc: .
3567285495:3567285495(0) ack 2463589704 win 1460 (DF)
03:37:13.585800 < ns1.starko.co.id.2957 > X.Y.Z.76.sunrpc: .
3557054307:3557054307(0) ack 142970471 win 1460 (DF)
03:37:13.612215 < ns1.starko.co.id.2958 > X.Y.Z.77.sunrpc: .
3567276734:3567276734(0) ack 3121275651 win 1460 (DF)
03:37:13.612336 < ns1.starko.co.id.2959 > X.Y.Z.78.sunrpc: .
3565457217:3565457217(0) ack 475152426 win 1460 (DF)
03:37:13.612339 < ns1.starko.co.id.2960 > X.Y.Z.79.sunrpc: .
3555311030:3555311030(0) ack 2592544801 win 1460 (DF)
03:37:13.617741 < ns1.starko.co.id.2966 > X.Y.Z.85.sunrpc: .
3552465940:3552465940(0) ack 3900666965 win 1460 (DF)
03:37:13.621182 < ns1.starko.co.id.2968 > X.Y.Z.87.sunrpc: .
3562252926:3562252926(0) ack 3916868388 win 1460 (DF)
03:37:13.625318 < ns1.starko.co.id.2972 > X.Y.Z.91.sunrpc: .
3554427435:3554427435(0) ack 2649615911 win 1460 (DF)
03:37:13.629579 < ns1.starko.co.id.2973 > X.Y.Z.92.sunrpc: .
3566238577:3566238577(0) ack 2940621434 win 1460 (DF)
03:37:13.632528 < ns1.starko.co.id.2974 > X.Y.Z.93.sunrpc: .
3553038299:3553038299(0) ack 1503976244 win 1460 (DF)
```

TCP SYN Handshake Completed

```
03:37:12.695785 < ns1.starko.co.id.2973 > X.Y.Z.92.sunrpc: S
3566238576:3566238576(0) win 32120  (DF)
03:37:12.695834 < X.Y.Z.92.sunrpc > ns1.starko.co.id.2973: S
2940621433:2940621433(0) ack 3566238577 win 5
03:37:13.629579 < ns1.starko.co.id.2973 > X.Y.Z.92.sunrpc: .
3566238577:3566238577(0) ack 2940621434 win 1460 (DF)
```

7. Evidence of active targeting:

The main thrust was a scan of the X.Y.Z.0/24 subnet. The only follow-up occurred when a host responded to the probe.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(4 + 2) - (5 + 5) = - 4

System criticality: **4** – All exposed systems are production servers on the Net. However, no Core servers are on this subnet.

Attack lethality: **2** - The goal is most likely to obtain further data from hosts

System countermeasures: **5** – No vulnerable services are running on the servers on this subnet.

Network Countermeasures: **5** – Restrictive firewall prevented traffic from passing into DMZ.

9. Defensive recommendation:

System defense is adequate. All systems are behind a restrictive firewall. Additionally, all production systems are Windows–based. The attack was successfully blocked by the firewall.

10. Write a question that is based on the trace and your analysis with your answer.

```
03:37:19.623343 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:24.634717 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:29.643963 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
03:37:34.653046 < ns1.starko.co.id.955 > X.Y.Z.92.sunrpc: udp 56
```

In the above trace, what port is being targeted?

a) tcp 111
b) udp 515
c) udp 111
d) tcp 445

Answer: c

Detect 3 – FTP Network Scan

SNORT ALERT LOG

Sep 26 03:34:05 62.211.56.54:1994 -> X.Y.Z.2:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:1995 -> X.Y.Z.3:21 SYN ******S*

Sep 26 03:34:05 62.211.56.54:1996 -> X.Y.Z.7:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:1999 -> X.Y.Z.14:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:2000 -> X.Y.Z.15:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:2001 -> X.Y.Z.16:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:2002 -> X.Y.Z.17:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:2003 -> X.Y.Z.18:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:2004 -> X.Y.Z.19:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.51:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.52:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.57:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.63:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.64:21 SYN ******S*
Sep 26 03:34:05 62.211.56.54:21 -> X.Y.Z.65:21 SYN ******S*

1. Source of trace

Sensor outside the DMZ Firewall. Time is CST. Offending host ID values not modified.

2. Detect was generated by:

SNORT v1.8 running on RH Linux v7.1 with current (09/01) ruleset. The rules that generated these detects were:

-TCP portscan settings of 5 addresses in 5 seconds for the port 515 catch.

3. Probability the source address was spoofed

LOW to Negligible - Scan data would require return packet to verify socket open. Also, in correlation from SHADOW log, a Reset packet is fired off to hosts that respond with an ACK. This would indicate a valid connection.

```
% This is the RIPE Whois server.
% The objects are in RPSL format.

inetnum:        62.211.56.0 - 62.211.56.255
netname:        TIN
descr:          Telecom Italia Net
```

```
descr:          Telecom Italia Net ADSL Lite in OSPF Area 11
descr:          PROVIDER
country:        IT
admin-c:        TAS10-RIPE
tech-c:         TAS10-RIPE
status:         ASSIGNED PA
remarks:        Please send abuse notification to abuse@tin.it
notify:         nettin@tin.it
mnt-by:         TIN-MNT
changed:        nettin@tin.it 20010216
source:         RIPE
```

4. Description of attack:

Network scan for port 21 FTP command channel. Across X.Y.Z.0/24 subnet.

5. Attack mechanism:

Portscan to port 21 of machines in the X.Y.Z.0/24. Initially source ports incrementing from port 21 to destination port 21. The pattern is SYN -> , SYN ACK<- , RST -> from the attacker. The pattern alters to source port of 2000 to port 21, now with the ECN CWR bit set in the TCP flags for an interspersed probe of boxes that responded to a prior connection. The sped of new connections argues for automation, as does the second round with ECN bits. Most likely multi-threaded.

6. Correlation:

SHADOW Logs

```
03:35:45.347322 < 62.211.56.54.1994 > X.Y.Z.2.ftp: S [ECN-Echo,CWR]
2546297494:2546297494(0) win 5808  (DF)
03:35:45.347371 < X.Y.Z.2.ftp > 62.211.56.54.1994: S
1203549781:1203549781(0) ack 2546297495 win 5
03:35:45.354860 < 62.211.56.54.1995 > X.Y.Z.3.ftp: S [ECN-Echo,CWR]
2548300428:2548300428(0) win 5808  (DF)
03:35:45.354908 < X.Y.Z.3.ftp > 62.211.56.54.1995: S 41326445:41326445(0)
ack 2548300429 win 5
03:35:45.360099 < 62.211.56.54.ftp > X.Y.Z.77.ftp: S
1622892143:1622892143(0) win 32579
03:35:45.360147 < X.Y.Z.77.ftp > 62.211.56.54.ftp: S
1257419349:1257419349(0) ack 1622892144 win 5
03:35:45.370586 < 62.211.56.54.ftp > X.Y.Z.78.ftp: S
1622892143:1622892143(0) win 32579
03:35:45.370635 < X.Y.Z.78.ftp > 62.211.56.54.ftp: S
889912847:889912847(0) ack 1622892144 win 5
03:35:45.378617 < 62.211.56.54.1996 > X.Y.Z.7.ftp: S [ECN-Echo,CWR]
2548301382:2548301382(0) win 5808  (DF)
```

```
03:35:45.378663 < X.Y.Z.7.ftp > 62.211.56.54.1996: S
1862871808:1862871808(0) ack 2548301383 win 5
03:35:45.391927 < 62.211.56.54.ftp > X.Y.Z.79.ftp: S
1622892143:1622892143(0) win 32579
03:35:45.391976 < X.Y.Z.79.ftp > 62.211.56.54.ftp: S
3046184213:3046184213(0) ack 1622892144 win 5
03:35:45.436332 < 62.211.56.54.1999 > X.Y.Z.14.ftp: S [ECN-Echo,CWR]
2541977028:2541977028(0) win 5808  (DF)

03:35:44.470256 < 62.211.56.54.ftp > X.Y.Z.2.ftp: S 983279622:983279622(0)
win 52613
03:35:44.470301 < X.Y.Z.2.ftp > 62.211.56.54.ftp: S
2923620627:2923620627(0) ack 983279623 win 5
03:35:44.483527 < 62.211.56.54.ftp > X.Y.Z.3.ftp: S 983279622:983279622(0)
win 52613
03:35:44.483575 < X.Y.Z.3.ftp > 62.211.56.54.ftp: S 568129853:568129853(0)
ack 983279623 win 5
03:35:44.522687 < 62.211.56.54.ftp > X.Y.Z.7.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.522733 < X.Y.Z.7.ftp > 62.211.56.54.ftp: S
1311226421:1311226421(0) ack 1622892144 win 5
03:35:44.590231 < 62.211.56.54.ftp > X.Y.Z.14.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.590280 < X.Y.Z.14.ftp > 62.211.56.54.ftp: S
408688740:408688740(0) ack 1622892144 win 5
03:35:44.603462 < 62.211.56.54.ftp > X.Y.Z.15.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.603508 < X.Y.Z.15.ftp > 62.211.56.54.ftp: S
1642401127:1642401127(0) ack 1622892144 win 5
03:35:44.608090 < 62.211.56.54.ftp > X.Y.Z.16.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.608139 < X.Y.Z.16.ftp > 62.211.56.54.ftp: S
3601212946:3601212946(0) ack 1622892144 win 5
03:35:44.622181 < 62.211.56.54.ftp > X.Y.Z.17.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.622230 < X.Y.Z.17.ftp > 62.211.56.54.ftp: S
1003241225:1003241225(0) ack 1622892144 win 5
03:35:44.627219 < 62.211.56.54.ftp > X.Y.Z.18.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.627266 < X.Y.Z.18.ftp > 62.211.56.54.ftp: S
2807162200:2807162200(0) ack 1622892144 win 5
03:35:44.639713 < 62.211.56.54.ftp > X.Y.Z.19.ftp: S
1622892143:1622892143(0) win 32579
03:35:44.639761 < X.Y.Z.19.ftp > 62.211.56.54.ftp: S
651241261:651241261(0) ack 1622892144 win 5
03:35:44.691939 < 62.211.56.54.ftp > X.Y.Z.2.ftp: R
983279623:983279623(0) win 0 (DF)
03:35:44.715533 < 62.211.56.54.ftp > X.Y.Z.3.ftp: R
983279623:983279623(0) win 0 (DF)
03:35:44.760098 < 62.211.56.54.ftp > X.Y.Z.7.ftp: R
1622892144:1622892144(0) win 0 (DF)
03:35:44.848779 < 62.211.56.54.ftp > X.Y.Z.14.ftp: R
1622892144:1622892144(0) win 0 (DF)
03:35:44.879541 < 62.211.56.54.ftp > X.Y.Z.15.ftp: R
1622892144:1622892144(0) win 0 (DF)
```

```
03:35:44.892855 < 62.211.56.54.ftp > X.Y.Z.16.ftp: R
1622892144:1622892144(0) win 0 (DF)
03:35:44.916734 < 62.211.56.54.ftp > X.Y.Z.17.ftp: R
1622892144:1622892144(0) win 0 (DF)
03:35:44.932177 < 62.211.56.54.ftp > X.Y.Z.18.ftp: R
1622892144:1622892144(0) win 0 (DF)
03:35:44.963266 < 62.211.56.54.ftp > X.Y.Z.19.ftp: R
1622892144:1622892144(0) win 0 (DF)
```

7. Evidence of active targeting:

There is no evidence of active targeting. The attacker is probing for boxes that will answer on TCP port 21. The second probe may have been an attempt to elicit a response to the ECN CWR bit. Currently, I have only seen this bit set on Windows 2000 server TCP packets. It could be Queso/NMAP in a fingerprinting attempt. This article from SANS discusses the issue. http://www.sans.org/y2k/ecn.htm

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(4 + 2) - (4 + 4) = - 2

System criticality: **4** – All exposed systems are production servers on the Net. However, no Core servers are on this subnet.

Attack lethality: **2** - The goal is most likely to obtain further data from hosts

System Countermeasures: **4** – Servers are hardened and patched to current.

Network Countermeasures: **4** – Restrictive firewall prevented extraneous traffic from passing into DMZ. Mapping data could not be prevented from serving ports. However, the LaBrea box should help invalidate the return data.

9. Defensive recommendation:

Defenses are adequate. A report should be filed regarding the scan, and the IP source added to the local watchlist in the event that a targeted effort is intended.

10. Write a question that is based on the trace and your analysis with your answer.

```
03:35:45.378617 < 62.211.56.54.1996 > X.Y.Z.7.ftp: S [ECN-Echo,CWR]
2548301382:2548301382(0) win 5808  (DF)
03:35:45.378663 < X.Y.Z.7.ftp > 62.211.56.54.1996: S
1862871808:1862871808(0) ack 2548301383 win 5
```

To test whether the [ECN-Echo, CWR] bits are set to 1, which would be the correct filter?

a) tcp[13] & 0xc0 = 192
b) tcp[13]&0xc0=2
c) ip[13]&0xc0=3
d) tcp[13] & 0xc0 = 1

Answer: a

Detect 4 – Nimda Worm

SNORT Alert Logs

```
09/25-19:06:42.677822  [**] [1:1256:1] WEB-IIS CodeRed v2
root.exe access [**] [Classification: Attempted Administrator
Privilege Gain] [Priority: 10] {TCP} 209.42.177.212:1342 ->
X.Y.Z.232:80
09/25-19:06:50.334307  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:1581 -> X.Y.Z.232:80
09/25-19:06:50.861218  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:1734 -> X.Y.Z.232:80
09/25-19:06:51.494752  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:1759 -> X.Y.Z.232:80
09/25-19:06:52.385884  [**] [1:1288:1] WEB-FRONTPAGE /_vti_bin/
access [**] [Classification: Potentially Bad Traffic] [Priority:
2] {TCP} 209.42.177.212:1787 -> X.Y.Z.232:80
09/25-19:06:56.558581  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:1827 -> X.Y.Z.232:80
09/25-19:06:57.195479  [**] [110:4:1] spp_unidecode: Invalid
Unicode String detected [**] {TCP} 209.42.177.212:2017 ->
X.Y.Z.232:80
09/25-19:06:57.717589  [**] [110:4:1] spp_unidecode: Invalid
Unicode String detected [**] {TCP} 209.42.177.212:2044 ->
X.Y.Z.232:80
09/25-19:06:58.521226  [**] [110:4:1] spp_unidecode: Invalid
Unicode String detected [**] {TCP} 209.42.177.212:2086 ->
X.Y.Z.232:80
```

```
09/25-19:07:02.428828  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:2118 -> X.Y.Z.232:80
09/25-19:07:06.415401  [**] [1:974:2] WEB-IIS .... access [**]
[Classification: Attempted Information Leak] [Priority: 3] {TCP}
209.42.177.212:2298 -> X.Y.Z.232:80
09/25-19:07:10.637577  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:2490 -> X.Y.Z.232:80
09/25-19:07:14.617595  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:2671 -> X.Y.Z.232:80
09/25-19:07:16.006802  [**] [1:1002:1] WEB-IIS cmd.exe access
[**] [Classification: Attempted User Privilege Gain] [Priority:
8] {TCP} 209.42.177.212:2867 -> X.Y.Z.232:80
09/25-19:07:19.854274  [**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8] {TCP}
209.42.177.212:2919 -> X.Y.Z.232:80
```

1. Source of trace

Sensor outside the DMZ Firewall. Time is CST. Offending host ID values not modified. Target is a production web server.

2. Detect was generated by:

SNORT v1.8 running on RH Linux v7.1 with current (09/01) ruleset. The rules that generated this detect were:

WEB-IIS CodeRed v2 root.exe access		
Rules with message "WEB-IIS CodeRed v2 root.exe access":		
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS CodeRed v2 root.exe access"; flags: A+; uricontent:"scripts/root.exe?"; nocase; classtype: attempted-admin; sid: 1256; rev: 1;) (from *web-iis.rules*)		

WEB-FRONTPAGE /_vti_bin/ access		
Rules with message "WEB-FRONTPAGE /_vti_bin/ access":		
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-FRONTPAGE /_vti_bin/ access";flags: A+; uricontent:"/_vti_bin/"; nocase; classtype:bad-unknown; sid:1288; rev:1;) (from *web-frontpage.rules*)		

spp_unidecode: Invalid Unicode String detected

WEB-IIS cmd.exe access		
Rules with message "WEB-IIS cmd.exe access":		
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS cmd.exe access"; flags: A+; content:"cmd.exe"; nocase; classtype:attempted-user; sid:1002; rev:1;) (from *web-iis.rules*)		

WEB-IIS .... access		
[BUGTRAQ:2218] [CVE:CAN-1999-0229]		
Rules with message "WEB-IIS .... access":		
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS ..\.. access";flags: A+; content:"|2e2e5c2e2e|"; reference:bugtraq,2218; reference:cve,CAN-1999-0229; classtype:attempted-recon; sid:974; rev:2;) (from *web-iis.rules*)		

2. Probability the source address was spoofed

LOW to Negligible - There is no indication this address was spoofed. The 3 way TCP handshake was completed, and the worm requires connectivity to replicate.

Server used for this query: [whois.arin.net]
Query: [209.42.177.212]

```
Voyager Online (NETBLK-VOYAGERONLINE-BLK1)
   401 Chestnut St, Suite 203
   Chattanooga, TN 37402
   US

   Netname: VOYAGERONLINE-BLK1
   Netblock: 209.42.128.0 - 209.42.191.255
   Maintainer: VGER

   Coordinator:
      Network Operations Center, Voyager Online  (VON-ARIN)  noc@VOL.COM
      (423) 209-2929

   Domain System inverse mapping provided by:

   NS.VOYAGERONLINE.NET               209.42.128.1
   NS2.VOYAGERONLINE.NET      209.42.128.22
```

```
ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 31-Jul-1998.
Database last updated on 27-Sep-2001 23:18:25 EDT.
```

4. Description of attack:

The worm modifies web documents (e.g., .htm, .html, and .asp files) and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names. The particular exploits seen here are attempts to utilize CodeRed compromised access and known IIS vulnerabilities.

5. Attack mechanism:

Intruders, if successful, can execute arbitrary commands within the LocalSystem security context on machines running the unpatched versions of IIS. In the case where a client is compromised, the worm will be run with the same privileges as the user who triggered it. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines.

6. Correlation:

http://vil.nai.com/vil/virusSummary.asp?virus_k=99209

"IIS spreading:

The worm uses backdoors on IIS servers such as the one CodeRed II installs. It scans random IP addresses for these backdoors. When a host is found to have one the worm instructs the machine to download the worm code (Admin.dll) from the host used for scanning. After this it executes the worm on the target machine this way infecting it.

" from: http://www.f-secure.com/v-descs/nimda.shtml

http://www.cert.org/advisories/CA-2001-26.html

http://www.incidents.org/react/nimda-update-sept27.pdf

NT 4.0 sp6a IIS 4 Logs

```
#Fields: time c-ip cs-method cs-uri-stem sc-status
```

```
00:06:20 209.42.177.212 GET /scripts/root.exe 404
00:06:25 209.42.177.212 GET /MSADC/root.exe 404
00:06:28 209.42.177.212 GET /c/winnt/system32/cmd.exe 404
00:06:28 209.42.177.212 GET /d/winnt/system32/cmd.exe 404
00:06:29 209.42.177.212 GET /scripts/..%5c../winnt/system32/cmd.exe 404
00:06:29 209.42.177.212 GET
/_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe 404
00:06:34 209.42.177.212 GET
/_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe 404
00:06:34 209.42.177.212 GET
/msadc/..%5c../..%5c../..%5c/..Á ../..Á ../..Á ../winnt/system32/cmd.exe 404
00:06:35 209.42.177.212 GET /scripts/..Á ../winnt/system32/cmd.exe 404
00:06:35 209.42.177.212 GET /scripts/winnt/system32/cmd.exe 404
00:06:40 209.42.177.212 GET /scripts/../../winnt/system32/cmd.exe 404
00:06:44 209.42.177.212 GET /scripts/..\../winnt/system32/cmd.exe 404
00:06:48 209.42.177.212 GET /scripts/..S5c../winnt/system32/cmd.exe 404
00:06:52 209.42.177.212 GET /scripts/..S5c../winnt/system32/cmd.exe 404
00:06:54 209.42.177.212 GET /scripts/..%5c../winnt/system32/cmd.exe 404
00:06:57 209.42.177.212 GET /scripts/..%2f../winnt/system32/cmd.exe 404
```

7. Evidence of active targeting:

This worm attacks by scanning for possible new host vulnerabilities. This would indicate that there is no direct intent to target any particular system.

8. Severity:

(System criticality + Attack lethality) - (Network countermeasures + System Countermeasures) = Severity

(4 + 4) - (5 + 3) = 1

System criticality: **5** – Web servers are opened to port 80/443

Attack lethality: **4** - Could result in a complete compromise

System Countermeasures: **5** - All patches applied

Network Countermeasures: **3** - Restrictive firewall and updated IDS

9. Defensive recommendation:

Compliance with “Section III. Solutions” of http://www.cert.org/advisories/CA-2001-26.html will remove the targeted vulerabilities. One additional recommended countermeasure is the use of a LaBrea box. The ‘tarpitting’, or forcing the connection to drop to a very low rate of exchange, causes the worm to expend cycles in a non-productive manner. A average 24 minute delay per unused host address was achieved with LaBrea, as shown here:

```
04:16:35.754424 < 00-10-b5-e6-1c-0b.bconnected.net.2282 > X.Y.Z.140.www: S
699103255:699103255(0) win 16384  (DF)
04:16:35.754471 < X.Y.Z.140.www > 00-10-b5-e6-1c-0b.bconnected.net.2282: S
3373585492:3373585492(0) ack 699103256 win 5
04:16:35.836305 < 00-10-b5-e6-1c-0b.bconnected.net.2282 > X.Y.Z.140.www: .
699103256:699103256(0) ack 3373585493 win 16616 (DF)
04:16:35.838107 < 00-10-b5-e6-1c-0b.bconnected.net.2282 > X.Y.Z.140.www: .
699103256:699103261(5) ack 3373585493 win 16616 (DF)

<snip>

04:39:16.327278 < 00-10-b5-e6-1c-0b.bconnected.net.3407 > X.Y.Z.140.www: .
815173391:815173396(5) ack 4046131302 win 16616 (DF)
04:39:28.331907 < 00-10-b5-e6-1c-0b.bconnected.net.3407 > X.Y.Z.140.www: .
815173391:815173396(5) ack 4046131302 win 16616 (DF)
04:39:52.367054 < 00-10-b5-e6-1c-0b.bconnected.net.3407 > X.Y.Z.140.www: .
815173391:815173396(5) ack 4046131302 win 16616 (DF)
04:40:40.434889 < 00-10-b5-e6-1c-0b.bconnected.net.3407 > X.Y.Z.140.www: .
815173391:815173396(5) ack 4046131302 win 16616 (DF)
```

Maintaining current security/OS patch levels, anti-viral updates, and NBAR filtering on internal routers, is highly recommended in the face of this, and similar threats. Other hosts on the network were protected by the restrictive firewall which prevented port 80 access.

10. Write a question that is based on the trace and your analysis with your answer.

```
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:06:20 209.42.177.212 GET /scripts/root.exe 404
00:06:25 209.42.177.212 GET /MSADC/root.exe 404
00:06:28 209.42.177.212 GET /c/winnt/system32/cmd.exe 404
```

Using the above log extract, what type of server is indicated by this format?

a) Apache Web Server
b) MS Internet Information Server
c) Tomcat Web Server
d) Netscape FastTrack Web server

Answer: b

Detect 5 – ACK Storm

```
          Observer Packet Capture
Packet 733:  00:02:16:AF:56:C0 -> 00:E0:1E:3E:54:7B
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 54.893 818s,  Diff. time: 0.002086
    Date:  Tue Jul 17 2001
IP,    ftp.server -> ftp.client
    Source IP:  ftp.server,  Destination IP:  ftp.client
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: F25Fh
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 126
    PROTOCOL: [6] TCP
    Header checksum: 05B7 (Good)
TCP  ACK,   [21] -> [16766]
    Source port: [21] ftp   Destination port: [16766]
    Sequence number: 18593068,   Acknowledgement: 90985374
    TCP header length: 05 (32 bit words),   Window: 7386
    TCP data length: 0,   Checksum: 3D5Ch (GOOD)
    Sequence number + TCP data length: 18593068
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------

Packet 734:  00:E0:1E:3E:54:7B -> 00:02:16:AF:56:C0
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.021 879s,  Diff. time: 0.128061
    Date:  Tue Jul 17 2001
IP,    ftp.client -> ftp.server
    Source IP:  ftp.client,  Destination IP:  ftp.server
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: CC20h
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 113
    PROTOCOL: [6] TCP
    Header checksum: 38F6 (Good)
TCP  ACK,   [16766] -> [21]
    Source port: [16766]    Destination port: [21] ftp
    Sequence number: 90985375,   Acknowledgement: 18593095
    TCP header length: 05 (32 bit words),   Window: 8685
    TCP data length: 0,   Checksum: 382Dh (GOOD)
    Sequence number + TCP data length: 90985375
FTP Section: 0 bytes
```

```
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------

Packet 735:  00:02:16:AF:56:C0 -> 00:E0:1E:3E:54:7B
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.023 886s,  Diff. time: 0.002007
    Date:  Tue Jul 17 2001
IP,    ftp.server -> ftp.client
    Source IP:  ftp.server,  Destination IP:  ftp.client
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: F45Fh
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 126
    PROTOCOL: [6] TCP
    Header checksum: 03B7 (Good)
TCP  ACK,   [21] -> [16766]
    Source port: [21] ftp   Destination port: [16766]
    Sequence number: 18593068,   Acknowledgement: 90985374
    TCP header length: 05 (32 bit words),   Window: 7386
    TCP data length: 0,   Checksum: 3D5Ch (GOOD)
    Sequence number + TCP data length: 18593068
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------

Packet 736:  00:E0:1E:3E:54:7B -> 00:02:16:AF:56:C0
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.146 726s,  Diff. time: 0.122840
    Date:  Tue Jul 17 2001
IP,    ftp.client -> ftp.server
    Source IP:  ftp.client,  Destination IP:  ftp.server
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: CD20h
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 113
    PROTOCOL: [6] TCP
    Header checksum: 37F6 (Good)
TCP  ACK,   [16766] -> [21]
    Source port: [16766]    Destination port: [21] ftp
    Sequence number: 90985375,   Acknowledgement: 18593095
    TCP header length: 05 (32 bit words),   Window: 8685
    TCP data length: 0,   Checksum: 382Dh (GOOD)
    Sequence number + TCP data length: 90985375
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
```

```
   ------------------------------------------------------------

Packet 737:  00:02:16:AF:56:C0 -> 00:E0:1E:3E:54:7B
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.148 720s,  Diff. time: 0.001994
    Date:  Tue Jul 17 2001
IP,    ftp.server -> ftp.client
    Source IP:  ftp.server,  Destination IP:  ftp.client
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: F55Fh
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 126
    PROTOCOL: [6] TCP
    Header checksum: 02B7 (Good)
TCP  ACK,   [21] -> [16766]
    Source port: [21] ftp   Destination port: [16766]
    Sequence number: 18593068,   Acknowledgement: 90985374
    TCP header length: 05 (32 bit words),   Window: 7386
    TCP data length: 0,   Checksum: 3D5Ch (GOOD)
    Sequence number + TCP data length: 18593068
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------

Packet 738:  00:E0:1E:3E:54:7B -> 00:02:16:AF:56:C0
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.275 606s,  Diff. time: 0.126886
    Date:  Tue Jul 17 2001
IP,    ftp.client -> ftp.server
    Source IP:  ftp.client,  Destination IP:  ftp.server
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: CE20h
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 113
    PROTOCOL: [6] TCP
    Header checksum: 36F6 (Good)
TCP  ACK,   [16766] -> [21]
    Source port: [16766]    Destination port: [21] ftp
    Sequence number: 90985375,   Acknowledgement: 18593095
    TCP header length: 05 (32 bit words),   Window: 8685
    TCP data length: 0,   Checksum: 382Dh (GOOD)
    Sequence number + TCP data length: 90985375
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------
```

```
Packet 739:  00:02:16:AF:56:C0 -> 00:E0:1E:3E:54:7B
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.277 672s,  Diff. time: 0.002066
    Date:  Tue Jul 17 2001
IP,    ftp.server -> ftp.client
    Source IP:  ftp.server,  Destination IP:  ftp.client
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: 0A60h
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 126
    PROTOCOL: [6] TCP
    Header checksum: EDB6 (Good)
TCP  ACK,   [21] -> [16766]
    Source port: [21] ftp   Destination port: [16766]
    Sequence number: 18593068,   Acknowledgement: 90985374
    TCP header length: 05 (32 bit words),   Window: 7386
    TCP data length: 0,   Checksum: 3D5Ch (GOOD)
    Sequence number + TCP data length: 18593068
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------

Packet 740:  00:E0:1E:3E:54:7B -> 00:02:16:AF:56:C0
    Network:  Ethernet
    Frame type:  802.3,  Frame size (including 4 bytes CRC):  64
    Time:  595h:54m 55.403 569s,  Diff. time: 0.125897
    Date:  Tue Jul 17 2001
IP,    ftp.client -> ftp.server
    Source IP:  ftp.client,  Destination IP:  ftp.server
    Version: 04,    IP header length: 05 (32 bit words)
    Service type:  0:  Precedence: 0, Delay: Norm, Throug: Norm, Reliab: Norm
    Total IP length: 40
    ID: CF20h
    Fragment flags: [10] - don't fragment - last fragment
    Fragment offset: 0
    Time to live: 113
    PROTOCOL: [6] TCP
    Header checksum: 35F6 (Good)
TCP  ACK,   [16766] -> [21]
    Source port: [16766]    Destination port: [21] ftp
    Sequence number: 90985375,   Acknowledgement: 18593095
    TCP header length: 05 (32 bit words),   Window: 8685
    TCP data length: 0,   Checksum: 382Dh (GOOD)
    Sequence number + TCP data length: 90985375
FTP Section: 0 bytes
    No FTP data sent with this packet
   ------------------------------------------------------------
   ------------------------------------------------------------
```

1. Source of trace

Network Instruments Observer v7 collecting filtered datastream on 100M Ethernet between WAN routers.

2. Detect was generated by:

MRTG indicated a flatline increased bandwidth usage of 3.5 standard deviations on a WAN link that is usually predicatble withtin 1 standard deviation. The client reported unusually long session timeouts. These justified protocol analysis time on the link.

3. Probability the source address was spoofed
None - The link is a private link across a VAN. The client verified host connectivity.

4. Description of attack:

ACK Storm
Acknowledgment Storm
On a TCP system every sender puts a serial number (A) to every packet send. A receiver confirms with sending an Acknowledgment packet containing the number of the next expected packet (A+1) and an own serial number (B). On number mismatch the receiver sends an ACK packet with the serial number (A) for retransmission. An ACK storm is described by lots of ACK packets from sender and receiver (sometimes up to 90% of all data load). It is most likely a symptom for an attack or an error situation alerting the sysop. http://home.t-online.de/home/boehmj/Glossar_A.html - ACK.

5. Attack mechanism:

Were this an attack the tools could be :

Juggernaut - (Simplex connection hijack - Allows the user to insert a command into a telnet-based TCP stream. A short ACK storm ensues until the connection is subsequently reset.)

http://beta.openphoto.net/mike/texts/Phrack50/P50-06.html

Hunt - (Normal active hijacking with the detection of the ACK storm)

http://www.securiteam.com/tools/Hunt__a_new_Hijacking_software.html

However, in this case it was an older version (3.1) of a Servu ftp server and a client passing through a proxy server.

6. Correlation:

Testing was initiated between the client and server networks by our network team with client cooperation. The situation was replicated while close monitoring was taking place. No instance of malicious activity was found.

7. Evidence of active targeting:

No active targeting was found. However, the instance was specific to two separate client networks that experienced this failure mode. No other instances were detected.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(4 + 4) - (2 + 3) = 3

System criticality: 4 – FTP server (line-of-business)
Attack lethality: 4 - Could result in a complete Denial of Service (DoS)
System countermeasures: 2 – FTP server code flaw existed in this version
Network Countermeasures: 3 - Restrictive firewall allowed ftp traffic as normal
However, bandwidth monitoring detected anomalous usage .

9. Defensive recommendation:

Upgrade ServU ftp server to latest release and test for failure mode. No occurrence of this failure was detected with new server software.

10. Write a question that is based on the trace and your analysis with your answer.

An ACK Storm my be caused by:

a) TCP/IP stack errors
b) Session Hijacking
c) Both a & b
d) None of the above

Answer: c

Assignment 3 - "Analyze This" Scenario (30 Points)

The following is an analysis based on the files:

Scans.010901	Alert.010901	Oos_Sep.1.2001
Scans.010902	Alert.010902	Oos_Sep.2.2001
Scans.010903	Alert.010903	Oos_Sep.3.2001
Scans.010904	Alert.010904	Oos_Sep.4.2001
Scans.010905	Alert.010905	Oos_Sep.5.2001

We have been asked to evaluate the data collected over the 5-day period from 1 Sept 2001 to 5 Sept 2001, inclusive. The log files were generated by Snort, an Intrusion Detection System (IDS), over these 5 days. This assessment is a brief overview of the issues seen as most prominent in these logs from an Information Systems security point-of-view. With additional in-depth analysis, the volume of data in these logs can provide useful insight into potential security and performance issue with the MY.NET network. Such analysis is recommended, but is beyond the scope of this report.

Recommendations for MY.NET

As you read this report, consider the following:

1. The large number of attempts by Internet worms indicates an exposure level that is quite high for any unpatched web server on MY.NET. Aggressive measures should be taken to identify and patch any web servers open to the internet to prevent introducing the worm into the MY.NET environment.
2. Any significant indicators of Trojan activity should be investigated. The large number of machines and connections create a very large target signature for intrusion attempts. A Trojan successfully introduced into the MY.NET environment could place many hosts at risk.
3. A high percentage of the alerts generated are related to Instant messaging and file-sharing utilities. If these utilities are to be permitted, it would be more effective to filter these alerts out of the ruleset to prevent the generation of excessive alerts for approved traffic.
4. If the users are to be permitted to run of file-sharing and Instant Messaging utilities, then user education, with regard to information systems security, should be considered a priority. These utilities offer an active conduit, through which malicious software can easily enter your network. Remediation at a systems level is often ineffective in these situations. However, raising the level of user security awareness is often most cost-effective when these the use of these utilities is involved.

A more thorough analysis of your network traffic, architecture and configuration would most likely reveal potential areas for increased efficiency and security, and is highly recommended.

MY.NET.98.190 is most likely compromised

Alerts over the 5-day period indicate a high incidence of port 27374 TCP traffic interacting with the **MY.NET.98.190** host address. This is most likely generated by a Trojan, Sub-Seven 2.1. Immediate attention should be given to the forensic analysis and remediation of this host. SubSeven is a remote control Trojan that was designed for Windows 9x systems. Consult: http://www.sans.org/infosecFAQ/malicious/subseven.htm for an excellent analysis of the SubSeven Trojan by Jamie Crapanzano. Additionally, an alert from the National Infrastructure protection center is available at: http://www.infragard.net/warnings/01_014.htm covering the increased threat level of SubSeven.

MY.NET.111.221 & MY.NET.111.142 may be compromised

This host has received a significant number of UDP packets with payload in excess of 4Kbytes on port 0. Neither the payload size, nor the port used is normally seen in traffic. **This traffic may indicate a covert tunnel.** Care should be taken to inspect the host 111.221 & 111.142 for possible compromise.

Detects over the 5 day period

The following table shows the top detects over the 5-day period. The cutoff was 2 orders of magnitude below the highest frequency detect. This does not imply that those detects that were lower in frequency are less of a risk to the systems targeted, only that relative frequency was chosen as the measure in this set.
Red - High potential threat level, hostile activity
Yellow – Warning threat level, reconnaissance activity

Detect	Day1	Day2	Day3	Day4	Day5	Total
WEB-MISC Attempt to execute cmd	79667	66521	65911	49350	44019	305468
IDS552/web-iis_IIS ISAPI Overflow ida nosize	70289	58251	57955	42941	38676	268112
ICMP Destination Unreachable (Communication Administratively Prohibited)	9989	7909	6198	4313	3902	32311
MISC Large UDP Packet	802	0	3571	1991	14260	20624
MISC traceroute	6360	5326	4079	2499	2189	20453
MISC source port 53 to <1024	4339	3834	3501	3339	4577	19590
CS WEBSERVER - external web traffic	5178	3151	2930	2410	1789	15458
INFO MSN IM Chat data	3320	3123	2584	2922	2904	14853
WEB-MISC prefix-get //	2716	2348	2643	2490	2061	12258
ICMP Echo Request Nmap or HPING2	1276	2001	1378	3107	3043	10805
INFO napster login	2846	1670	2054	1079	954	8603
Possible trojan server activity	3861	0	0	0	2188	6049
Watchlist 000220 IL-ISDNNET-990517	610	321	399	1110	2875	5315
ICMP Destination Unreachable (Network Unreachable)	1029	1525	876	720	556	4706

High port 65535 tcp - possible Red Worm - traffic	0	0	0	4256	0	4256
ICMP Destination Unreachable (Host Unreachable)	1103	1169	597	408	321	3598

Alert	Explanation
WEB-MISC Attempt to execute cmd	An attempt was made on port 80 to execute 'cmd.exe', a windows NT/2000 command shell prompt. This could, if successful, result in compromise of the host. Currently seen in profusion from variety of IIS worms on the Internet. Hosts serving port 80 traffic should be patched and verified. Reference: http://www.sans.org/infosecFAQ/threats/unicode.htm
IDS552/web-iis_IIS ISAPI Overflow ida nosize	This event indicates that a remote attacker has attempted to exploit a vulnerability in Microsoft IIS. An unchecked buffer in the Microsoft IIS Index Server ISAPI Extension could enable a remote intruder to gain SYSTEM access to the web server. Currently a common symptom of Code Red Worm/Nimda probes from infected hosts.
ICMP Destination Unreachable (Communication Administratively Prohibited)	A packet directed to hosts on MY.NET that indicates that the host is blocked by a router or firewall. When it appears in large clusters without outgoing traffic to the host address, it often indicates 'backscatter' or packets generated in response to a DOS attack on the victim host.
MISC Large UDP Packet	Data payload of Greater than 4Kbytes in a UDP packet. This is not always hostile. However, it is not usual to send large amounts of data via UDP due to the connectionless nature of the protocol. This may indicate an improperly configured host or application.
MISC traceroute	Traceroute is a utility for tracing the IP route from host to destination server by hops. This can be used to probe for internal network architecture, or verify connectivity issues. Not always an indication of hostile intent.
MISC source port 53 to <1024	DNS source port 53, for answering requests, utilizes the ephemeral destination port that the client used to send the request. The return of data to a port below 1024 may indictae attempted zone transfer, or potential exploit attempts.
CS WEBSERVER - external web traffic	CS Webserver apparently resides on the server MY.NET 100.165 at port 80. This rule was crafted to detect traffic from outside MY.NET accessing this server.
INFO MSN IM Chat data	This alert tracks the transfer of Instant messenger Chat data from the MSN Instant Messenger utility being run by a MY.NET client. The potential for hostile code being brought in through this channel can be significant.
WEB-MISC prefix-get //	A reconnaissance probe against a webserver. Servers should be configured and patched to disallow this instruction.
ICMP Echo Request Nmap or HPING2	An Echo request generated by the NMAP or HPING2 utility that is often used for reconnaissance probes of hosts or networks. CVE:CAN-1999-0523

INFO napster login	a Napster client is logging in to port 8888 of a server outside MY.NET. This will cause the client IP to be announced as a napster server for external access. A potential security violation if napster is not normally permitted on the MY.NET system.
Possible trojan server activity	Many known trojan horse applications have fixed communication ports. These are considered in this rule. While legitimate traffic may make use of these same ports, heavy, or consistent traffic, may well indicate the prescene of a trojan. (e.g., host MY.NET.98.190).
Watchlist 000220 IL-ISDNNET-990517	This alert indicates detection of traffic involving: Company Name: ISDNnet LTD Contact People: Tony Nitzan Address: 21 Yagia Kapain St. Park Daniv Kiryat Arie, Petach-Tikva 49130 This is considered a high-risk network from which many hostile attempts have originated. Any pattern of traffic involving this network should be viewed with suspicion.
ICMP Destination Unreachable (Network Unreachable)	A packet directed to hosts on MY.NET that indicates that the destination network is not accessible at this time. When it appears in large clusters without outgoing traffic to the host address, it often indicates 'backscatter' or packets generated in response to a DOS attack on the victim host. Otherwise it is not abnormal traffic.
High port 65535 tcp - possible Red Worm - traffic	This alert should be of concern, given the large incidence of Code Red traffic directed at MY.NET. This alert indicates that traffic on tcp port 65535 is present involving MY.NET hosts. This is often the result of a busy host or port address translation box. However, given the current environment, indicated hosts should be examinedfor possible infection by the Code Red Worm.
ICMP Destination Unreachable (Host Unreachable)	A packet directed to hosts on MY.NET that indicates that the destination host is not accessible at this time. When it appears in large clusters without outgoing traffic to the host address, it often indicates 'backscatter' or packets generated in response to a DOS attack on the victim host. Otherwise it is not abnormal traffic.

Top 10 Alert Source Addresses

During the 5 days of September 1 through September 5 the top ten alert source addresses were:

Source Host	Day1	Day2	Day3	Day4	Day5	Total	
211.90.176.59	4981	5032	4996	3680	3245	21934	China United Telecommunications Corporation (cnnic.net.cn)
MY.NET.14.1	4911	3973	3052	2271	1884	16091	**MY.NET.14.1**
MY.NET.16.5	4693	3385	2910	1871	1842	14701	**MY.NET.16.5**
211.90.164.34	2389	2504	2378	970	3117	11358	China United Telecommunications Corporation (cnnic.net.cn)
211.90.88.43	0	2450	2424	2687	1703	9264	China United Telecommunications Corporation (cnnic.net.cn)
61.153.17.244	0	0	2982	0	5916	8898	Ningbo Telecommunication Corporation, China (dcb.hz.zj.cn)
200.250.65.1	2541	1828	1117	687	1295	7468	Embratel.net, Brazil
217.57.15.133	1488	1019	1623	1365	1182	6677	Multigraf-SRL,(cgi.interbusiness.it), Italy

61.153.17.24	0	0	0	0	6654	6654	Ningbo Telecommunication Corporation, China (dcb.hz.zj.cn)
211.96.99.59	2537	1386	1960	728	0	6611	Unicom China,(cnuninet.com)

Yellow – Source is considered to be hostile, or unfriendly

Source hosts **MY.NET.14.1 & .16.5** contributed solely ICMP destination unreachable (communication administratively prohibited) alerts. These were in response to hosts on the MY.NET network. Either a configuration error is preventing access to 14.1 & 16.5, or these hosts are continually attempting access to blocked destinations. No other alert traffic was found logged from these boxes. An inquiry should be made to determine the issue and bring the configurations into synchronization.

http://www.infragard.net/warnings/01_009.htm is from the NIPC, 26 April 2001 – 7 May 2001. The bulletin covers the increased state of tension between the United States and the People's Republic of China, and the increase in cyberterrorism that may result. A continued level of increased hostile activity from mainland China-based IP addresses has been observed since that time. While Code Red and Code RedII are generating the majority of these alerts, a small number of manual probes and attempts are interspersed.

Top 10 Alert Destination Addresses

During the 5 days of September 1 through September 5, of the sample, the top ten destination addresses of traffic that generated alerts:

Host	Day1	Day2	Day3	Day4	Day5	Total
MY.NET.140.9	7497	6295	4790	2936	2568	24086
MY.NET.100.165	5245	3202	2992	2486	1827	15752
MY.NET.253.114	2718	2322	2647	2494	2070	12251
MY.NET.111.221	0	0	0	0	6879	6879
MY.NET.1.3	1473	1319	1248	1115	1491	6646
MY.NET.219.154	1983	1768	1420	724	0	5895
MY.NET.111.142	0	0	0	0	5702	5702
MY.NET.1.4	1111	1154	859	809	1158	5091
MY.NET.1.5	892	732	800	738	1134	4296
MY.NET.178.236	0	3407	0	0	0	3407

MY.NET.140.9
The majority of traffic to this host was logged as traceroute alerts. If this host is exposed to the internet for advertised services, most especially DNS, this will be a normal occurrence. Consideration should be given to filtering these alerts out of the ruleset.

MY.NET.100.165
This host appears to be a web server exposed to the outside networks. The majority of log entries are CS-Webserver alerts. There are numerous probes and command shell access

attempts. In light of the visibility of this address, particular attention should be given to verifying the patch level and configuration of the server.

MY.NET.253.114
This webserver has generated mostly 'prefix-get //' alerts. This may be web page coding outside the permitted standard. If so, the code should be remediated. If however, you wish to allow this coding, the alert rule should be altered for this host to avoid false positives.

MY.NET.111.221 & MY.NET.111.142
On the 5th, this host received a significant number of UDP packets with payload in excess of 4Kbytes on port 0. Neither the payload size, nor the port used, is normally seen in traffic. The source host, 61.153.17.244, resides on a network registered to the People's Republic of China, a source currently considered hostile. **This traffic may indicate a covert tunnel.** Care should be taken to inspect the hosts 111.221 & 111.142 for possible compromise.

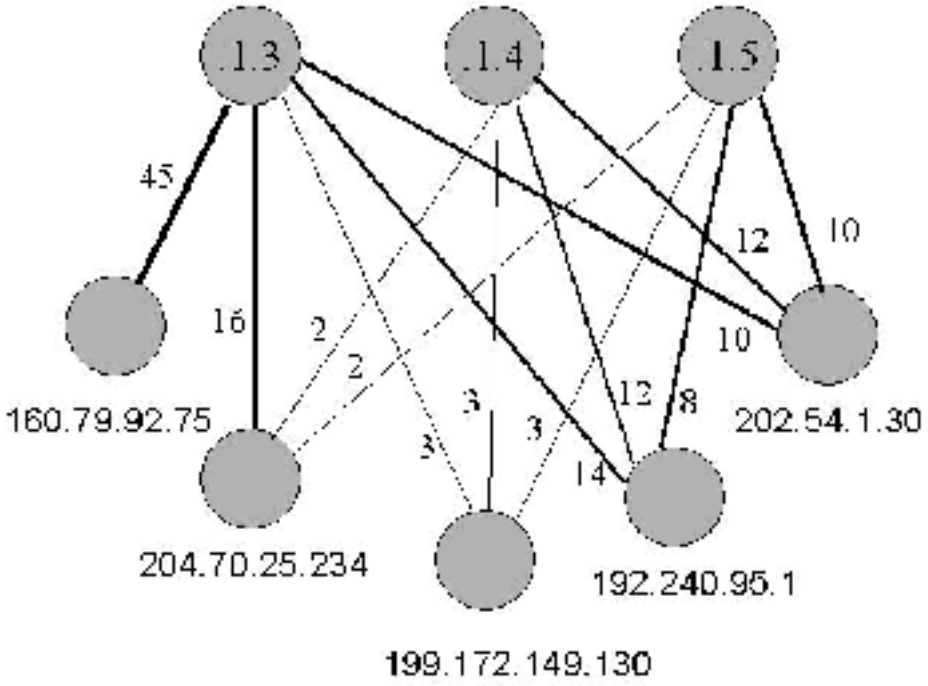
% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois6.apnic.net)

inetnum: 61.153.17.0 - 61.153.17.255
netname: NINGBO-ZHILAN-NET
descr: NINGBO TELECOMMUNICATION CORPORATION ,ZHILAN APPLICATION SERVICE PROVIDER
descr: Ningbo, Zhejiang Province
country: CN
admin-c: CZ61-AP
tech-c: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20010512
source: APNIC

person: CHINANET ZJMASTER
address: no 378,yan an road,hangzhou,zhejiang
country: CN
phone: +86-571-7015441
fax-no: +86-571-7027816
e-mail: master@dcb.hz.zj.cn
nic-hdl: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20001219
source: APNIC

MY.NET.1.3, .4, & .5
These hosts appear to be heavily tasked DNS servers. The alerts attributed to these addresses are related to port 53 traffic. If these hosts are indeed DNS servers, and operating normally, consideration should be given to altering the ruleset to eliminate these alerts.

A link graph showing what appears to be normal distribution of DNS calls between the top 5 source addresses on 1 September and the three DNS servers supports the proposition that the alerts are generated by normal DNS traffic. Distribution between hosts falls in a fairly even pattern, with heavier loading on .1.3 which is most likely the Primary DNS server.



MY.NET.219.154

The alerts associated with this host are ICMP Destination Unreachable(communication Administratively prohibited) from MY.NET.16.5 & 14.1 hosts. This activity was constant until 20:01 hours 4 September, after which it was no longer observed. Most likely a configuration error on either the host or router access controls lists. Confirmation should be obtained from relevant sources to be certain that this activity was benign.

MY.NET.178.236

Several Null scans and a large number of 'tiny fragment' (data size less than 25 bytes) alerts were generated by Host 208.26.55.145 (mail.geray.com) to this host.

GE-RAY FABRICS, INC (NETBLK-FON-349137908879051)
705 GINESI DR
MORGANVILLE, NJ 07751
US

Netname: FON-349137908879051
Netblock: 208.26.55.144 - 208.26.55.151

Coordinator:
KENNEY, GRANT (GK324-ARIN) gkenny@geray.com
(732)972-4033

Record last updated on 15-Oct-2001.
Database last updated on 28-Oct-2001 01:20:07 EDT.

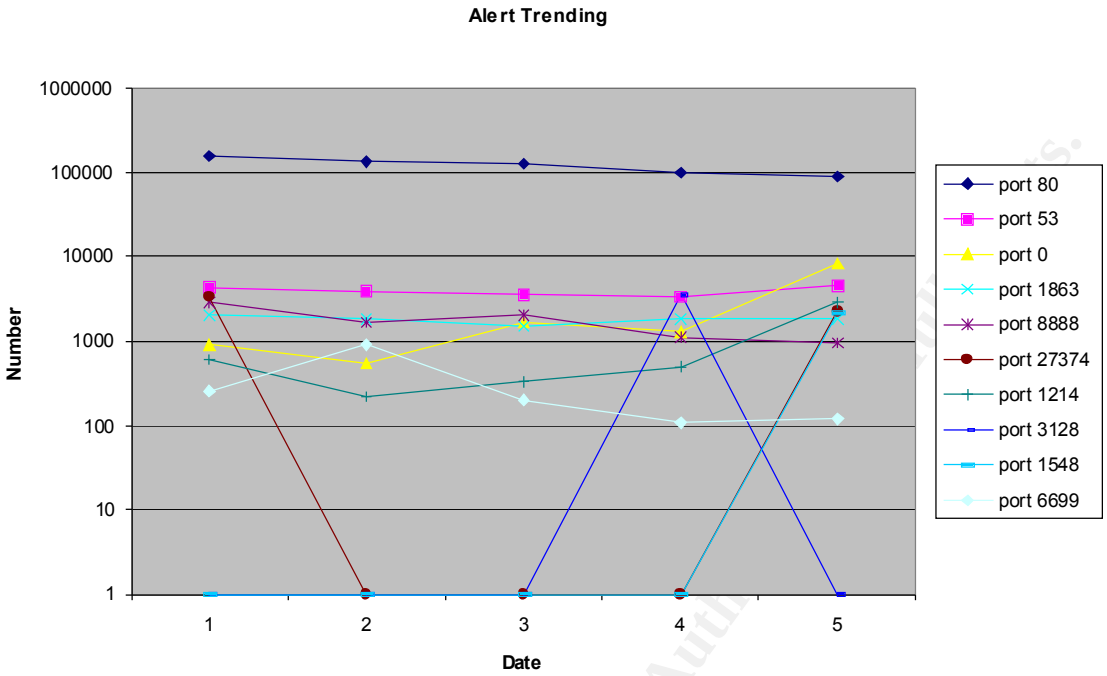
This activity occurred between 06:24 and 06:25 on the 2nd September. This may well have been system error originating from 208.26.55.145. However, the administrator of MY.NET 178.236 should be consulted regarding this incident to verify that the contact with 208.26.55.145 was not malicious.

Top Alert Destination Ports

These ports received traffic that generated alerts in the database. The ten most active were:

Port	Day1	Day2	Day3	Day4	Day5	Total	Service
80	158345	132548	129695	97396	86764	**604748**	**HTTP(Web)**
53	4342	3835	3504	3328	4579	**19588**	**DNS**
0	914	543	1669	1257	8187	**12570**	**abnormal traffic**
1863	2012	1872	1522	1808	1800	**9014**	**MSN Messenger**
8888	2853	1670	2054	1083	954	**8614**	**Napster**
27374	3379	0	0	0	2185	**5564**	**SubSeven 2.1**
1214	602	220	329	483	2886	**4520**	**Kazaa**
3128	0	0	0	3602	0	**3602**	**Squid Proxy scan**
1548	0	0	0	0	2172	**2172**	**Axon License Manager**
6699	256	917	202	107	118	**1600**	**Napster**

The most significant trends over time are the steady decrease in port 80 alerts from the worm probes, and the increase in port 0 traffic.



Top Ten Scan Outside Source Hosts Addresses

This table represents the top ten scan source host ip addresses originating from outside the MY.NET address space. These are most likely recon probes into MY.NET space. In the instances of spinner.com and sony.com, these are most likely marketing/performance probes returned to MY.NET by the vendor. The nature of your user population would suggest this as the most likely cause.

The table below represents the top ten outside host source statistics:

Host	Count	nslookup
212.199.28.76	15469	Host at linux.goldenlines.net.il
216.162.3.20	14869	q2server.asheboro.com
217.128.232.163	6446	ABayonne-101-1-3-163.abo.wanadoo.fr
205.188.246.121	5949	g2lb3.spinner.com
64.37.156.9	5547	sdinf4.station.sony.com
210.95.106.2	5226	Host at nic.or.kr
130.89.229.75	4711	cal034031.student.utwente.nl
129.2.144.201	2602	129-2-144-201.student.umd.edu
130.161.37.101	2458	ntcarme.its.tudelft.nl
217.11.167.47	2200	Host at cedacriovest.it

Nslookup data for 5 suspect scan source addresses

The five highlighted source addresses were chosen for the high volume of scans that they generated, as well as the suspect nature of their origin by infosec standards (i.e., high number of suspect traffic sources in these domains).

212.199.28.76

%This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 212.199.28.0 - 212.199.28.255
netname: GOLDENLINES
descr: DAILUP-PT
country: IL
admin-c: DR5299-RIPE
tech-c: DR5299-RIPE
status: ASSIGNED PA
notify: lir@linux.goldenlines.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: lir@linux.goldenlines.net.il 20010226
changed: lir@linux.goldenlines.net.il 20010626
source: RIPE

route: 212.199.0.0/16
descr: Golden Lines
origin: AS9116
mnt-by: AS9116-MNT
changed: lir@linux.goldenlines.net.il 20010807
source: RIPE

role: DNS REG
address: 25 Hsivim st. Petach-Tiikva, Israel
e-mail: dnsreg@012.net.il
trouble: dnsreg@012.net.il
admin-c: OM2369-RIPE
tech-c: GE2074-RIPE
nic-hdl: DR5299-RIPE
notify: lir@linux.goldenlines.net.il
changed: lir@linux.goldenlines.net.il 20001126
source: RIPE

217.128.232.163

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum: 217.128.232.0 - 217.128.232.255
netname: IP2000-ADSL-BAS
descr: France Telecom IP2000 ADSL BAS
descr: BSBAY101 Bayonne Bloc2
country: FR
admin-c: WITR1-RIPE
tech-c: WITR1-RIPE
status: ASSIGNED PA
remarks: for hacking, spamming or security problems send mail to
remarks: postmaster@wanadoo.fr AND abuse@wanadoo.fr
remarks: for ANY problem send mail to gestionip.ft@francetelecom.com
notify: gestionip.ft@francetelecom.com
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.com 20010817
source: RIPE

route: 217.128.0.0/16
descr: RAIN
descr: Reseaux d'Acces a l'INternet
origin: AS3215
mnt-by: FT-BRX
mnt-by: RAIN-TRANSPAC
changed: karim@rain.fr 20010611
source: RIPE

role: Wanadoo Interactive Technical Role
address: France Telecom Wanadoo Interactive
address: 41, rue Camille Desmoulins
address: 92442 ISSY LES MOULINEAUX Cedex
address: FR
phone: +33 1 41 33 39 00
fax-no: +33 1 41 33 39 01
e-mail: abuse@wanadoo.fr
e-mail: postmaster@wanadoo.fr
admin-c: FTI-RIPE
tech-c: TEFS1-RIPE
nic-hdl: WITR1-RIPE
notify: gestionip.ft@francetelecom.com
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.com 20010504
changed: gestionip.ft@francetelecom.com 20010912
source: RIPE

210.95.106.2

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois7.apnic.net)

inetnum: 210.92.0.0 - 210.95.255.255
netname: KRNIC-KR
descr: KRNIC
descr: Korea Network Information Center
country: KR
admin-c: HM127-AP
tech-c: HM127-AP
remarks: **
remarks: KRNIC is the National Internet Registry
remarks: in Korea under APNIC. If you would like to
remarks: find assignment information in detail
remarks: please refer to the KRNIC Whois DB
remarks: http://whois.nic.or.kr/english/index.html
remarks: **
mnt-by: APNIC-HM

mnt-lower: MNT-KRNIC-AP
changed: hostmaster@apnic.net 19981001
changed: hostmaster@apnic.net 20010606
source: APNIC

person: Host Master
address: Korea Network Information Center
address: Narajongkeum B/D 14F, 1328-3, Seocho-dong, Seocho-ku, Seoul, 137-070, Republic of Korea
country: KR
phone: +82-2-2186-4500
fax-no: +82-2-2186-4496
e-mail: hostmaster@nic.or.kr
nic-hdl: HM127-AP
mnt-by: MNT-KRNIC-AP
changed: hostmaster@nic.or.kr 20010514
source: APNIC

inetnum: 210.95.106.0 - 210.95.106.63
netname: YSSORA-E-KR
descr: Sora Elementary School
descr: 1220 Duckyang-Li Sora-Myun Yosu-Si
descr: CHONNAM
descr: 556-810
country: KR
admin-c: YH118-KR
tech-c: YH119-KR
remarks: This IP address space has been allocated to KRNIC.
remarks: For more information, using KRNIC Whois Database
remarks: whois -h whois.nic.or.kr
remarks: This information has been partially mirrored by APNIC from
remarks: KRNIC. To obtain more specific information, please use the
remarks: KRNIC whois server at whois.krnic.net.
mnt-by: MNT-KRNIC-AP
changed: hostmaster@nic.or.kr 20011022
source: KRNIC

person: YoonPyo Hwang
country: KR
phone: 0662-683-8117
fax-no: 0662-683-2679
e-mail: missi@ppp.kornet21.net
nic-hdl: YH118-KR
remarks: This information has been partially mirrored by APNIC from
remarks: KRNIC. To obtain more specific information, please use the
remarks: KRNIC whois server at whois.krnic.net.

mnt-by: MNT-KRNIC-AP
changed: hostmaster@nic.or.kr 20011022
source: KRNIC

130.89.229.75

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 130.89.0.0 - 130.89.255.255
netname: UTNET
descr: University of Twente
descr: Enschede
country: NL
admin-c: GM3191-RIPE
tech-c: GM3191-RIPE
status: ASSIGNED PI
mnt-by: RIPE-NCC-NONE-MNT
changed: bos@surfnet.nl 20010826
source: RIPE

route: 130.89.0.0/16
descr: UTNET
origin: AS1103
mnt-by: AS1103-MNT
changed: ripe-dbm@ripe.net 19941121
source: RIPE

person: Gert Meijerink
address: Universiteit Twente
address: P.O. Box 217
address: NL-7500 AE Enschede
address: The Netherlands
phone: +31 53 892326
e-mail: gert@utwente.nl
nic-hdl: GM3191-RIPE
remarks: This object is no longer maintained by hostmaster@cwi.nl
remarks: and is or may soon become obsolete.
notify: info@SURFnet.nl
mnt-by: SN-LIR-MNT
mnt-by: SN-LIR-MNT
changed: hostmaster@cwi.nl 19930112
changed: ripe-dbm@ripe.net 19950809

changed: ripe-dbm@ripe.net 19990615
changed: Derk.Reinders@SURFnet.nl 20010326
source: RIPE

130.161.37.101

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 130.161.0.0 - 130.161.255.255
netname: DUNET
descr: Delft University of Technolgy Network (Main network)
descr: Technische Universiteit Delft
descr: Delft
country: NL
admin-c: FK200-RIPE
tech-c: AB6061-RIPE
tech-c: FR392-RIPE
mnt-by: RIPE-NCC-NONE-MNT
changed: F.deKruijf@RC.TUDelft.NL 19920811
changed: ripe-dbm@ripe.net 19920815
changed: scheun@sara.nl 19930806
changed: ripe-dbm@ripe.net 19990706
changed: ripe-dbm@ripe.net 20000225
source: RIPE

route: 130.161.0.0/16
descr: DUNET
origin: AS1103
mnt-by: AS1103-MNT
changed: ripe-dbm@ripe.net 19941121
source: RIPE

person: Freek de Kruijf
address: Technische Universiteit Delft
address: Dienst Technische Ondersteuning
address: P.O. Box 354
address: NL-2600 AJ Delft
address: The Netherlands
phone: +31 15 2783226
fax-no: +31 15 2783787
e-mail: F.deKruijf@DTO.TUDelft.nl
nic-hdl: FK200-RIPE
remarks: Abuse reports to abuse@tudelft.nl

notify: info@SURFnet.nl
mnt-by: SN-LIR-MNT
changed: F.deKruijf@DTO.TUDelft.NL 19991229
changed: F.deKruijf@DTO.TUDelft.NL 20001113
changed: Derk.Reinders@SURFnet.nl 20010326
source: RIPE

person: Aad Boer
address: Technische Universiteit Delft
address: Dienst Technische Ondersteuning
address: P.O. Box 354
address: NL-2600 AJ Delft
address: The Netherlands
phone: +31 15 2781808
fax-no: +31 15 2783787
e-mail: Aad.Boer@DTO.tudelft.nl
nic-hdl: AB6061-RIPE
changed: Henk.Steenman@surfnet.nl 19960402
changed: ripe-dbm@ripe.net 19990615
changed: F.deKruijf@DTO.TUDelft.NL 20001113
source: RIPE

person: Fred Roeling
address: Technische Universiteit Delft
address: Dienst Technische Ondersteuning
address: P.O. Box 354
address: NL-2600 AJ Delft
address: The Netherlands
phone: +31 15 2785010
fax-no: +31 15 2783787
e-mail: Fred.Roeling@rc.tudelft.nl
nic-hdl: FR392-RIPE
changed: Henk.Steenman@surfnet.nl 19960402
changed: F.deKruijf@DTO.TUDelft.NL 20001113
source: RIPE

Top Portscan Destination Ports

This table represents the top ten ranking:

Count	Port	Type	Service
54233	**27005**	UDP	FLEX-LM License Manager
36916	**28800**	UDP	MSN Gaming Zone
34238	**6257**	UDP	Real-Time Streaming protocol 1.0 (RTSP)
33539	**137**	UDP	NETBIOS-Name Service
30406	**21**	TCP	FTP Command channel
17461	**6346**	TCP	GNUTella-svc
15678	**13139**	UDP	GameSpy Arcade UDP pings, NetLinx ICSP (AMX)
11130	**6112**	UDP	Diablo 2/Heavy Gear 2(FSGS) , dtspcd
6978	**80**	TCP	HTTP Web Server
6836	**1214**	TCP	KAZAA (file-sharing utility)

Yellow – Service is likely being scanned for possible compromise. These are services that are often exposed to the Internet, and are often exploited, if vulnerable.
Gray – These services are file sharing utilities. The likelihood of introducing malicious code into the network is increased greatly by the presence of these services.

The top ranking scan port, MY.NET.160.114 on source port 777 UDP (Multiling HTTP translation server), originated attachment attempts to 27005 UDP, accounting for 95% of the instances. This could indicate a server with heavy loading, or possible misconfiguration. If the FLEX-LM license manager service is not being run on these ports, it would be well to identify the service responsible for these connections.
The gaming and streaming media services are often seen in open environment with equivalent user populations. Beyond bandwidth considerations, they are not indicative of a threat situation. Given their prevalence, monitoring of vulnerability lists with regard to these services would seem indicated.

Out-of-Spec packet analysis

The following were the highest incidence packets that violated accepted standards for construction of IP packets.

Out of Spec – Internal Hosts
The following Internal Hosts were reported as the source IP of OOS alerts:

Source	Port	Destination	Port
MY.NET.218.158	1249	24.218.180.0	1214
MY.NET.218.158	1214	159.230.137.230	1114
MY.NET.218.158	173	209.179.162.129	2542
MY.NET.237.6	3267	129.59.32.168	7668

MY.NET.225.82	0	131.118.254.39	1677
MY.NET.229.122	0	63.116.175.52	1399
MY.NET.234.102	0	24.219.228.200	3756

09/04-06:04:42.449664 MY.NET.218.158:1249 -> 24.218.180.0:1214
TCP TTL:125 TOS:0x0 ID:34177 DF
21SF*PAU Seq: 0x21BA92 Ack: 0xDD09 Win: 0x8010
22 38 E0 D0 00 00 01 01 05 0A DD 09 4C AF DD 09 "8.....L...

09/05-12:48:51.251712 MY.NET.218.158:1214 -> 159.230.137.230:1114
TCP TTL:125 TOS:0x0 ID:55342 DF
*1SFR*AU Seq: 0x6B74FC3 Ack: 0x4037FB63 Win: 0x5010
04 BE 04 5A 06 B7 4F C3 40 37 FB 63 00 B7 50 10 ...Z..O.@7.c..P.

09/05-13:41:07.025953 MY.NET.218.158:173 -> 209.179.162.129:2542
TCP TTL:125 TOS:0x0 ID:9547 DF
2*SFRPA* Seq: 0x4BE06E4 Ack: 0xA8780117 Win: 0x5010
04 BE 06 E4 A8 78 01 17 14 5F 50 10 00 00 0B 2D .....x..._P....-
00 00 00 00 00 00 ......

The occurrence of these three packets from host MY.NET.218.158, containing pieces of data which are replicated in the TCP header, would indicate a router, or gateway device, that is mishandling the packet headers. Also, while the SYN bit is set, among others, the acknowledgement number is greater than zero. There is correlation for this in the "demon.net" incident, in which the router at demon.co.uk was performing a similar "mangling" of packet headers. Most likely this will happen when the device is under stress from heavy traffic loading. Given the sparse and random pattern of these packets, this would seem to be more probable than malicious packet crafting as the cause.

09/05-21:43:01.712620 MY.NET.237.6:3267 -> 129.59.32.168:7668
TCP TTL:125 TOS:0x0 ID:40130 DF
21S***A* Seq: 0x209 Ack: 0x77B5B23E Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 0402 00C0 06CE 0000 0000 0000 0000 0000 0000 0000 0000 0000

09/01-09:07:41.494783 MY.NET.225.82:0 -> 131.118.254.39:1677
TCP TTL:125 TOS:0x0 ID:47650 DF
21SF**AU Seq: 0x5004E2 Ack: 0xE1EE5217 Win: 0x5018

TCP Options => EOL EOL

09/05-20:50:39.356616 MY.NET.229.122:0 -> 63.116.175.52:1399
TCP TTL:125 TOS:0x0 ID:39185 DF
21SFRPAU Seq: 0x5000D0 Ack: 0x37A915F2 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK

09/01-02:56:12.807681 MY.NET.234.102:0 -> 24.219.228.200:3756
TCP TTL:125 TOS:0x0 ID:28489 DF
SFA* Seq: 0x1DF4037A Ack: 0x1E41557F Win: 0x5010
21 80 34 07 00 00 00 00 00 00 !.4.....

There have been reports of similar types of traffic:
http://www.sans.org/y2k/041700.htm
04/14-06:21:23.402593 MY.NET.202.98:0 -> 207.172.3.46:3194
TCP TTL:126 TOS:0x0 ID:56306 DF
2*SF**A* Seq: 0x770335 Ack: 0x643DFA07 Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 2424 3031 3233
3435 0000 0000 0000 0000 0000 0000 0000 0000 0000

While the source port of 0 is more suspicious than the other packets examined, probability is still in favor of faulty, or misconfigured, hardware or software. However, care should be taken to examine the hosts involved with a source port 0 packet to insure that these are not crafted packets for the purpose of a Denial of Service, or reconnaissance probing, effort.

Out of Spec – Incoming packets destinations

The top five internal hosts receiving packets that generated OOS alerts were:

Count	Host
73	MY.NET.208.62
31	MY.NET.253.53
27	MY.NET.253.52
23	MY.NET.99.85
14	MY.NET.218.194

MY.NET.208.62

09/04-03:42:17.282833 151.38.11.166:2638 -> MY.NET.208.62:6346
TCP TTL:51 TOS:0x0 ID:41332 DF
21S***** Seq: 0x7EEBBEB7 Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 68558787 0 EOL EOL EOL EOL

09/04-03:48:25.997693 151.38.11.166:2946 -> MY.NET.208.62:6346

TCP TTL:51 TOS:0x0 ID:43268 DF

21S***** Seq: 0x953E06C2 Ack: 0x0 Win: 0x16B0

TCP Options => MSS: 1452 SackOK TS: 68595654 0 EOL EOL EOL EOL

09/04-03:52:31.787424 151.38.11.166:3159 -> MY.NET.208.62:6346

TCP TTL:51 TOS:0x0 ID:47146 DF

21S***** Seq: 0xA509B7EA Ack: 0x0 Win: 0x16B0

TCP Options => MSS: 1452 SackOK TS: 68620224 0 EOL EOL EOL EOL

The packets arriving at MY.NET.208.62 from 151.38.11.166 appear to be valid SYN packets opening normal conversations. The EOL is end-of-option-list delimiter, and may be used as padding in place of NOP. With TTLs at 51 and random TCP sequence numbers, with otherwise well formed packets, this would seem to indicate the use of Explicit Congestion Notification bits from the source as a normal occurrence. These Congestion bits are often seen when packets originate from Windows 2000 hosts or proxies. The constant connects to port 6346 argues against a Queso mapping attempt. Most likely host MY.NET.208.62 is running GNUTella at port 6346. The initial 6346 activity begins on the 4th and an inbound GNUTella connect accept was recorded at 21:50 on the 4th for that machine.

```
alert.010904:09/04-21:50:39.552717  [**] INFO Inbound GNUTella Connect accept
[**] MY.NET.208.62:6346 -> 213.73.142.27:3269
```

MY.NET.253.52 & .53

09/01-05:20:05.996521 198.186.202.147:41055 -> MY.NET.253.53:113

TCP TTL:47 TOS:0x0 ID:25394 DF

21S***** Seq: 0x3B77D4EE Ack: 0x0 Win: 0x16D0

TCP Options => MSS: 1460 SackOK TS: 80394204 0 EOL EOL EOL EOL

09/01-07:35:16.067884 198.186.202.147:43231 -> MY.NET.253.53:113

TCP TTL:47 TOS:0x0 ID:61567 DF

21S***** Seq: 0x397DE7A5 Ack: 0x0 Win: 0x16D0

TCP Options => MSS: 1460 SackOK TS: 81205210 0 EOL EOL EOL EOL

09/01-08:20:20.630373 198.186.202.147:49440 -> MY.NET.253.53:113

TCP TTL:47 TOS:0x0 ID:11137 DF

21S***** Seq: 0xE3ED13D1 Ack: 0x0 Win: 0x16D0

TCP Options => MSS: 1460 SackOK TS: 81475664 0 EOL EOL EOL EOL

These servers appear to be Mail servers serving SMTP and identd authentication services. This would account for the preponderance of spp_portscans attributed to these servers. It would seem that the out-of-spec packets encountered are also of the ECN variety. The captures contain no other signs of malicious intent. It would be recommended that the filters in the IDS ruleset be adjusted to account for the volume and type of traffic that these servers will see.

However, be advised that Host .53 was subjected to Null scans and fingerprinting from 141.156.45.125 on the 5th. Blocking 141.156.45.125 and verifying the security of the .53 server would seem warranted.

Sample packets from 141.156.45.125:

```
alert.010905:09/05-10:50:25.820303  [**] Null scan! [**] 141.156.45.125:0 ->
MY.NET.253.53:0
alert.010905:09/05-10:39:57.176132  [**] Probable NMAP fingerprint attempt
[**] 141.156.45.125:26965 -> MY.NET.253.53:31059
```

MY.NET.99.85

09/02-18:00:32.411196 128.46.156.155:43876 -> MY.NET.99.85:80

TCP TTL:55 TOS:0x0 ID:10277 DF

21S***** Seq: 0xB152FFE0 Ack: 0x0 Win: 0x16D0

TCP Options => MSS: 1460 SackOK TS: 26204101 0 EOL EOL EOL EOL

09/02-23:00:27.688733 128.46.156.155:56030 -> MY.NET.99.85:80

TCP TTL:55 TOS:0x0 ID:11571 DF

21S***** Seq: 0x1C8961EC Ack: 0x0 Win: 0x16D0

TCP Options => MSS: 1460 SackOK TS: 28003551 0 EOL EOL EOL EOL

Thost My.NET.99.85 would appear to be a web/ftp server serving anonymous ftp. The connections from 128.46.156.155 appear to be of the ECN variety, and not malicious. As above, the EOL padding is legal.

MY.NET.218.194

09/03-17:10:18.209610 66.68.190.4:6346 -> MY.NET.218.194:1077
TCP TTL:110 TOS:0x0 ID:63926 DF
21SFRP** Seq: 0x59A Ack: 0xE4D09896 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK NOP

```
alert.010903:09/03-17:04:19.250939  [**] Null scan! [**] 66.68.190.4:6346 ->
MY.NET.218.194:1077
```

```
alert.010903:09/03-17:04:19.250939  [**] Null scan! [**] 66.68.190.4:6346 ->
MY.NET.218.194:1077
alert.010903:09/03-17:17:44.221887  [**] spp_portscan: PORTSCAN DETECTED from
66.68.190.4 (STEALTH) [**]
alert.010903:09/03-17:17:45.678945  [**] spp_portscan: portscan status from
66.68.190.4: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
alert.010903:09/03-17:17:47.286333  [**] spp_portscan: End of portscan from
66.68.190.4: TOTAL time(0s) hosts(1) TCP(1) UDP(0) STEALTH [**]
alert.010903:09/03-17:20:00.106031  [**] spp_portscan: PORTSCAN DETECTED from
66.68.190.4 (STEALTH) [**]
alert.010903:09/03-17:20:01.335492  [**] spp_portscan: portscan status from
66.68.190.4: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
alert.010903:09/03-17:20:02.637531  [**] spp_portscan: End of portscan from
66.68.190.4: TOTAL time(0s) hosts(1) TCP(1) UDP(0) STEALTH [**]
```

This first packet is of some concern. It would seem to be part of a recon probe against MY.Net.218.194. The inverted use of EOL preceding the options would indicate a crafted packet, in addition to the 6 high order bits of TCP flag and a non-zero ack value being set. The additional detects would seem to indicate hostile intent by 66.68.190.4.

09/03-20:04:01.782756 212.194.4.183:33471 -> MY.NET.218.194:6346
TCP TTL:50 TOS:0x0 ID:30578 DF
21S***** Seq: 0xBE9BAC72 Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 1891072 0 EOL EOL EOL EOL

09/03-20:07:05.098713 212.194.4.183:33495 -> MY.NET.218.194:6346
TCP TTL:50 TOS:0x0 ID:29186 DF
21S***** Seq: 0xCA615098 Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 1909402 0 EOL EOL EOL EOL

These packets appear to be normal well-formed GNUTella SYN packets. These appear to be the result of 218.194 making several successful GNUTella connections on this same day. Most likely not of concern if GNUTella is not an issue on the network.

Out of Spec – Incoming packets sources

The top ten external source hosts that generated OOS alerts were:

Count	Host
71	151.38.11.166
58	198.186.202.147
20	128.46.156.155
13	212.194.4.183
11	151.38.84.194
6	24.147.31.25
5	193.137.96.74
4	158.75.57.4
4	203.97.82.178
4	213.23.38.230

Attached is an example of OOS packets generated by the number one top talker:

09/04-03:06:13.783977 151.38.11.166:4817 -> MY.NET.208.62:6346
TCP TTL:51 TOS:0x0 ID:648 DF
21S***** Seq: 0xF6D9D037 Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 68342463 0 EOL EOL EOL EOL

09/04-03:20:36.340867 151.38.11.166:1559 -> MY.NET.208.62:6346
TCP TTL:51 TOS:0x0 ID:52692 DF
21S***** Seq: 0x2C8EEE70 Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 68428708 0 EOL EOL EOL EOL

09/04-03:26:48.036515 151.38.11.166:1864 -> MY.NET.208.62:6346
TCP TTL:51 TOS:0x0 ID:34299 DF
21S***** Seq: 0x4489312A Ack: 0x0 Win: 0x16B0
TCP Options => MSS: 1452 SackOK TS: 68465873 0 EOL EOL EOL EOL

The packet traffic would seem to indicate a GNUTella client with ECN bits set. These could be with the intent to evade detection by an IDS. However, the most likely explanation is normal activity from a congested client.

These hosts should be monitored for baseline performance. OOS packets can indicate an attempt to evade an IDS, or OS fingerprinting. There is also a possibility that mis-configured, or failing, network equipment or damaged software on the hosts could also be responsible for these packets.

198.186.202.147

The number 2 talker also presents a similar profile. Although the subject trips several alerts, they appear to be related to normal ECN bit-flagged traffic to port 113 identd.

09/04-16:15:35.703251 198.186.202.147:40848 -> MY.NET.253.53:113
TCP TTL:47 TOS:0x0 ID:23158 DF
21S***** Seq: 0x9F3F1C9C Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110249706 0 EOL EOL EOL EOL

```
alert.010905:09/05-19:31:43.625463  [**] spp_portscan: PORTSCAN DETECTED from
198.186.202.147 (STEALTH) [**]
```

```
alert.010905:09/05-19:31:44.834829  [**] spp_portscan: portscan status from
198.186.202.147: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
alert.010905:09/05-19:31:46.342567  [**] spp_portscan: End of portscan from
198.186.202.147: TOTAL time(0s) hosts(1) TCP(1) UDP(0) STEALTH [**]
alert.010905:09/05-22:16:40.914920  [**] Queso fingerprint [**]
198.186.202.147:48684 -> MY.NET.253.53:113
```

Analysis process

Given the large volume of data, some form of handling was required. Research prior SANS GCIA papers, I chose to incorporate much of the prior work in data parsing as a foundation. The papers that most closely met my needs were:

Guy Bruneau, 0255
http://www.sans.org/y2k/practical/Guy_Bruneau.doc

Teri Bidwell, 0267
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc

Lenny Zeltser, 0231
http://www.sans.org/y2k/practical/Lenny_Zeltser.htm

The scripts provided by Lenny Zeltser offered the base construction of the logs into a BDB format with general breakout queries of the database files. This allowed me to parse and review the logs, looking for an overall pattern to the traffic and alerts.

The scripts from Guy Bruneau and Teri Bidwell offered insight into possible permutations of command line tools (e.g.,grep, awk, tr, sort, uniq, etc.) that accelerated my further searching through the alert files for more detailed data streams.

For the most part, my methodology was to sift through the reports returned by the BDB queries for items of interest. Finding such, I would craft a command line such as:

'grep –i web 211.90 | awk –F] ' {print $3}'|tr : ' '|awk ' {print $1,$4}'| sort| uniq –c | sort > file211.sort'

This would draw the relevant data to the surface. The parsed data would then provide the springboard for the next iteration. Not knowing what I might find on any given pass, kept me from drafting queries to seek supporting data, and allowed me to 'follow my nose' as the results dictated. Each new data set seemed to open new possible relationships between detects. The challenge was to focus the search down to a chain of logical events each time.

The port service data was retrieved from:

Whitehats.CA

http://www.whitehats.ca/screen/whitehatsca/publications/port_query/port_query.html

NeoHapsis
http://www.treachery.net/security_tools/ports/

SANS Institute
http://www.sans.org/newlook/home.htm

Exploit data came from:

Whitehats.com
http://www.whitehats.com/

SANS Institute
http://www.sans.org/newlook/home.htm

Functionality, with regard to protocols, was found in:

Stevens, W. Richard, TCP/IP Illustrated, Vol. 1
Addison-Wesley, 1994

I believe there are many more correlations that could be made based on time, frequency, timing, and other factors yet to be explored. Perhaps the concept of a data cube, a construct that can be 'sliced' in various ways, would allow greater freedom in analysis. In any event, the exercise was extremely enlightening, and only the beginning, I am sure.

And, attending Stephen Northcutt and Vicki Irwin's presentations at Infragard Houston, on 24 and 25 October added grist for the mill in the final moments. Not to mention the course material in the online GCIA Intrusion detection in depth. My personal thanks go to all the contributors for some great material.

The journey of a thousand li, begins with a single step……