GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

© SANS Institute 2000 - 2002, Author retains full rights.

GCIA Practical for Win Miller

GIAC [Web Based] 30 June 2001

V 2.8

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

GCIA PRACTICAL FOR WIN MILLER **1**

ASSIGNMENT 1 NETWORK DETECTS (FIVE TRACES) **3**

TRACE 1 3
TRACE 2 4
TRACE 3 5
TRACE 4 6
TRACE 5 7

ASSIGNMENT 2 - WHAT SHOULD THE INTRUSION ANALYST TELL THE CEO, IF SHE ASKS. **8**

INTRODUCTION 8
MANAGEMENT'S VIEW OF RISK 9
'AFTER THE FACT' ANALYSIS OF INTRUSIONS 10
ANALYSIS CAPABILITY FOR EGRESS FILTERING 10
VERIFICATION OF FIREWALL'S CONFIGURATION AND OPERATION 10
COORDINATION FOCAL POINT FOR INCIDENT HANDLING ACTIVITIES/INTERNAL THREATS 11
RESOURCES FOR "DEFENSE IN DEPTH" CAPABILITIES TO PROTECT VALUABLE ASSETS. 11
REFERENCES 13

ASSIGNMENT 3 - ANALYZE THIS [MY.NET] **14**

EXECUTIVE SUMMARY 14
OVERVIEW 15
ANALYSIS PRIORITIES 16
FINDINGS 17
General Findings *17*
Isolate Existing Trojan *17*
Potential Additions to Watchlist *18*
Scan Specific Activities *20*
SYN Scan Details *21*
FULL_XMAS Details *23*

APPENDIX A – MY.NET DETAILED ANALYSIS **26**

DETAILED ANALYSIS OF NULL SCAN 29
DETAILED ANALYSIS OF RAMEN 30
DETAILED ANALYSIS OF SYN-FIN 33
DETAILED ANALYSIS OF WATCHLIST 34

APPENDIX B – TRAFFIC BREAKOUT **36**

APPENDIX C – DATA REDUCTION TOOLS (AWK) **38**

APPENDIX D – RAW TRACE FILES FOR ASSIGNMENT 1 ..... **47**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 Network Detects (Five Traces)

The following traces came from my home e-mail PC with a single dial-up to an ISP. The Freeware ZoneAlarm (http://www.zonealarm.com) provided a capture (abbreviated, with nearly 4000 records) for all traffic since it was installed in April 2000. The following analysis was a subset of the inception to June 2001.

Trace 1

```
FWIN,2001/05/20,20:58:16,211.217.47.51:137,MY.ISP.WINMILLER.180:137,UDP
```

1. **Source of Trace:** My home network through a local ISP
2. **Detect Generated by:** My ZoneAlarm [Freeware]
3. **Probability the source address was spoofed:** Unlikely, routine Name Service is not hostile.

Source of Whois: http://packetderm.cotse.com/cgi-bin/lookuptools
Hostname: No Reverse DNS Entries
IP Address: 211.217.47.51
Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-BLK)
These addresses have been further assigned to Asia-Pacific users.
[snipped]
Netname: APNIC-CIDR-BLK2
Netblock: 210.0.0.0 - 211.255.255.255
Coordinator:
Administrator, System (SA90-ARIN) [No mailbox]
+61-7-3367-0490
[snipped]
Record last updated on 03-May-2000.
Database last updated on 28-Jun-2001 22:56:48 EDT.

4. **Description of attack:** Simple NetBIOS name service scan
5. **Attack mechanism:** Standard Microsoft Windows query following normal connection.
6. **Correlation:** P.J.Goodwin_GCIA (V2.6, Dec 2000) http://www.sans.org/giac, Page 91.
7. **Evidence of active targeting:** None, routine Name Service request within Windows.
8. **Severity:** (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3 + 1) – (4 + 4) = -4
   Critical = 3 – home e-mail
   Lethal = 1 – normal IP/name lookup
   System = 4 – current Win98 with SP1
   Net Countermeasures = 4 – ZoneAlarm in High mode
9. **Defensive recommendations:** No additional effort required, current configuration sufficient
10. **Multiple Choice Question:**

What is the primary Internet background noise?
A) DNS Lookups
B) NMAP Scans
C) 137 UDP NetBIOS Name Service

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Trace 2

```
20010417, 21:17:50, 63.208.157.51, 80, 207.192.132.183, 2049, TCP [FWIN]
```

1. **Source of Trace:** My home network through a local ISP
2. **Detect Generated by:** My ZoneAlarm [Freeware]
3. **Probability the source address was spoofed:** Not likely as this is probably a precursor scan with exploitation scripts ready to attack the target if the vulnerability (NFS) is recognized. Likely cable-modem node compromised for these types of scanning efforts.
   Source for Whois:
   http://www.samspade.org/t/lookat.cgi?address=63.208.157.51&whois=on&ipblock=on&clueless=no
   whois -h whois.arin.net 63.208.157.51
   Level 3 Communications, Inc. (NETBLK-LEVEL4-CIDR)
   1450 Infinite Drive
   Louisville, CO 80027
   US
   Netname: LEVEL4-CIDR
   Netblock: 63.208.0.0 - 63.215.255.255
   Maintainer: LVLT
   Coordinator:
   level Communications (LC-ORG-ARIN) ipaddressing@level3.com
   +1 (877) 453-8353
   Domain System inverse mapping provided by:
   NS1.LEVEL3.NET 209.244.0.1
   NS2.LEVEL3.NET 209.244.0.2
   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
   Record last updated on 30-May-2001.
   Database last updated on 29-Jun-2001 23:03:45 EDT.
4. **Description of attack:** Scan for NFS using source-port 80 as a cover. No additional scans were observed.
5. **Attach mechanism:** Unknown, best guess is a standard scanning tool like NMAP.
6. **Correlation:** J. Scambray, S McClure & G Kurtz, Hacking Exposed (2nd Edition), McGraw-Hill, Berkeley, CA, 2001, Page 106.
7. **Evidence of active targeting:** Not likely, as this is a Unix vulnerability not a Win98 issue.
8. **Severity:** (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3 + 4) – (4 + 4) = -1
   Critical = 3 –home e-mail
   Lethal = 4 – older Unix vulnerability
   System = 4 – current Win98 with SP1
   Net Countermeasures = 4 – ZoneAlarm in High mode
9. **Defensive recommendations:** Do not use NFS outside a very well protected enclave.
10. **Multiple Choice Question:**

When is source port 80 used?

A) Only for http packets.
B) Whatever the RFC allows.
C) <u>When you want to penetrate a protected network.</u>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Trace 3

```
FWIN,2000/09/17,22:09:04,208.225.40.17:2198,MY.ISP.WINMILLER.140:111,TCP
```

1. **Source of Trace:** My home network through a local ISP
2. **Detect Generated by:** My ZoneAlarm [Freeware]
3. **Probability the source address was spoofed:** Low, the source system could not complete the penetration if the three-way handshake was not available.

Whois from http://www.geektools.com/cgi-bin/proxy.cgi

UUNET Technologies, Inc. (NETBLK-UUNET1996B) UUNET1996B
208.192.0.0 - 208.255.255.255
Prime Communication Systems Corp (NETBLK-UU-208-225-40) UU-208-225-40
208.225.40.0 - 208.225.40.255
Technology Distribution Network (NETBLK-P-208-225-40-16) P-208-225-40-16
208.225.40.16 - 208.225.40.31

4. **Description of attack:** Portmapper (SunRPC) scan.
5. **Attack mechanism:** Likely a standard scanning tool
6. **Correlation**: J. Scambray, S McClure & G Kurtz, Hacking Exposed (2nd Edition), McGraw-Hill, Berkeley, CA, 2001, Page 326-327
7. **Evidence of active targeting:** Not likely, as this is a Server vulnerability not a Win98 issue.
8. **Severity:** (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3 + 4) – (4 + 4) = -1
   Critical = 3 – home e-mail
   Lethal = 4 – reconnaissance of all popular exploitations
   System = 4 – current Win98 with SP1
   Net Countermeasures = 4 – ZoneAlarm in High mode
9. **Defensive recommendations :** No action required, existing configurations effective.
10. **Multiple Choice Question:**

NFS provides:
A) Secure file sharing over networks.
B) Reduced workload for System Managers
C) Overtime for CERT Staff and Incident Handlers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Trace 4

```
FWIN,2000/07/19,16:58:04,205.188.6.86:5190,MY.ISP.WINMILLER.140:1735,TCP
FWIN,2000/07/19,16:58:04,205.188.7.77:5190,MY.ISP.WINMILLER.140:1729,TCP
FWIN,2000/07/19,16:58:36,205.188.7.125:5190,MY.ISP.WINMILLER.140:1725,TCP
FWIN,2000/07/28,19:03:28,205.188.4.130:5190,MY.ISP.WINMILLER.145:4370,TCP
FWIN,2000/07/28,19:03:40,205.188.2.117:5190,MY.ISP.WINMILLER.145:4362,TCP
```

1. **Source of Trace:** My home network through a local ISP
2. **Detect Generated by:** My ZoneAlarm [Freeware]
3. **Probability the source address was spoofed:** Not likely, AOL Instant Messager uses port 5190 to set up connections.
   whois -h whois.arin.net 205.188.6.86 from http://www.samspade.org
   America Online, Inc (NETBLK-AOL-DTC)
   22080 Pacific Blvd
   Sterling, VA 20166
   US
   Netname: AOL-DTC
   Netblock: 205.188.0.0 - 205.188.255.255
   Coordinator:
   America Online, Inc. (AOL-NOC-ARIN) domains@AOL.NET
   703-265-4670
   [snipped]
   Record last updated on 27-Apr-1998.
   Database last updated on 28-Jun-2001 22:56:48 EDT.
4. **Description of attack:** AOL's attempt to send instant messages to this system, probably a low level scanning technique, as AIM is not installed.
5. **Attack mechanism:** Probably a simple scan, not hostile.
6. **Correlation:** Ryan Russell & Stace Cunningham, Hack Proofing Your Network, Syngress, Rockland, MA, 2000
7. **Evidence of active targeting:** Two active attempts over 9 days suggest an invalid address, or standard scan.
8. **Severity:** (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3 + 1) – (4 + 4) = -4
   Critical = 3 – home e-mail
   Lethal = 1 – reconnaissance or bad e-mail address
   System = 4 – current Win98 with SP1
   Net Countermeasures = 4 – ZoneAlarm in High mode
9. **Defensive recommendations:** No action required, existing configurations effective.
10. **Multiple Choice Question:**

What would you use to identify AIM traffic on a MS/Windows machine?

A) Netstat
B) Ipconfig
C) Whois

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Trace 5

```
FWIN,2000/12/13,20:36:10,147.208.171.139:0,MY.ISP.WINMILLER.179:0,ICMP
FWIN,2000/12/13,20:36:28,147.208.171.139:1782,MY.ISP.WINMILLER.179:21,TCP
FWIN,2000/12/13,20:36:28,147.208.171.139:1784,MY.ISP.WINMILLER.179:23,TCP
FWIN,2000/12/13,20:36:28,147.208.171.139:1786,MY.ISP.WINMILLER.179:25,TCP
FWIN,2000/12/13,20:36:28,147.208.171.139:1788,MY.ISP.WINMILLER.179:79,TCP
```

[200+ additional packets snipped]

```
FWIN,2000/12/13,20:38:46,147.208.171.139:4817,MY.ISP.WINMILLER.179:5000,TCP
FWIN,2000/12/13,20:38:46,147.208.171.139:4819,MY.ISP.WINMILLER.179:5001,TCP
FWIN,2000/12/13,20:38:46,147.208.171.139:4821,MY.ISP.WINMILLER.179:5321,TCP
FWIN,2000/12/13,20:38:46,147.208.171.139:4823,MY.ISP.WINMILLER.179:5400,TCP
```

1. **Source of Trace:** My home network through a local ISP
2. **Detect Generated by:** ZoneAlarm [Freeware version]
3. **Probability the source address was spoofed:** None, this is a vulnerability scan service offered by Norton.com. Note that there is some issues about the IP address from the DNS point of view.

http://www.samspade.org/t/lookat.cgi?address=147.208.171.139&whois=on&clueless=no

Official name: security.norton.com
Addresses: 147.208.171.139
Possible forgery - security.norton.com is claiming to be 147.208.171.139, but 147.208.171.139 isn't a valid address for security.norton.com
[snipped]
Technical Contact:
Domain Registrar (DR206-ORG) domain@SYMANTEC.COM
Symantec Corporation
20330 Stevens Creek Blvd
Cupertino, CA 95014
US
+ 1 408 253-9600
Fax- + 1 408 517-8128
[snipped]
Database last updated on 29-Jun-2001 00:10:00 EDT.

4. **Description of attack:** Vulnerability Scan from network security vendor.
5. **Attach mechanism:** Symantec Security Check
6. **Correlation:** Product is used to Validate Norton Internet Security package for Win98/NT
7. **Evidence of active targeting:** Self-inflicted
8. **Severity:** (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3 + 2) – (4 + 5) = -4
   Critical = 3 – home e-mail
   Lethal = 2 – reconnaissance of all popular exploitations
   System = 4 – current Win98 with SP1
   Net Countermeasures = 5 – ZoneAlarm in High mode
9. **Defensive recommendations:** It's probably a bad idea if you are not testing a personal firewall.
10. **Multiple Choice Question:**
    How do you confirm your firewall's configuration?
    A) Trust the vendor to give you out of the box security
    B) Announce to the world your protected by firewall 'X'
    C) <u>Develop and run test scripts against it on a regular basis</u>
    D) Use the web to maintain up-to-date configurations, via trial by fire.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 - What should the Intrusion Analyst tell the CEO, if she asks.

Introduction

It's a safe bet that most of us involved in the GIAC Intrusion Detection Analysis Course have focused on the specialized skills of information technology (IT), computer security and hex dump analysis. We were trained by our mentors, supervisors and fellow technologist to approach problems from an "IF-THEN-ELSE" viewpoint. Nothing was impossible, everything could be repaired, replaced or upgraded, and most importantly, the budget decisions were "management's problem." The skilled, efficient and laborsaving solutions we provided the organization propelled it to the top if its sector. That has been true for the last 20 years. We have success beyond our wildest imagination; we actually did change the world. Our skills are in high demand and we are needed more than ever, but not for the same reasons. The world has switched from research & development to production. The shift in the IT "product life-cycle" now focuses on the cost-cutting, steady-state, maintenance mode, with the information system becoming a commodity to be built, deployed, managed and disposed. One more thing has changed; our role in that society.

The intrusion analyst is the beat-cop of the cyber age. Its our job to get to know the locals and the daily traffic patterns on our beat. The tempo of systems under our care should become as familiar as the commute to work, or shuffle to the den for those really lucky "net-workers." We can take pride that we actually did build the place with our bare hands. But wait, how could we expect to keep the same income, perks and lifestyle when we have moved from the architect to the beat-cop? That's the question that we need to answer. And the answer revolves around the net value provided to the organization. Senior management, at some point, will want to know what value we provide.

The bad news is that senior management has one and only one interest, staying afloat. The "front office" will put their time, talent and money where the best return on investment (ROI) will be. The issues of stockholder relationships, Regulators [Securities and Exchange Commission] attention and media probing of sensitive corporate issues have their full attention.

The good news is that anything that you do to keep them from facing enraged stockholders, aggressive SEC investigators or hostile media will be welcomed, appreciated and rewarded. And that's where the Information Security capability comes into play. As a proud member of the Infosec Ninjas, we have pledged ourselves to the warning banner, "Authorized Users Only", "Proprietary Data" and "Business Use Only."

What we provide the corporate organization has not changed as much as it has evolved. The products must be repackaged so that management can understand the capabilities, limitations, and cost and performance issues necessary to focus their attention and money. It is our mission to develop a better way of packaging the products for the internal consumer. Historically, the tools and techniques of Infosec was the sole province of the System Staff. In this new age of IT, everything is subject to cost/benefit analysis, be it data, software, hardware services, or staff. Every item in the corporate inventory has to compete for space on the shelf, including the senior technical staff. How can we provide our very specialized tools, services, techniques and reporting when the average third grader is more IT savvy than the entire corporate staff? It's

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

done by providing the tools, services and techniques corporate management understands. They understand the need to protect the organization and ensure ongoing uninterrupted access to clean, safe data. The issues of detailed implementation, resource trade-off, dependencies and development models are best left inside the data-center. When management gives you five minutes to present a strategy for "security" the words that come to mind should include:

B	Threat → vulnerabilities (asset) => impact
U	Threat → vulnerabilities (asset) => impact
D	----------Risk Threshold ----------
G	Threat → vulnerabilities (asset) => impact
E	Threat → vulnerabilities (asset) => impact
T	Threat → vulnerabilities (asset) => impact
⇓	Threat → vulnerabilities (asset) => impact

Management's View of Risk
(Note: Probability element = 1.0, Murphy's law)

Assets	- What management want's to protect
Budget	- What resources management has available
Impact	- What is the result to the organization (minor, major, fatal)
Risk threshold	- Ranking for budget purposes
Threats	- Who and what might damage the assets
Vulnerabilities	- Some of the ways those assets can be damaged
Cost savings	- Ways to prune cost without impacting the Risk Threshold (Removing minor assets and their accompanying vulnerabilities)
Cost avoidance	- Modifying a vulnerability or reducing a threat
Risk mitigation	- Insurance policy or reserves to recover/restore an asset
Risk management	- Business practice of identifying and classifying threats and Vulnerabilities to the corporate assets worth protecting
Training	- Teaching staff how to properly use an asset
Awareness	- Keeping staff up-to-date on the current threats and vulnerabilities
Education	- Teaching staff why, where and when an asset can be used
Cost/Benefit	- What it cost to protect an asset versus what it cost to replace it

Before we move into the specifics of Infosec, lets take a "real world" example to test the model. When the World Trade Center's power, water and environmental system were "compromised" several years ago, several hundred businesses located in the building were required to relocate to their "off-site facility." Of the several dozen businesses that took more than 10 days to restore their information systems, few survived.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

So, if the asset called information system has a denial of service vulnerability of over 10 days, and management has put that item below the risk threshold (meaning corrective actions are not funded) any implementation of that threat would result in collapse. Now that we have management's attention, lets proceed with the Intrusion Detection.

Aside from the technical issues, that we so much enjoy, the realities of IDS are that the tool provides five unique capabilities (using the Infosec's vocabulary):

1) 'After the fact' analysis of intrusions,
2) Analysis capability for egress filtering (with appropriate permissions, of course),
3) Verification of firewall's configuration and operation,
4) Coordination focal point for incident handling activities and/or "internal threats", and
5) Resources for deploying "defense in depth" capabilities to protect valuable assets.

Each of these capabilities will be addressed in terms of the corporate management Risk model with some help from the TV version of law enforcement.

'After the fact' analysis of intrusions
This is the *crime scene investigator*, expert witness preparation and autopsy phase of the incident. The evidence is collected, recorded, analyzed and maintained within strict control to allow the proper presentation if further legal actions are warranted. The organizational security policy provides the framework for any and all actions resulting from an incident, at the direction of Legal Advise and the Human Resource Officer. If the standards of the organization are to "repair and resume" rather than "pursue and prosecute" no further direct action is warranted. The analysis of the incident will be valuable in identifying the original vulnerability and providing means to mitigate that threat in the future. Impact on Media, Regulators and Stockholders = moderate. [2 out of 4]

Analysis capability for egress filtering
This is the *stakeout*, looking for known criminal activity. One of the few successful ways to identify and control some web-based attacks is to look for things that should not be leaving your network. Egress filtering is the use of the intrusion detection tools to monitor for those signatures. The common approach to the denial of service (DOS) and distributed denial of service (DDOS) attacks is to take over someone else's system to launch the attack. If your system has been compromised in that way, and the attacker was skilled and careful, the only notice of an active attack is the phone call from the victim, his lawyer or the media asking why you put the victim out of business. Impact on Media, Regulators, and Stockholders = high. [3 out of 4]

Verification of firewall's configuration and operation
This is the *traffic cop* that manages and directs the flow of data in and out of the organization. The firewall, according to the media is the single most important means available to protect the critical systems. That is true. Unfortunately, there are many hundreds of systems in each organization that may not be "critical." In violation of the security policy, they, the non-critical system "managers" use their internal modems to access outside the firewall. Since the firewall is defending a fixed space, much of the internal activities are hidden from view of the firewall and her logs. The use of an intrusion detection system allows for the better view of the organizations

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

assets and can verify the proper settings on the firewall by analysis of what passes and what is stopped by it. An improperly configured firewall is a dual threat; it provides no protection while reducing the paranoia that is healthy in the Infosec arena. Impact on Stockholders = moderate. [2 out of 4]

Coordination focal point for incident handling activities/internal threats
This is the *swat team* that will clean up whatever the bad guys left after a successful intrusion, virus infections, e-mail based Trojan, or…(the list is open ended). Depending on the structure of the Computer Incident Team, and the depth of skills available, the IDS analysts will probably be among the better prepared to brief the team on the objectives and procedures needed to identify the target. It's the combination of skills and talent that build the IT infrastructure, but it will be a different combination of skills and talent to keep it safe from harm. The society at large needs the social worker and the beat cop/swat team member, but seldom finds it worth while to have them switch roles.

This is the *internal affairs* investigator that will work with the Legal and HR staff on the problem that comes from rapid changes in staffing, outsourcing, downsizing, mergers, takeovers and assorted criminal and non-criminal behavior. The e-mail stalker, the porno collector and a wide variety of illegal and threatening behavior attempt to hide behind a fake-mail address and compromised IP-address. The team of legal, HR and the IT specialist will be needed to detect, verify and turnover the incident to law enforcement for proper resolution. Impact on Stockholders, Regulators and Media = high. [3 out of 4]

Resources for "defense in depth" capabilities to protect valuable assets.
Consider this activity as a *convoy duty* for the most important assets the organization has. The patents, the strategic plans and the sealed bids need to be carefully protected and stored where no harm can come to them. Multiple levels of protection can be applied to allow controlled access to the items while providing a high level of assurance that they have not been destroyed, modified or compromised while in storage, transport or production. It must be assumed that any illegal access to these items is a critical blow against the organization, thus worthy of protection. Impact on Stockholders = Very High. [4 out of 4]
The raw score is 14 out of 20, but any lapse by the Intrusion Analyst could be fatal to the reputation, image and market-share of the organization.

Okay, lets recap. We have a presentation approach in terms of budgets, threats, vulnerabilities, assets and impact. We have a set of capabilities provided by the Intrusion Detection System that includes analysis, filtering, verification, coordination, and protection (as in Defense in Depth). Now, we will conclude with a 'draft' layout of a presentation. The simulation will hopefully provide a guide that can be adopted to meet the need, provided some realistic numbers, dates, duration, and staffing requirements can be developed. The Cost% column is my attempt to quantify one approach to distribution of assets in response the broad range of threats identified by an organization. Remember to verify your facts, be wildly pessimistic with your numbers and be careful what turf you defend.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Information System Security Overview

Cost%	Threat	Vulnerability	Asset	Impact	Defense
15	Hacker	Any weakness	Full system	Reputation	Layered Defense
25	Competitor	Focused Attack	Plans, Prices	Mkt. Share	Access Ctl
40	Insider	Everything	Everything	Total	Policy/Vigilance
5	Design Flaw	Software/System	Full System	Time/Staff	Config Mgt
10	Trojan	Un-patched SW	Full system	Time/Staff	Firewall
5	Virus	Outdated Scanner	Full system	Time/Staff	Procedures

Corporate Information System Security Exposure

Design Constraints

Corporate By-in
Policy Documents
Implementation Procedures
Available Staff
Available Systems/Network/Hardware
Time/budget/staff factors
Tools/Techniques/Technology Curve

Corporate Information System Design Constraints

Layered Defense (Defense in Depth)

External Router

External IDS Sensor

Firewall

Internal Router

DMZ Network

Public Web Site
Public Mail System
Internal IDS Sensor

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	Application Network	
		Data Servers
		Application Servers
		Internal IDS Sensor
	User Network	
		User Workstation
		Networked Printers
		Internal IDS Sensor
Protected Sub-nets		
Firewalls/IDS/VPN ->	Finance Network	
Firewalls/IDS/VPN ->	Human Resource Network	
Firewalls/IDS/VPN ->	Marketing Network	
Firewalls/IDS/VPN ->	Network Operations Center (IDS Management)	

Corporate Information System Layered Defense

It will up to you to develop the tie in between the Defense column in the Exposure Slide and the layered defense in the final slide. It will be this link that will provide the justification and rational for the acceptance of information system security in general and the intrusion detection system in particular by the organization.

References

Dan Chandler, Planning Concerns Considerations, and Tips for IDS in Federal IT Systems, March 30, 2001, http://www.sans.org/infosecFAQ/intrusion/fed_IT.htm

Tom Conley , Internal Investigations - Procedures and Techniques: An Overview, April 9, 2001, http://www.sans.org/infosecFAQ/intrusion/investigations.htm

Scott Manderscheid, An Intrusion Detection System Process: Defense in Depth, February 9, 2001, http://www.sans.org/infosecFAQ/intrusion/process.htm

Steven A. Sandberg, Computer Crime: The Insecurity of Your Network, December 14, 2000, http://www.sans.org/infosecFAQ/threats/comp_crime.htm

Geoffrey H Wold and Robert F Shiver, Risk Analysis Techniques, http://www.drj.com/new2dr/w3_030.htm

[Alwin Miller], Evolving Security Architecture toward the Defense Information Infrastructure, CDRL A011-A697-004-002, Contract Number DAHA90-96-D-005, October 1998

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 3 - Analyze This [My.NET]

Executive Summary

My.Net is a University network that has several days of Snort IDS traffic from several unspecified sensor locations collected and delivered for analysis. The problem set includes the request to identify possible system compromise, as well as provide a clear methodology for analysis. The initial finding are that the network has been penetrated and two machines, MY.NET.70.38 and MY.NET.217.150 have been used to actively scan inside and externally for future targets. The traffic available for analysis does not provide sufficient material to determine the compromise vector, nor the depth of exposure, but immediate action is necessary to limit the Universities exposure and remove the threat to the internal network. There is a long list of potential threatening probes and scans, as shown in the Messages table, some of which may have been successful. Additionally, the University's network does not have an effective barrier to external probing of the internal machines. The several individual hosts do not appear to be hardened against common threats (Back Orafice, Wingate, RAMEN, etc). Finally the management of the Intrusion Detection System has delivered fifteen log files with a January 2000 and February 2000 date stamp, making them invalid for further analysis.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Overview

My.Net is a University network that has several days of Snort IDS traffic from several unspecified sensor locations collected and delivered for analysis. The problem set includes the request to identify possible system compromise, as well as provide a clear methodology for analysis. The first part of this section will address the analysis process, tools development, data reduction approach and abbreviated presentation of findings. The more detailed analysis and generated tables are attached as Appendix A.

The initial review of the traffic shows that there are three primary types of data formats: Alert, Out of Specification (OOS) and Scan. There was a problem with a subset of the traffic (fifteen files from all three types) having an invalid collection date, February and March 2000. All files with invalid dates in the header were removed from the analysis process. If the analysis of the traffic led to conformation of a system compromise, with sufficient evidence for prosecution, the use of any "tainted" data would not help law enforcement, legal staff or the Incident Handler.

The remaining data was then sorted by type and processed by AWK scripts to provide a "normal" data format for increased searching, sorting, consolidation, analysis, and reporting. At each successive level of detail, items of interest could be culled from the data set and reduced for more specific review. The data reduction and reporting script (q2a) provides a single tool for this purpose.

Extract of Traffic from/to MY.NET reduced the load to 40,000-70,000 records (depending on actual query request) from original Total Traffic of 526,338 records. Exact breakout of traffic is shown in Appendix B. The source code for the analysis is show in Appendix C.

The methodology for analysis is to use the SANS Top Ten Threats, http://www.sans.org/topten.htm with AWK's string processing capabilities to reduce the "eye-ball" time required to locate "interesting traffic." The underlying concept is that anomalies [interesting traffic] tend to jump off the page, if the information has been prepared and rendered appropriately. By selecting the Count of top 20 for several of the recorded fields in the traffic, and displaying the output in table format, the weirdness shines through. For this effort, three AWK scripts were developed, listing in Appendix C, to prepare, normalize and report the traffic. When items of further interest appear, the analyst can create a subdirectory one more level down and the use the Linux grep command to copy all occurrences of that type of traffic to a new "raw" file. That new "raw" file can then be further processed using the same Q2a report script. Whether the "interesting traffic" is valid and normal is up the analyst, but:

- correlation with the message field,
- known Trojan ports,
- time of activity,
- duration of specific action, and
- Sequence of activities tends to alert not-normal traffic.

The process for reduction: grep "<Select Phrase>" new_cnt > <new dir>/new_cnt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Analysis Priorities

The search for Existing Trojans is a high priority as it shows successful penetration of the network and exposes the organization to legal and operational issues that are best avoided. Some of the techniques for alerting and exposing the Trojans include:

- -Egress Filtering - items without verified request
- -ACK from external probes
- -IRC Response traffic
- -"Random" internal traffic to unknown external destinations (IRC)

The SANS Top 10 Threats (http://www.sans.org/topten.htm) provides a secondary priority in that the penetration may be in process, or soon to occur. Current literature offers that a clean install of an unpatched operating system (any flavor) on a newly networked machine can be identified, scanned, penetrated, compromised, and taken-over in under half an hour. Given the increasing bandwidth in the last few months, this "grace time" will probably shrink to under a minute fairly soon. The list of vulnerabilities include:

- -Bind
- -CGI
- -RPC
- -RDS
- -Sendmail
- -SADMIND/MOUNTD
- -NetBIOS/NFS
- -IMAP
- -SNMP
- -WINNT/OFFICE 2000

The third level of priority for network/system protection is the identification and blocking of Hostile Scans. These are normally used to identify and catalog future targets for the Cracker. The tools of choice evolve daily and constant vigilance is necessary.

The fourth and final priority is the collection of "Interesting Traffic" that may yet turn out to be a new wrinkle in the attacker toolkit. The collection and sharing of these developing signatures provide the advanced warning and lead-time.

This is the central point of the Intrusion Analyst effort, that of identifying and preventing compromised systems, further details are available at http://www.sans.org/topten.htm.

The following table from the MY.NET Detailed Analysis provides one view of the threats identified in the Snort Traffic.

Messages (All)

Watchlist 000220 IL-ISDNNET-990517	16378
SYN-FIN scan!	12716
Possible RAMEN server activity	7033
NMAP TCP ping!	2408
SNMP public access	1147
SMB Name Wildcard	608

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Queso fingerprint	463
WinGate 1080 Attempt	411
Attempted Sun RPC high port access	409
Tiny Fragments - Possible Hostile Activity	230
connect to 515 from inside	135
Null scan!	110
Watchlist 000222 NET-NCFC	92
Back Orifice	25
SUNRPC highport access!	14
External RPC call	5
TCP SMTP Source Port traffic	4
Security 000516-1	4
Probable NMAP fingerprint attempt	2
SITE EXEC - Possible wu-ftpd exploit - GIAC000623	1
Russia Dynao - SANS Flash 28-jul-00	1

Findings

General Findings

The initial finding are that the network has been penetrated and two machines, MY.NET.70.38 and MY.NET.217.150 have been used to actively scan inside and externally for future targets. The traffic available for analysis does not provide sufficient material to determine the compromise vector, nor the depth of exposure, but immediate action is necessary to limit the Universities exposure and remove the threat to the internal network. Additionally, the University's network does not have an effective barrier to external probing of the internal machines. The several individual hosts do not appear to be hardened against common threats (Back Orafice, SubSeven, etc). Finally the management of the Intrusion Detection System has delivered fifteen log files with a January 2000 and February 2000 date stamp, making them invalid for further analysis. The ability of internal system to generate XMAS scan should be a clear violation of the Accepted Use Policy Agreement signed by all system and network users prior to system access. The high level of UDP traffic suggests that the border router does not filter external traffic sufficiently, as well as permitting "high risk" traffic into the University's network. Of the several warning messages from the Snort Alert's many may turn out to be "noise, but more likely they are valid threats against the network, and should be investigated completely. The quick response requirements preclude a full analysis.

Isolate Existing Trojan

Preliminary analysis of MY.NET suggests the network has been compromised, penetrated and is probably a staging facility for at least two active scanners, MY.NET.70.38 and MY.NET.217.150. The use of the XMAS scan and both internal and external RMAN probes as shown in the FULL_XMAS Detail and RMAN sections should confirm the suspicions. These two machines need to be removed from service immediately because of their active probing of external networks. In accordance with your site security manual and information system security policy, activate the Incident Handler to resolve the problems with these two machines. Additional machines with the MY.NET may have been compromised at the same time and are dormant until activated by the perpetrator.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

POSSIBLE TROJAN (MY.NET HOST)

IP ADDRESS	COUNT
MY.NET.70.38	9977
MY.NET.217.150	2800
MY.NET.179.78	1718
MY.NET.204.94	1586
MY.NET.208.10	1538
MY.NET.206.30	1484
MY.NET.227.78	1333
MY.NET.222.122	1321
MY.NET.253.24	1117

Potential Additions to Watchlist

Using the whois capability at www.incident.org, http://www.samspade.org/ and other support sites, along with the volume, characteristics and time of the "unwanted traffic" the intrusion analyst can isolate and defend against point targets. Care must be taken not to create your own "denial of service" by locking out an existing business relationship or acting upon a spoofed ip address. The following sites are candidates to lockout at the router and/or firewall level if the traffic is not truly business related. The whois lookup is provided to identify possible compromised or "bad-behavior" locations.

POSSIBLE TROJAN SCANNER (EXTERNAL)

169.226.202.234	12129
130.234.184.112	9446
24.67.186.244	4760
132.235.177.123	4419
194.42.97.1	2536
208.14.222.201	2099
64.224.193.144	2049
211.13.192.37	1402
63.89.128.4	1392
213.224.161.89	1315

Source of whois:
http://www.geektools.com/cgi-bin/proxy.cgi

169.226.202.234	12129

University at Albany, State University of New York (NET-U-ALBANY)
1400 Washington Av
Albanyr, NY 12222
US
Netname: U-ALBANY
Netblock: 169.226.0.0 - 169.226.255.255
Coordinator:
Nirenberg, Isabel L. (ILN1-ARIN) sysiln@csc.albany.edu

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(518) 442-3736

130.234.184.112	9446

NORDU Nets (NET-NORDU1)
University of Jyvaskyla Computing Center, PL 35 (MaD)
Jyvaskyla, FIN-40351
FI
Netname: JUNE
Netblock: 130.234.0.0 - 130.234.255.255
Coordinator:
University of Jyvaskyla Hostmaster (UJ-ORG-ARIN) hostmaster@JYU.FI
+358 14 260 3600
Fax- +358 14 260 3611

24.67.186.244	4760

Shaw Fiberlink ltd. (NETBLK-FIBERLINK-CABLE)
630 3rd Avenue SW, Suite 900
Calgary AB, 4L4
CA
Netname: FIBERLINK-CABLE
Netblock: 24.64.0.0 - 24.71.255.255
Maintainer: FBCA
Coordinator:
Shaw@Home (SH2-ORG-ARIN) internet.abuse@SHAW.CA
(403) 750-7420

132.235.177.123	4419

Ohio University (NET-OHIOU-NET)
Ohio University - Communications Network Services
Athens, OH 45701-2979
US
Netname: OHIOU-NET
Netblock: 132.235.0.0 - 132.235.255.255
Coordinator:
Watkins, Robert B. (RBW-ARIN) watkins1@OHIOU.EDU
(740)-593-1212 (FAX) (740)-593-1944

169.197.49.83	3603

TUCSON NEWSPAPERS (NET-TNIB)
4850 S. PARK AVE.
TUCSON, AZ 85719
US
Netname: TNIB
Netblock: 169.197.0.0 - 169.197.63.255
Coordinator:
Operations Center, AzStarNet Network (AN320-ARIN) noc@AZSTARNET.COM
520-573-4220 (FAX) 520-573-4268
[snipped]
Record last updated on 16-Mar-1999.
Database last updated on 27-Jun-2001 23:01:38 EDT.

65.1.199.105	1642

Source of whois:
http://www.incidents.org/cid/ipinfo.php?ip=65.0.101.209

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

65.0.101.209
HostName: c1442566-a.sttln1.wa.home.com
Whois: @Home Network (NETBLK-HOME-3BLK)HOME-3BLK 65.0.0.0 - 65.15.255.255
@Home Network (NETBLK-STTLWA1-WA-7) STTLWA1-WA-7 65.0.96.0 - 65.0.110.255
[snipped]

24.129.200.234	15

Source of whois:
http://www.samspade.org/

Continental Cablevision of Jacksonville (JACKSONVILLE2-DOM)
5934 Richard Street
Jacksonville, FL 32216
Domain Name: JACKSONVILLE.NET

[SNIPPED]

Technical Contact:
Domain Contact (DC1660-ORG) domain@SE.MEDIAONE.NET
AT&T Broadband Business Internet Services
5934 Richard St.
Jacksonville, FL 32216
US

904 680 2638

Fax- 904 374 8410
Record last updated on 12-Apr-2001.
Record expires on 11-Apr-2005.

Scan Specific Activities

These are scans that have become the background noise of the Internet. A few specialized scans are handled as precursors to intrusions as show below.

Src-Dst Subnet16 IP Count of Top 20

MY.NET-MY.NET	13512
169.226-MY.NET	12129
206.112-MY.NET	9992
130.234-MY.NET	9446
MY.NET-213.83	7063
[snipped]	
TOTAL	526338

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

MY.NET.229.154	19785
MY.NET.70.38	13513

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.227.254	12682
169.226.202.234	12129
MY.NET.228.214	10005
[snipped]	
TOTAL	526338

Source Port Count of Top 20

27888	77203
28800	25739
13139	24269
21	23435
0	21734
[snipped]	
TOTAL	526338

Destination Subnet16 IP Count of Top 20
[snipped]
Destination Subnet24 IP Count of Top 20
[snipped]

Destination IP Count of Top 20

MY.NET.160.109	9994
169.197.49.83	3603
[snipped]	
TOTAL	526338

Destination Port Count of Top 20

28800	26044
7778	25326
21	23994
13139	22601
0	21583
[snipped]	20251
TOTAL	526338

Messages (All)

UDP	441741
SYN **S*****	54275
SYNFIN **SF****	21411
XMAS ***F*P*U	4995
SYN 21S***** RESERVEDBITS	687
NULL ********	268
[snipped]	

SYN Scan Details

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

These scans have traditionally been used to avoid network defenses, but are now commonly trapped and dropped by properly configured routers and firewalls.

Src-Dst Subnet16 IP Count of Top 20

169.226-MY.NET	12129
130.234-MY.NET	9446
MY.NET-MY.NET	5228
24.67-MY.NET	4760
[snipped]	
TOTAL	76452

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

169.226.202.234	12129
130.234.184.112	9446
MY.NET.70.38	5228
24.67.186.244	4760
132.235.177.123	4419
[snipped]	
TOTAL	76452

Source Port Count of Top 20

21	23431
36338	4157
54321	1392
53	660
[snipped]	
TOTAL	76452

Destination Subnet16 IP Count of Top 20
[snipped]
Destination Subnet24 IP Count of Top 20
[snipped]

Destination IP Count of Top 20

24.3.45.174	1538
208.231.55.57	1446
216.240.241.70	1321
129.21.131.101	906
[snipped]	
TOTAL	76452

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Destination Port Count of Top 20

21	23980
53	11141
6346	6864
27374	5346
1214	3354
23	2114
25	2010
8888	1663
54321	1392
2100	924
111	823
2000	706
6355	629
6347	362
3100	329
113	190
13720	189
59	144
2340	83
All_Other	14209
TOTAL	76452

Messages (All)

SYN **S*****	54275
SYNFIN **SF****	21411
SYN 21S***** RESERVEDBITS	687
SYNFIN 21SF**** RESERVEDBITS	25
SYNFIN *1SF**** RESERVEDBITS	18
SYN *1S***** RESERVEDBITS	18
SYNFIN 2*SF**** RESERVEDBITS	15
SYN 2*S***** RESERVEDBITS	3

FULL_XMAS Details

This scaning technique has a clearly hostile signature as there is no "normal"occurance within the guidelines of the networking practice.

Src-Dst Subnet16 IP Count of Top 20

MY.NET-24.129,	15
MY.NET-128.255,	13
MY.NET-24.66,	5
MY.NET-65.80,	3
MY.NET-64.160,	3
MY.NET-24.68,	3
MY.NET-24.43,	3
MY.NET-207.172,	3
MY.NET-64.108,	2
MY.NET-66.1,	1
MY.NET-64.229,	1
MY.NET-64.228,	1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET-62.225,	1
MY.NET-24.71,	1
MY.NET-24.64,	1
MY.NET-24.159,	1
MY.NET-216.78,	1
MY.NET-213.73,	1
MY.NET-212.161,	1
All_Other	9
TOTAL,	69

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

MY.NET.217.150	63
66.20.28.21	1
65.26.247.13	1
62.142.204.31	1
213.89.88.29	1
208.59.31.50	1
169.229.55.6	1
All_Other	
TOTAL	69

Source Port Count of Top 20
[snipped]
Destination Subnet24 IP Count of Top 20
[snipped]

Destination IP Count of Top 10

24.129.200.234	15
128.255.203.6	13
24.66.57.35	5
[snipped]	
62.225.225.74	1
All_Other	9
TOTAL	69

Destination Port Count of Top 20

2340	11
1874	11
2666	8
2572	3
[snipped]	2
2376	1
All_Other	18
TOTAL	69

Messages (All)

FULLXMAS 21SFRPAU RESERVEDBITS	33

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FULLXMAS **SFRPAU	19
FULLXMAS 2*SFRPAU RESERVEDBITS	14
FULLXMAS *1SFRPAU RESERVEDBITS	3

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX A – MY.NET Detailed Analysis

Src-Dst Subnet16 IP Count of Top 20

212.179-MY.NET	16378
130.234-MY.NET	9337
MY.NET-MY.NET	2917
24.67-MY.NET	2439
211.248-MY.NET	2216
MY.NET-24.67	1309
128.61-MY.NET	1162
128.46-MY.NET	1140
128.138-MY.NET	729
MY.NET-128.138	553
64.244-MY.NET	362
MY.NET-148.129	322
141.30-MY.NET	274
MY.NET-208.5	244
148.129-MY.NET	210
MY.NET-216.181	118
159.226-MY.NET	92
208.5-MY.NET	72
All_Other	2092
TOTAL	42196

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

130.234.184.112	9336
212.179.21.179	4372
212.179.41.169	4061
24.67.186.244	2438
MY.NET.70.38	2379
211.248.112.67	2216
212.179.33.82	1599
212.179.125.114	1444
128.61.136.233	1159
128.46.156.197	1140
212.179.72.226	791
128.138.2.112	728
212.179.79.2	720
MY.NET.201.146	553
212.179.47.83	544
MY.NET.253.12	530
212.179.58.193	520
212.179.44.62	441
212.179.29.250	414
All_Other	6811
TOTAL	42196

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Source Port Count of Top 20

21	10494
1172	4373
1113	4061
27374	2619
36339	2379
53	2222
63891	1246
26835	791
12708	651
137	580
4781	555
1572	544
2226	521
21304	436
12693	412
1546	409
7777	362
23	322
63255	304
All_Other	8915
TOTAL	42196

Destination Subnet16 IP Count of Top 20
[snipped]
Destination Subnet24 IP Count of Top 20
[snipped]

Destination IP Count of Top 20

MY.NET.207.226	4372
MY.NET.213.250	4069
MY.NET.209.114	1599
MY.NET.207.126	1451
24.67.186.244	1309
MY.NET.100.99	872
MY.NET.220.42	792
MY.NET.201.146	730
128.138.2.112	553
MY.NET.204.22	546
MY.NET.224.34	522
MY.NET.210.34	436
MY.NET.217.98	415
MY.NET.217.42	413
MY.NET.225.50	407
MY.NET.223.254	362
148.129.143.2	322
MY.NET.225.186	306
All_Other	22490
TOTAL	42196

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Destination Port Count of Top 20

21	10496
6688	7333
6699	5923
27374	4414
53	2241
4718	1451
161	1147
4781	730
6346	693
137	608
41003	437
32771	423
4222	415
1080	411
23	210
4971	156
515	135
4116	110
All_Other	4747
TOTAL	42196

Messages (All)

Watchlist 000220 IL-ISDNNET-990517	16378
SYN-FIN scan!	12716
Possible RAMEN server activity	7033
NMAP TCP ping!	2408
SNMP public access	1147
SMB Nae Wildcard	608
Queso fingerprint	463
WinGate 1080 Attept	411
Attepted Sun RPC high port access	409
Tiny Fragents - Possible Hostile Activity	230
connect to 515 fro inside	135
Null scan!	110
Watchlist 000222 NET-NCFC	92
Back Orifice	25
SUNRPC highport access!	14
External RPC call	5
TCP SMTP Source Port traffic	4
Security 000516-1	4
Probable NMAP fingerprint attept	2
SITE EXEC - Possible wu-ftpd exploit - GIAC000623	1
Russia Dynao - SANS Flash 28-jul-00	1

More detailed analysis of "interesting" material developed above

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detailed Analysis of NULL Scan

Src-Dst Subnet16 IP Count of Top 20

64.48-MY.NET	6
63.253-MY.NET	6
24.201-MY.NET	6
62.137-MY.NET	5
209.255-MY.NET	5
63.252-MY.NET	4
131.155-MY.NET	4
63.91-MY.NET	3
65.0-MY.NET	2
64.196-MY.NET	2
63.255-MY.NET	2
62.59-MY.NET	2
24.9-MY.NET	2
24.200-MY.NET	2
24.180-MY.NET	2
24.156-MY.NET	2
24.141-MY.NET	2
24.10-MY.NET	2
212.232-MY.NET	2
All_Other	49
TOTAL	110

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]
Source IP Count of Top 20
[snipped]
Source Port Count of Top 20
[snipped]

Destination Subnet16 IP Count of Top 20

MY.NET	110
All_Other	
TOTAL	110

Destination Subnet24 IP Count of Top 20
[snipped]
Destination IP Count of Top 20
[snipped]
Destination Port Count of Top 20
[snipped]

Messages (All)

Null scan!	110

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detailed Analysis of RAMEN

Src-Dst Subnet16 IP Count of Top 20

24.67-MY.NET	2438
MY.NET-24.67	1309
128.138-MY.NET	728
MY.NET-128.138	553
MY.NET-MY.NET	531
MY.NET-148.129	322
MY.NET-208.5	244
148.129-MY.NET	210
208.5-MY.NET	70
MY.NET-208.169	45
MY.NET-217.52	39
MY.NET-24.180	18
208.169-MY.NET	18
MY.NET-24.48	15
MY.NET-209.130	15
24.48-MY.NET	14
MY.NET-24.169	13
MY.NET-24.23	10
MY.NET-217.80	10
All_Other	431
TOTAL	7033

Source Subnet16 IP Count of Top 20
[snipped]

Source Subnet24 IP Count of Top 20

24.67.186	2438
128.138.2	728
MY.NET.201	604
MY.NET.253	537
MY.NET.97	364
MY.NET.60	351
148.129.143	210
MY.NET.225	74
208.5.8	70
MY.NET.217	61
MY.NET.223	56
MY.NET.200	48
MY.NET.222	45
MY.NET.98	40
MY.NET.227	40
MY.NET.226	39
MY.NET.209	39
MY.NET.204	39
MY.NET.207	37
All_Other	1213
TOTAL	7033

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Source IP Count of Top 20

24.67.186.244	2438
128.138.2.112	728
MY.NET.201.146	553
MY.NET.253.12	530
MY.NET.97.154	330
MY.NET.60.11	326
148.129.143.2	210
MY.NET.225.66	57
MY.NET.217.202	30
MY.NET.223.42	20
MY.NET.227.94	16
24.48.121.105	13
MY.NET.60.8	12
MY.NET.97.61	11
MY.NET.201.242	10
134.29.48.235	10
24.180.160.210	9
203.79.69.182	9
203.106.99.237	8
All_Other	1713
TOTAL	7033

Source Port Count of Top 20

27374	2619
4781	554
23	322
2154	8
1494	6
4268	5
3288	5
2878	5
1347	5
4814	4
4612	4
4330	4
4217	4
4184	4
4120	4
4088	4
3244	4
3117	4
3064	4
All_Other	3464
TOTAL	7033

Destination Subnet16 IP Count of Top 20
[snipped]
Destination Subnet24 IP Count of Top 20
[snipped]

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Destination IP Count of Top 20

24.67.186.244	1309
MY.NET.201.146	728
128.138.2.112	553
148.129.143.2	322
MY.NET.60.11	211
MY.NET.97.154	93
MY.NET.225.66	36
MY.NET.217.202	21
24.180.160.210	18
24.48.121.105	15
MY.NET.227.94	13
24.169.221.72	13
209.130.161.33	12
24.23.131.82	10
217.80.182.238	10
203.79.69.182	10
203.106.99.237	10
64.231.218.26	9
208.5.8.169	9
All_Other	3631
TOTAL	7033

Destination Port Count of Top 20

27374	4414
4781	730
23	210
2154	6
1871	6
3764	5
4189	4
4026	4
3440	4
3014	4
2753	4
2732	4
2412	4
1902	4
1810	4
1338	4
110	4
4970	3
4870	3
All_Other	1612
TOTAL	7033

Messages (All)

Possible RAMEN server activity	7033

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detailed Analysis of SYN-FIN

Src-Dst Subnet16 IP Count of Top 20

130.234-MY.NET	9336
211.248-MY.NET	2216
128.61-MY.NET	1158
63.252-MY.NET	2
66.25-MY.NET	1
24.50-MY.NET	1
209.255-MY.NET	1
128.206-MY.NET	1
All_Other	
TOTAL	12716

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

130.234.184.112	9336
211.248.112.67	2216
128.61.136.233	1158
63.252.15.242	2
66.25.174.123	1
24.50.25.5	1
209.255.180.130	1
128.206.176.25	1
All_Other	
TOTAL	12716

Source Port Count of Top 20

21	10494
53	2216
2754	2
6699	1
6688	1
32808	1
2474	1
All_Other	
TOTAL	12716

Destination Subnet16 IP Count of Top 20

MY.NET	12716
All_Other	
TOTAL	12716

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Destination Subnet24 IP Count of Top 20
[snipped]
Destination IP Count of Top 20
[snipped]

Destination Port Count of Top 20

21	10494
53	2216
443	2
412	1
259	1
1700	1
1415	1
All_Other	
TOTAL	12716

Messages (All)

SYN-FIN scan!	12716

Detailed Analysis of WATCHLIST

Src-Dst Subnet16 IP Count of Top 20

212.179-MY.NET	16378
159.226-MY.NET	92
All_Other	
TOTAL	16470

Source Subnet16 IP Count of Top 20
[snipped]
Source Subnet24 IP Count of Top 20
[snipped]

Source IP Count of Top 20

212.179.21.179	4372
212.179.41.169	4061
212.179.33.82	1599
212.179.125.114	1444
212.179.72.226	791
212.179.79.2	720
212.179.47.83	544
212.179.58.193	520
212.179.44.62	441
212.179.29.250	414
212.179.41.14	407
212.179.40.132	398
212.179.27.6	187
212.179.95.5	159
212.179.72.163	142
212.179.8.165	72
159.226.39.4	35

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

212.179.41.220	30
159.226.210.6	10
All_Other	124
TOTAL	16470

```
Source Port Count of Top 20
     [snipped]
Destination Subnet16 IP Count of Top 20
     [snipped]
Destination Subnet24 IP Count of Top 20
     [snipped]
Destination IP Count of Top 20
     [snipped]
Destination Port Count of Top 20
     [snipped]
```

Messages (All)

Watchlist 000220 IL-ISDNNET-990517	16378
Watchlist 000222 NET-NCFC	92

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX B – Traffic Breakout

1. Validate data for date/time, rejecting all data with invalid date range.

The following traffic has invalid dates (Year 2000).
REJECT.DIR

```
-r-x------    1 root     root       189782 Jun  9 20:44 OOSche24.txt
-r-x------    1 root     root       110188 Jun  9 20:44 OOSche26.txt
-r-x------    1 root     root       112312 Jun  9 20:44 OOSche28.txt
-r-x------    1 root     root      4993461 Jun  9 20:44 SnortA25.txt
-r-x------    1 root     root      5081154 Jun  9 20:44 SnortS27.txt
-rw-rw-rw-    1 root     root      2115215 Mar 15 21:28 UMBCNI25.txt
-r-x------    1 root     root      2513718 Jun  9 20:44 UMBCNI32.txt
-r-x------    1 root     root       264078 Jun  9 20:44 UMBCNI33.txt
-r-x------    1 root     root       572102 Jun  9 20:44 UMBCNI34.txt
-rw-rw-rw-    1 root     root      2282216 Mar 15 21:30 UMBCNI35.txt
-r-x------    1 root     root      4956801 Jun  9 20:44 UMBCNI3.txt
-rw-rw-rw-    1 root     root      1538514 Mar 15 21:32 UMBCNI43.txt
-rw-rw-rw-    1 root     root      2006106 Mar 15 21:32 UMBCNI44.txt
-rw-rw-rw-    1 root     root      1100513 Mar 15 21:33 UMBCNI45.txt
-r-x------    1 root     root      4078061 Jun  9 20:44 UMBCNI4.txt
-rw-rw-rw-    1 root     root      2712052 Mar 15 21:34 UMBCNI53.txt
-rw-rw-rw-    1 root     root      2824253 Mar 15 21:34 UMBCNI54.txt
-rw-rw-rw-    1 root     root      2131339 Mar 15 21:34 UMBCNI55.txt
-r-x------    1 root     root      4956801 Jun  9 20:44 UMBCNI5.txt
```

2. Separate raw data into type of activity, Alerts, Out of Specification, and Scan.

```
      Grep "Alert" *.txt > alert.lst
      Grep "OOS" *.txt > oos.lst
      Grep "Spp" *.txt > scan.lst
```

Using the list move the text files to the proper subdirectory for further analysis.

ALERT.DIR

```
-r-x------    1 root     root      2824253 Jun  9 20:44 UMBCNI54.txt
-r-x------    1 root     root      3110599 Mar 15 21:38 UMBCNI28.txt
-r-x------    1 root     root      4594904 Mar 15 21:35 UMBCNI60.txt
-r-x------    1 root     root      3704507 Mar 15 21:35 UMBCNI58.txt
-r-x------    1 root     root      4940025 Mar 15 21:34 UMBCNI52.txt
-r-x------    1 root     root      3815788 Mar 15 21:32 UMBCNI41.txt
-r-x------    1 root     root      4929935 Mar 15 21:31 UMBCNI39.txt
-r-x------    1 root     root      2963121 Mar 15 21:29 UMBCNI30.txt
-r-x------    1 root     root      4502134 Mar 15 21:29 UMBCNI27.txt
-r-x------    1 root     root      4492808 Mar 15 21:27 SnortA36.txt
-r-x------    1 root     root      4492808 Mar 15 21:27 SnortA35.txt
-r-x------    1 root     root      3493605 Mar 15 21:20 SnortA6.txt
-r-x------    1 root     root      4584151 Mar 15 21:20 SnortA3.txt
-r-x------    1 root     root      5257424 Mar 15 21:19 SnortAle.txt
```

OOS.DIR

```
-r-x------    1 root     root      3350885 Mar 15 21:29 OOSche29.txt
-r-x------    1 root     root        62968 Mar 15 21:25 OOSche30.txt
-r-x------    1 root     root       495502 Mar 15 21:26 OOSche31.txt
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
-r-x------    1 root     root       398812 Mar 15 21:30 OOSche32.txt
-r-x------    1 root     root       383059 Mar 15 21:26 OOSche33.txt
-r-x------    1 root     root        58863 Mar 15 21:30 OOSche34.txt
-r-x------    1 root     root        50702 Mar 15 21:20 OOSche4.txt
-r-x------    1 root     root       109071 Mar 15 21:20 OOSche5.txt
-r-x------    1 root     root        60542 Mar 15 21:20 OOScheck.txt
-r-x------    1 root     root        54302 Mar 15 21:31 UMBCNI37.txt
-r-x------    1 root     root        86160 Mar 15 21:31 UMBCNI38.txt
-r-x------    1 root     root       842288 Mar 15 21:32 UMBCNI42.txt
-r-x------    1 root     root      1100513 Jun  9 20:44 UMBCNI45.txt
-r-x------    1 root     root       472338 Mar 15 21:33 UMBCNI48.txt
-r-x------    1 root     root       310258 Mar 15 21:33 UMBCNI49.txt
-r-x------    1 root     root       503828 Mar 15 21:34 UMBCNI50.txt
-r-x------    1 root     root        62057 Mar 15 21:35 UMBCNI56.txt

SCAN.DIR
-r-x------    1 root     root      4116547 Mar 15 21:29 SnortS26.txt
-r-x------    1 root     root      3917789 Mar 15 21:25 SnortS29.txt
-r-x------    1 root     root      4121627 Mar 15 21:19 SnortS2.txt
-r-x------    1 root     root      4156462 Mar 15 21:26 SnortS32.txt
-r-x------    1 root     root      3002771 Mar 15 21:26 SnortS34.txt
-r-x------    1 root     root      3432816 Mar 15 21:21 SnortS7.txt
-r-x------    1 root     root      3472005 Mar 15 21:21 SnortS8.txt
-r-x------    1 root     root      2849102 Mar 15 21:19 SnortSca.txt
-r-x------    1 root     root      2115215 Jun  9 20:44 UMBCNI25.txt
-r-x------    1 root     root      3482517 Mar 15 21:36 UMBCNI26.txt
-r-x------    1 root     root      1411882 Mar 15 21:37 UMBCNI29.txt
-r-x------    1 root     root      2269971 Mar 15 21:22 UMBCNI2.txt
-r-x------    1 root     root      2115215 Mar 15 21:30 UMBCNI31.txt
-r-x------    1 root     root      2282216 Jun  9 20:44 UMBCNI35.txt
-r-x------    1 root     root      1556558 Mar 15 21:30 UMBCNI36.txt
-r-x------    1 root     root      1752326 Mar 15 21:31 UMBCNI40.txt
-r-x------    1 root     root      1538514 Jun  9 20:44 UMBCNI43.txt
-r-x------    1 root     root      2006106 Jun  9 20:44 UMBCNI44.txt
-r-x------    1 root     root      2293842 Mar 15 21:33 UMBCNI46.txt
-r-x------    1 root     root      2024673 Mar 15 21:33 UMBCNI47.txt
-r-x------    1 root     root      2030502 Mar 15 21:34 UMBCNI51.txt
-r-x------    1 root     root      2712052 Jun  9 20:44 UMBCNI53.txt
-r-x------    1 root     root      2131339 Jun  9 20:44 UMBCNI55.txt
-r-x------    1 root     root      3652061 Mar 15 21:35 UMBCNI57.txt
-r-x------    1 root     root      1825860 Mar 15 21:35 UMBCNI59.txt
-r-x------    1 root     root      3134240 Mar 15 21:36 UMBCNI61.txt
```

3. By Activity (Scan, Alert, OOS) process the data from original form to "normal" form for further processing and reporting using R2a shell script.

4. Generate first level analysis by activity using Q2a shell script.

5. If interesting traffic has merit, use "grep" command scripts to extract subset of the data to subdirectory for more detailed processing.
   Grep "RMAN" *.txt > rman/new_cnt
   Cd rman
   ../Q2a
6. Review the rpt_all.txt output for more detailed analysis and indicators.

7. Review the current Top10 list from Sans.org to establish the priority for analysis and countermeasure development.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX C – Data Reduction Tools (AWK)

```
##########################################################
# P2a   prescan to remove invalid dated files and
#       estimate the noise level of the raw data
#
# amm/8jun01
#  desc :
#
#    within subdirectory (source) loop
#      for each file *.txt
#        remove noise
#      output to noise.cnt
#     end loop
#
##########################################################
# clear out old
rm -f  src_* dst_* report* noise*

for x in `ls *.txt`
do
# Preprocess for portscan, Tiny Fragments, and ICMP SRC alerts
#
gawk '{  ++cnt
      gsub(/\m/,"")
        gsub(/\r/,"")

      if (($1 ~/Subject:/)&&($0 ~/2000/)) {
            print FILENAME "," $0", "
                ++invalid_date
               next }
      if ($0 ~ /^$/) {
            next }
        if ($0 ~ /spp_portscan/) {
            ++portscan
            next}
        if ($0 ~ /Tiny/) {
            ++frag
            next}
        if ($0 ~ /ICMP/) {
            ++icmp
            next}
}
END {                        print FILENAME ", Record Count , " cnt
     if (invalid_date > 0) { print FILENAME ", Invalid Date , " invalid_date}
     if (portscan > 0)     { print FILENAME ", spp_portscan , " portscan}
     if (frag > 0)         { print FILENAME ", Tiny Fragments, " frag}
     if (icmp > 0)         { print FILENAME ", ICMP SRC     , " icmp}
}' $x  >> noise_cnt
done

gawk  ' BEGIN{FS=","}
{       if ($2 ~/Record Count/)   { cnt+=$3}
      if ($2 ~/Invalid Date/)   { ++invalid_year ; badyear[NR] = $1 }
        if ($2 ~/spp_portscan/)   { portscan+=$3}
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
        if ($2 ~/Tiny/)           { frag+=$3}
        if ($2 ~/ICMP/)           { icmp+=$3}
}

END { print "\n\tPre-scan Results for Noise Items\n"
      print "\t\t Invalid Year on File Header\t" invalid_year
      print "\t\t spp_portscan               \t" portscan
      print "\t\t Tiny Fragents              \t" frag
      print "\t\t ICMP SRC                   \t" icmp
      print "\t\t   TOTAL RECORD COUNT                   \t" cnt

      if ( invalid_year > 0 ) {
      print "\nNote: There are " invalid_year " files that have an INVALID
date"
      print "[ 2000 for the year ] that will probably compromise any legal
actions"
      print "and reduce the credibility of the Intrusion Analyst effort."
      print "\nThese file should be manually removed from the 'raw' directory
before"
      print "proceding with the Analysis and Reporting of the data.\n"
      for (fn in badyear)
            printf("%s\t  ", badyear[fn])
      }
      print "\n\n"
}'  < x


##########################################################
# P2a   prescan to remove invalid dated files and
#       estimate the noise level of the raw data
#
# amm/8jun01
#  desc :
#
#    within subdirectory (source) loop
#      for each file *.txt
#        remove noise
#      output to noise.cnt
#     end loop
#
##########################################################
# clear out old
rm -f  src_* dst_* report* noise*

for x in `ls raw/*.txt`
do
# Preprocess for portscan, Tiny Fragments, and ICMP SRC alerts
#
gawk '{  ++cnt
      gsub(/\m/,"")
        gsub(/\r/,"")

      if (($1 ~/Subject:/)&&($0 ~/2000/)) {
            print FILENAME "," $0", "
                ++invalid_date
               next }
      if ($0 ~ /^$/) {
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
            next }
        if ($0 ~ /spp_portscan/) {
            ++portscan
            next}
        if ($0 ~ /Tiny/) {
            ++frag
            next}
        if ($0 ~ /ICMP/) {
            ++icmp
            next}
}
END {                        print FILENAME ", Record Count , " cnt
     if (invalid_date > 0) { print FILENAME ", Invalid Date , " invalid_date}
     if (portscan > 0)     { print FILENAME ", spp_portscan , " portscan}
     if (frag > 0)         { print FILENAME ", Tiny Fragments, " frag}
     if (icmp > 0)         { print FILENAME ", ICMP SRC     , " icmp}
}' $x  >> noise_cnt
done

gawk  ' BEGIN{FS=","}
{       if ($2 ~/Record Count/)   { cnt+=$3}
      if ($2 ~/Invalid Date/)   { ++invalid_year ; badyear[NR] = $1 }
        if ($2 ~/spp_portscan/)   { portscan+=$3}
        if ($2 ~/Tiny/)           { frag+=$3}
        if ($2 ~/ICMP/)           { icmp+=$3}
}

END { print "\n\tPre-scan Results for Noise Items\n"
      print "\t\t Invalid Year on File Header\t" invalid_year
      print "\t\t spp_portscan               \t" portscan
      print "\t\t Tiny Fragents              \t" frag
      print "\t\t ICMP SRC                   \t" icmp
      print "\t\t   TOTAL RECORD COUNT                   \t" cnt

      if ( invalid_year > 0 ) {
      print "\nNote: There are " invalid_year " files that have an INVALID
date"
      print "[ 2000 for the year ] that will probably compromise any legal
actions"
      print "and reduce the credibility of the Intrusion Analyst effort."
      print "\nThese file should be manually removed from the 'raw' directory
before"
      print "proceding with the Analysis and Reporting of the data.\n"
      for (fn in badyear)
            printf("%s\t  ", badyear[fn])
      }
      print "\n\n"
}'  noise_cnt

#########################################################
# Q1
#   amm/8jun01
#   counts on src_ip, src_port, dst_ip, dst_port
#   desc :
#     loop
#         on (item.. src_ip) sum to array
#     end loop
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#         print
#         src_ip (col 3/4/5/6)  count
#     end loop
#########################################################
  rm -f src_* dst_* msg_* rep_*
#
#  Source-Destination IP (col 4 and 6) subnet /16
#
gawk 'BEGIN{FS=","} {
      split($4,a,".")
      split($6,b,".")
      subnet=a[1]"."a[2]"-"b[1]"."b[2]
      ++hits[subnet]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1  > src-dst_subnet16.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other       " othr
      print "TOTAL,                 " totl
}' src-dst_subnet16.cnt >  src-dst_subnet16.lst

#
#  Source IP (col 4) subnet /16
#
gawk 'BEGIN{FS=","} {
      split($4,a,".")
      subnet=a[1]"."a[2]
      ++hits[subnet]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1  > src_subnet16.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "TOTAL,                  " totl
}' src_subnet16.cnt > src_subnet16.lst
#
#  Source IP (col 4) subnet /24
#
gawk 'BEGIN{FS=","} {
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
      split($4,a,".")
      subnet=a[1]"."a[2]"."a[3]
      ++hits[subnet]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1 > src_subnet24.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' src_subnet24.cnt > src_subnet24.lst
#
# Source IP/32 (col 4)
#
gawk 'BEGIN{FS=","} {
      ++hits[$4]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1  > src_ip.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' src_ip.cnt > src_ip.lst
#
# Source Port (col 5)
#
gawk 'BEGIN{FS=","} {
      ++hits[$5]
}
END { for (port in hits)
        print port ",\t" hits[port]
}' new_cnt | sort -gr  +1  > src_port.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' src_port.cnt > src_port.lst

#
# Destination IP (col 6) subnet /16
#
 gawk 'BEGIN{FS=","} {
      split($6,a,".")
      subnet=a[1]"."a[2]
      ++hits[subnet]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1  > dst_subnet16.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' dst_subnet16.cnt > dst_subnet16.lst
#
#  Destination IP (col 4) subnet /24
#
gawk 'BEGIN{FS=","} {
      split($6,a,".")
      subnet=a[1]"."a[2]"."a[3]
      ++hits[subnet]
}
END { for (ip in hits)
        print ip ",\t", hits[ip]
}' new_cnt | sort -gr  +1  > dst_subnet24.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' dst_subnet24.cnt > dst_subnet24.lst
#
# Destination IP (col 6)
#
gawk 'BEGIN{FS=","} {
      ++hits[$6]
}
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
END { for (ip in hits)
        print ip ",\t" hits[ip]
}' new_cnt | sort -gr  +1  > dst_ip.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL,       " totl
}' dst_ip.cnt > dst_ip.lst
#
# Destination Port (col 7)
#
gawk 'BEGIN{FS=","} {
      ++hits[$7]
}
END { for (port in hits)
        print port ",\t" hits[port]
}' new_cnt | sort -gr  +1  > dst_port.cnt
#
#  consolidate report for final report
#
gawk '{
    if(NR < 20) {print $0}
    if (NR >=20) { othr+=$2 }
    totl+=$2
}
END {
      print "All_Other,       " othr
      print "          TOTAL ,      " totl
}' dst_port.cnt > dst_port.lst
#
# Warning Messages (col 8) Print ALL Messages
#
gawk  'BEGIN{FS=","}
{
    if (length($8) > 3) {
      ++hits[$8]      }
}
END { for (ln in hits)
        print ln,",",  hits[ln]
}' new_cnt  | sort -grt ,  +1   > msg_all.cnt

gawk 'BEGIN{FS=","}{printf("%-55s\t%10d\n",$1, $2)}' msg_all.cnt >
msg_all.lst
   rm -f rpt_all.txt
echo " Src-Dst Subnet16 IP Count of Top 20" >> rpt_all.txt
head -21 src-dst_subnet16.lst >> rpt_all.txt
echo " Source Subnet16 IP Count of Top 20" >> rpt_all.txt
head -21 src_subnet16.lst >> rpt_all.txt
echo " Source Subnet24 IP Count of Top 20" >> rpt_all.txt
head -21 src_subnet24.lst >> rpt_all.txt
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
echo " Source IP Count of Top 20" >> rpt_all.txt
head -21 src_ip.lst >> rpt_all.txt
echo " Source Port Count of Top 20" >> rpt_all.txt
head -21 src_port.lst >> rpt_all.txt
echo " Destination Subnet16 IP Count of Top 20" >> rpt_all.txt
head -21 dst_subnet16.lst >> rpt_all.txt
echo " Destination Subnet24 IP Count of Top 20" >> rpt_all.txt
head -21 dst_subnet24.lst >> rpt_all.txt
echo " Destination IP Count of Top 20" >> rpt_all.txt
head -21 dst_ip.lst >> rpt_all.txt
echo " Destination Port Count of Top 20" >> rpt_all.txt
head -21 dst_port.lst >> rpt_all.txt
echo " Messages (All) " >> rpt_all.txt
cat  msg_all.lst >> rpt_all.txt

 more rpt_all.txt

##########################################################
# R2a
#
# amm/8jun01
#  desc :
#
#    within subdirectory (source) loop
#      for each file *.txt
#        remove noise
#      output to noise.cnt
#     end loop
#
#    within subdirectory (source) loop
#      for each file *.txt
#      if type3 [FEB 1 -HH:MM:SS.ssssss....]
#      if type2 [**] tttttt [**]
#      if type1 [01/01-HH:MM:SS:HHHHHH]
#         print filename   (col 0)  ymd (col 1) hms.ssssss (col 2)
#         src_ip (col 3) src_port (col 4) dst_ip (col 5) dst_port (col 6)
#         other_items (col 7)
#       endif
#     store output to new_cnt
#########################################################
# clear out old
rm -f new_cnt   noise_cnt
for x in `ls raw/*.txt`
do
#
# Process the pre_cnt for data extraction
#
gawk ' BEGIN{ monlst="JanFebMarAprMayJunJulAugSepOctNovDec" }
{
      gsub(/\m/,"")
        gsub(/\r/,"")
      if($0 ~/spp_portscan/) {next}
if($0 ~/^[A-Z][a-z][a-z] [0-9]/)
      {
       # log type 3
        m1=(index(monlst,$1)+2)/3
      if (m1 <10) {m1 = "0" m1}
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
        if ($2 < 10) { $2 = "0" $2 }
      src_ip   =substr($4,1,(index($4,":")-1))
      src_port =substr($4,(index($4,":")+1))
      dst_ip   =substr($6,1,(index($6,":")-1))
      dst_port =substr($6,(index($6,":")+1))
        pt1      =length($6)
      cmts     =substr($0,(index($0,$6)+pt1))
        print FILENAME","        \
      " 2001"                  \
      m1                       \
      $2              ","      \
      $3              ","      \
        src_ip          ","      \
        src_port        ","      \
      dst_ip          ","      \
        dst_port        ","      \
        cmts
      next
        }
if(( $0 ~/^[0-1][0-9]\/[0-3][0-9]\-[0-2][0-9]\:[0-5]/ ))
        {
      # snort alert logs
      gsub(/\[\*\*\]/,"_")
        split($0,a,"_")
        K=NF - 2
      src_ip   =substr($K,1,(index($K,":")-1))
      src_port =substr($K,(index($K,":")+1))
      dst_ip   =substr($NF,1,(index($NF,":")-1))
      dst_port =substr($NF,(index($NF,":")+1))
        print  FILENAME ","     \
      " 2001"                 \
      substr($1,1,2)          \
      substr($1,4,2) ","      \
      substr($1,7)   ","      \
        src_ip         ","      \
        src_port       ","      \
      dst_ip         ","      \
        dst_port       ","      \
        a[2]
      next
        }
if(($0 ~/^[0-1][0-9]\/[0-3][0-9]-/) && ( $0 !~ /[**]/))
      {
        print FILENAME ","                  \
      " 2001"                            \
      substr($1,1,2)                     \
      substr($1,4,2) ","                 \
      substr($1,7) ","                   \
        substr($2,1,(index($2,":")-1)) ","   \
      substr($2,(index($2,":")+1))   ","   \
        substr($4,1,(index($4,":")-1)) ","   \
      substr($4,(index($4,":")+1))
      next
      }
} ' $x  >> new_cnt
done
##########################################################################
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX D – Raw Trace Files For ASSIGNMENT 1

```
Trace 5
FWIN,2000/12/13,20:36:10 -5:00 GMT,147.208.171.139:0,MY.ISP.WINMILLER.179:0,ICMP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1782,MY.ISP.WINMILLER.179:21,TCP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1784,MY.ISP.WINMILLER.179:23,TCP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1786,MY.ISP.WINMILLER.179:25,TCP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1788,MY.ISP.WINMILLER.179:79,TCP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1790,MY.ISP.WINMILLER.179:80,TCP
FWIN,2000/12/13,20:36:28 -5:00 GMT,147.208.171.139:1792,MY.ISP.WINMILLER.179:110,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1794,MY.ISP.WINMILLER.179:113,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1796,MY.ISP.WINMILLER.179:119,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1798,MY.ISP.WINMILLER.179:139,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1800,MY.ISP.WINMILLER.179:143,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1802,MY.ISP.WINMILLER.179:443,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1804,MY.ISP.WINMILLER.179:445,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1806,MY.ISP.WINMILLER.179:1723,TCP
FWIN,2000/12/13,20:36:30 -5:00 GMT,147.208.171.139:1808,MY.ISP.WINMILLER.179:5631,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2146,MY.ISP.WINMILLER.179:21,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2148,MY.ISP.WINMILLER.179:23,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2150,MY.ISP.WINMILLER.179:25,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2152,MY.ISP.WINMILLER.179:79,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2154,MY.ISP.WINMILLER.179:80,TCP
FWIN,2000/12/13,20:37:00 -5:00 GMT,147.208.171.139:2156,MY.ISP.WINMILLER.179:110,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2158,MY.ISP.WINMILLER.179:113,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2160,MY.ISP.WINMILLER.179:119,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2162,MY.ISP.WINMILLER.179:139,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2164,MY.ISP.WINMILLER.179:143,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2166,MY.ISP.WINMILLER.179:443,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2168,MY.ISP.WINMILLER.179:445,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2170,MY.ISP.WINMILLER.179:1723,TCP
FWIN,2000/12/13,20:37:02 -5:00 GMT,147.208.171.139:2172,MY.ISP.WINMILLER.179:5631,TCP
FWIN,2000/12/13,20:37:34 -5:00 GMT,147.208.171.139:1417,MY.ISP.WINMILLER.179:137,UDP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3341,MY.ISP.WINMILLER.179:31,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3344,MY.ISP.WINMILLER.179:41,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3349,MY.ISP.WINMILLER.179:58,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3352,MY.ISP.WINMILLER.179:146,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3355,MY.ISP.WINMILLER.179:531,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3358,MY.ISP.WINMILLER.179:555,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3361,MY.ISP.WINMILLER.179:666,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3364,MY.ISP.WINMILLER.179:911,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3366,MY.ISP.WINMILLER.179:999,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3370,MY.ISP.WINMILLER.179:1001,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3373,MY.ISP.WINMILLER.179:1010,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3376,MY.ISP.WINMILLER.179:1011,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3379,MY.ISP.WINMILLER.179:1012,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3382,MY.ISP.WINMILLER.179:1015,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3385,MY.ISP.WINMILLER.179:1024,TCP
FWIN,2000/12/13,20:38:04 -5:00 GMT,147.208.171.139:3388,MY.ISP.WINMILLER.179:1042,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3391,MY.ISP.WINMILLER.179:1045,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3394,MY.ISP.WINMILLER.179:1090,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3397,MY.ISP.WINMILLER.179:1234,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3400,MY.ISP.WINMILLER.179:1243,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3403,MY.ISP.WINMILLER.179:1492,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3406,MY.ISP.WINMILLER.179:1600,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3409,MY.ISP.WINMILLER.179:1807,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3412,MY.ISP.WINMILLER.179:1981,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3415,MY.ISP.WINMILLER.179:1999,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3418,MY.ISP.WINMILLER.179:2000,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3421,MY.ISP.WINMILLER.179:2001,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3424,MY.ISP.WINMILLER.179:2002,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3427,MY.ISP.WINMILLER.179:2003,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3430,MY.ISP.WINMILLER.179:2004,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3433,MY.ISP.WINMILLER.179:2005,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3436,MY.ISP.WINMILLER.179:2023,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3439,MY.ISP.WINMILLER.179:2115,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3442,MY.ISP.WINMILLER.179:2140,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3445,MY.ISP.WINMILLER.179:2565,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3448,MY.ISP.WINMILLER.179:2583,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3451,MY.ISP.WINMILLER.179:2773,TCP
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3454,MY.ISP.WINMILLER.179:2774,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3457,MY.ISP.WINMILLER.179:2801,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3460,MY.ISP.WINMILLER.179:3024,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3463,MY.ISP.WINMILLER.179:3129,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3466,MY.ISP.WINMILLER.179:3150,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3469,MY.ISP.WINMILLER.179:3700,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3472,MY.ISP.WINMILLER.179:4092,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3475,MY.ISP.WINMILLER.179:4567,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3478,MY.ISP.WINMILLER.179:5000,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3481,MY.ISP.WINMILLER.179:5001,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3484,MY.ISP.WINMILLER.179:5321,TCP
FWIN,2000/12/13,20:38:06 -5:00 GMT,147.208.171.139:3487,MY.ISP.WINMILLER.179:5400,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3490,MY.ISP.WINMILLER.179:5401,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3493,MY.ISP.WINMILLER.179:5402,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3496,MY.ISP.WINMILLER.179:5555,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3499,MY.ISP.WINMILLER.179:5556,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3502,MY.ISP.WINMILLER.179:5557,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3505,MY.ISP.WINMILLER.179:5569,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3508,MY.ISP.WINMILLER.179:5742,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3511,MY.ISP.WINMILLER.179:6400,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3514,MY.ISP.WINMILLER.179:6670,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3517,MY.ISP.WINMILLER.179:6771,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3520,MY.ISP.WINMILLER.179:6776,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3523,MY.ISP.WINMILLER.179:6939,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3526,MY.ISP.WINMILLER.179:6969,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3529,MY.ISP.WINMILLER.179:6970,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3532,MY.ISP.WINMILLER.179:7000,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3535,MY.ISP.WINMILLER.179:7215,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3538,MY.ISP.WINMILLER.179:7300,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3541,MY.ISP.WINMILLER.179:7301,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3544,MY.ISP.WINMILLER.179:7306,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3547,MY.ISP.WINMILLER.179:7307,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3550,MY.ISP.WINMILLER.179:7308,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3553,MY.ISP.WINMILLER.179:7789,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3556,MY.ISP.WINMILLER.179:9872,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3559,MY.ISP.WINMILLER.179:9873,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3562,MY.ISP.WINMILLER.179:9874,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3565,MY.ISP.WINMILLER.179:9875,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3568,MY.ISP.WINMILLER.179:9989,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3571,MY.ISP.WINMILLER.179:10067,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3574,MY.ISP.WINMILLER.179:10167,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3577,MY.ISP.WINMILLER.179:10520,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3580,MY.ISP.WINMILLER.179:10607,TCP
FWIN,2000/12/13,20:38:08 -5:00 GMT,147.208.171.139:3583,MY.ISP.WINMILLER.179:11000,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3586,MY.ISP.WINMILLER.179:11223,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3589,MY.ISP.WINMILLER.179:12076,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3592,MY.ISP.WINMILLER.179:12223,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3596,MY.ISP.WINMILLER.179:12345,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3600,MY.ISP.WINMILLER.179:12346,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3604,MY.ISP.WINMILLER.179:12361,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3608,MY.ISP.WINMILLER.179:12362,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3612,MY.ISP.WINMILLER.179:12363,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3616,MY.ISP.WINMILLER.179:12631,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3620,MY.ISP.WINMILLER.179:13000,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3624,MY.ISP.WINMILLER.179:16959,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3628,MY.ISP.WINMILLER.179:20034,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3632,MY.ISP.WINMILLER.179:21554,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3636,MY.ISP.WINMILLER.179:22222,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3640,MY.ISP.WINMILLER.179:23456,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3644,MY.ISP.WINMILLER.179:23476,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3648,MY.ISP.WINMILLER.179:23477,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3651,MY.ISP.WINMILLER.179:26274,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3654,MY.ISP.WINMILLER.179:27374,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3657,MY.ISP.WINMILLER.179:30100,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3660,MY.ISP.WINMILLER.179:30101,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3663,MY.ISP.WINMILLER.179:30102,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3666,MY.ISP.WINMILLER.179:31337,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3669,MY.ISP.WINMILLER.179:31785,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3672,MY.ISP.WINMILLER.179:31787,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3675,MY.ISP.WINMILLER.179:31788,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3678,MY.ISP.WINMILLER.179:31789,TCP
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3680,MY.ISP.WINMILLER.179:31791,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3682,MY.ISP.WINMILLER.179:31792,TCP
FWIN,2000/12/13,20:38:10 -5:00 GMT,147.208.171.139:3684,MY.ISP.WINMILLER.179:40421,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3686,MY.ISP.WINMILLER.179:40422,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3688,MY.ISP.WINMILLER.179:40423,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3690,MY.ISP.WINMILLER.179:40426,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3692,MY.ISP.WINMILLER.179:54283,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3694,MY.ISP.WINMILLER.179:54320,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3696,MY.ISP.WINMILLER.179:54321,TCP
FWIN,2000/12/13,20:38:12 -5:00 GMT,147.208.171.139:3698,MY.ISP.WINMILLER.179:60000,TCP
FWIN,2000/12/13,20:38:42 -5:00 GMT,147.208.171.139:4727,MY.ISP.WINMILLER.179:31,TCP
FWIN,2000/12/13,20:38:42 -5:00 GMT,147.208.171.139:4729,MY.ISP.WINMILLER.179:41,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4731,MY.ISP.WINMILLER.179:58,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4733,MY.ISP.WINMILLER.179:146,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4735,MY.ISP.WINMILLER.179:531,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4737,MY.ISP.WINMILLER.179:555,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4739,MY.ISP.WINMILLER.179:666,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4741,MY.ISP.WINMILLER.179:911,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4743,MY.ISP.WINMILLER.179:999,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4745,MY.ISP.WINMILLER.179:1001,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4747,MY.ISP.WINMILLER.179:1010,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4749,MY.ISP.WINMILLER.179:1011,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4751,MY.ISP.WINMILLER.179:1012,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4753,MY.ISP.WINMILLER.179:1015,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4755,MY.ISP.WINMILLER.179:1024,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4757,MY.ISP.WINMILLER.179:1042,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4759,MY.ISP.WINMILLER.179:1045,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4761,MY.ISP.WINMILLER.179:1090,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4763,MY.ISP.WINMILLER.179:1234,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4765,MY.ISP.WINMILLER.179:1243,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4767,MY.ISP.WINMILLER.179:1492,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4769,MY.ISP.WINMILLER.179:1600,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4771,MY.ISP.WINMILLER.179:1807,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4773,MY.ISP.WINMILLER.179:1981,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4775,MY.ISP.WINMILLER.179:1999,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4777,MY.ISP.WINMILLER.179:2000,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4779,MY.ISP.WINMILLER.179:2001,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4781,MY.ISP.WINMILLER.179:2002,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4783,MY.ISP.WINMILLER.179:2003,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4785,MY.ISP.WINMILLER.179:2004,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4787,MY.ISP.WINMILLER.179:2005,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4789,MY.ISP.WINMILLER.179:2023,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4791,MY.ISP.WINMILLER.179:2115,TCP
FWIN,2000/12/13,20:38:44 -5:00 GMT,147.208.171.139:4793,MY.ISP.WINMILLER.179:2140,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4794,MY.ISP.WINMILLER.179:2565,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4797,MY.ISP.WINMILLER.179:2583,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4799,MY.ISP.WINMILLER.179:2773,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4801,MY.ISP.WINMILLER.179:2774,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4803,MY.ISP.WINMILLER.179:2801,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4805,MY.ISP.WINMILLER.179:3024,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4807,MY.ISP.WINMILLER.179:3129,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4809,MY.ISP.WINMILLER.179:3150,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4811,MY.ISP.WINMILLER.179:3700,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4813,MY.ISP.WINMILLER.179:4092,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4815,MY.ISP.WINMILLER.179:4567,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4817,MY.ISP.WINMILLER.179:5000,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4819,MY.ISP.WINMILLER.179:5001,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4821,MY.ISP.WINMILLER.179:5321,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4823,MY.ISP.WINMILLER.179:5400,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4825,MY.ISP.WINMILLER.179:5401,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4827,MY.ISP.WINMILLER.179:5402,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4829,MY.ISP.WINMILLER.179:5555,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4831,MY.ISP.WINMILLER.179:5556,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4833,MY.ISP.WINMILLER.179:5557,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4835,MY.ISP.WINMILLER.179:5569,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4837,MY.ISP.WINMILLER.179:5742,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4839,MY.ISP.WINMILLER.179:6400,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4841,MY.ISP.WINMILLER.179:6670,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4843,MY.ISP.WINMILLER.179:6771,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4845,MY.ISP.WINMILLER.179:6776,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4847,MY.ISP.WINMILLER.179:6939,TCP
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4849,MY.ISP.WINMILLER.179:6969,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4851,MY.ISP.WINMILLER.179:6970,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4853,MY.ISP.WINMILLER.179:7000,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4855,MY.ISP.WINMILLER.179:7215,TCP
FWIN,2000/12/13,20:38:46 -5:00 GMT,147.208.171.139:4857,MY.ISP.WINMILLER.179:7300,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4859,MY.ISP.WINMILLER.179:7301,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4861,MY.ISP.WINMILLER.179:7306,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4863,MY.ISP.WINMILLER.179:7307,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4865,MY.ISP.WINMILLER.179:7308,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4867,MY.ISP.WINMILLER.179:7789,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4869,MY.ISP.WINMILLER.179:9872,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4871,MY.ISP.WINMILLER.179:9873,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4873,MY.ISP.WINMILLER.179:9874,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4875,MY.ISP.WINMILLER.179:9875,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4877,MY.ISP.WINMILLER.179:9989,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4879,MY.ISP.WINMILLER.179:10067,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4881,MY.ISP.WINMILLER.179:10167,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4883,MY.ISP.WINMILLER.179:10520,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4885,MY.ISP.WINMILLER.179:10607,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4887,MY.ISP.WINMILLER.179:11000,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4889,MY.ISP.WINMILLER.179:11223,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4891,MY.ISP.WINMILLER.179:12076,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4893,MY.ISP.WINMILLER.179:12223,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4895,MY.ISP.WINMILLER.179:12345,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4897,MY.ISP.WINMILLER.179:12346,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4899,MY.ISP.WINMILLER.179:12361,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4901,MY.ISP.WINMILLER.179:12362,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4903,MY.ISP.WINMILLER.179:12363,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4905,MY.ISP.WINMILLER.179:12631,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4907,MY.ISP.WINMILLER.179:13000,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4909,MY.ISP.WINMILLER.179:16959,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4910,MY.ISP.WINMILLER.179:20034,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4913,MY.ISP.WINMILLER.179:21554,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4915,MY.ISP.WINMILLER.179:22222,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4917,MY.ISP.WINMILLER.179:23456,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4919,MY.ISP.WINMILLER.179:23476,TCP
FWIN,2000/12/13,20:38:48 -5:00 GMT,147.208.171.139:4921,MY.ISP.WINMILLER.179:23477,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4923,MY.ISP.WINMILLER.179:26274,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4925,MY.ISP.WINMILLER.179:27374,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4928,MY.ISP.WINMILLER.179:30100,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4931,MY.ISP.WINMILLER.179:30101,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4935,MY.ISP.WINMILLER.179:30102,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4936,MY.ISP.WINMILLER.179:31337,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4938,MY.ISP.WINMILLER.179:31785,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4941,MY.ISP.WINMILLER.179:31787,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4942,MY.ISP.WINMILLER.179:31788,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4944,MY.ISP.WINMILLER.179:31789,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4946,MY.ISP.WINMILLER.179:31791,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4948,MY.ISP.WINMILLER.179:31792,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4950,MY.ISP.WINMILLER.179:40421,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4953,MY.ISP.WINMILLER.179:40422,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4954,MY.ISP.WINMILLER.179:40423,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4957,MY.ISP.WINMILLER.179:40426,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4959,MY.ISP.WINMILLER.179:54283,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4961,MY.ISP.WINMILLER.179:54320,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4963,MY.ISP.WINMILLER.179:54321,TCP
FWIN,2000/12/13,20:38:50 -5:00 GMT,147.208.171.139:4964,MY.ISP.WINMILLER.179:60000,TCP
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 30th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, Switzerland	May 15, 2017 - May 20, 2017	Live Event
Mentor Session - SEC503	Oceanside, CA	May 29, 2017 - Jun 29, 2017	Mentor
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio Fall 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego Fall 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced