Global Information Assurance Certification Paper

GIAC Certified Intrusion Analyst (GCIA) Candidate

Wade Walker

SANS Network Security 2001, San Diego, CA

GCIA Practical Assignment – Version 3.0

Assignment 1 – Describe the State of Intrusion Detection

Event Correlation from Separate Systems
Challenges when Analyzing Events of Interest from Multiple Systems

Introduction

Detecting network intrusions is an integral part of an organization's overall security policy. There are many different types of systems that can be used to detect intrusions, including: network-based intrusion detection systems (NIDS), host-based intrusion detection systems (HIDS), packet sniffers, log files, and more. While an NIDS is sometimes implemented as an organization's sole solution for network intrusion detection, a comprehensive intrusion detection solution includes using these other, disparate systems. Using disparate systems for intrusion detection creates a model known as distributed intrusion detection system (DIDS).

One of the major hurdles of a DIDS system is event correlation. Correlating DIDS information is difficult since each system usually reports information in a unique manner. Obviously, correlating events and alerts is a key component when analyzing events with the DIDS model. Quite often in an intrusion, multiple systems will have "events of interest" (EOI) about the intrusion and these systems will generate alerts if configured to do so. It will then be necessary to correlate this information in order for the organization to make an informed decision regarding the possible intrusion.

Correlating events is one of the tasks that the IDWG (Intrusion Detection Working Group) has undertaken. The IDWG was developed to address numerous IDS-related issues, including event correlation. The IDWG has published a couple of

documents related to event correlation, “Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition” and “The Intrusion Detection Exchange Protocol (IDXP)”. Using the standards suggested by the IDWG, event correlation could be feasible in a DIDS environment.

Another key component of event correlation is having a naming convention for vulnerabilities. This task has been undertaken by The MITRE Corporation, a not-for-profit corporation working in the public interest, which has developed the Common Vulnerabilities and Exposures (CVE) dictionary “of standardized names for vulnerabilities and other information security exposures”.

Distributed Intrusion Detection System (DIDS)

Distributed Intrusion Detection Systems (DIDS) can be comprised of many different components depending on the organization’s financial and labor resources. A smaller organization’s DIDS may consist of web server logs and firewall logs. While this may not seem like a DIDS, this may be all that a smaller organization can afford.

Larger organizations tend to have more financial and labor resources than smaller organizations. As such, a larger organization’s DIDS may consist of commercial NIDS (NetProwler, NFR, etc.), freeware NIDS (Snort), packet sniffers (tcpdump, Shadow, etc.), firewall logs, router logs, server logs, and more.

In both cases, the DIDS consist of multiple systems with differing output formats. The benefit of a DIDS is that more information can be captured making it more likely that an intrusion will be detected. The flip side is that more information will need to be processed and this processing will likely be more complex. Also, as more information is captured, event correlation becomes increasingly more important.

Event Correlation in a DIDS Environment

Correlating DIDS event information will be key to effectively detecting network intrusions. DIDS event correlation can also help filter out the false positives that are so prevalent in intrusion detection. It is estimated that 9 out of 10 detected intrusions are actually false positives.

How should events be correlated to satisfy both the small and the large organization? There are a number of methods to correlate event data; however, the challenge is deciding which methods work best for the organization.

Event correlation in the small organization will likely be difficult because the personnel will likely be lacking in security experience. Some organizations may choose to manually correlate the events with simple visual inspection while other organizations may choose to implement some tools for event correlation.

Event correlation in the large organization will likely be difficult because of the various sources of event information and the sheer volume of data. Successful event correlation in the large organization will almost certainly require some additional tools.

So, how can events be correlated in a DIDS environment? Because standards are new and emerging, event correlation is a little more tricky than just concatenating files, exporting them into a database, and generating reports. The different event logging formats that vendors follow make this task nearly impossible without investing significant time and money into third part and/or home grown solutions. Even with third party and/or home grown solutions, the overall results are usually inadequate. If every vendor followed the standards set forth by the IDWG, event correlation would be easier.

The IDWG wrote the Internet-Draft addressing IDS events, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition". An IDMEF (Intrusion Detection Message Exchange Format) event message is an XML (Extensible Markup Language) formatted message which contains the event in an encapsulated format. Since XML is an extensible format, vendors are able to specify additional data for an event beyond the standard IDMEF DTD (Document Type Definition).

IDMEF messages can be transported using the IDWG specified IDXP (Intrusion Detection Exchange Protocol). The IDXP protocol was developed to use the new connection-oriented protocol BEEP (Blocks Extensible Exchange Protocol). One of the features in BEEP is the ability to utilize authentication through the use of new profiles. This ability within BEEP allows IDXP to establish TLS (Transport Layer Security) sessions, resulting in encrypted communications between IDXP systems.

IDMEF/IDXP compatible systems would allow for a centralized IDS management console receiving IDMEF alerts from IDS systems, firewalls, routers, servers, etc. over IDXP. Centralized consoles with correlated events would greatly improve the effectiveness of DIDS solutions and would put a smile on the face of every analyst.

Silicon Defense, a security research and services organization, has focused a lot of attention on the IDWG standards, and their founder and president holds a chair position on the IDWG. Silicon Defense's website contains a wealth of information about the IDWG and its documents. They have developed a free, open-source library (LIBIDMEF) for generating IDMEF XML messages from raw

data. They have also developed a Snort plug-in to allow Snort to generate IDMEF XML alerts.

Another semi-event correlation system of note is ACID (Analysis Console for Intrusion Databases). According to the CERT Coordination Center, "the Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools". It is important to note that ACID relies on the post-processing of information to correlate events and is not a universal event correlation system.

ACID currently accepts information from Snort, Linux ipchains/ipfw, and Cisco firewall-rejected packets. Snort can write to the underlying database in real-time but the Linux and Cisco information needs to be gathered from another application, logsnorter, in order to be inputted into the underlying database.

Since the ACID project is an open source product with GPL licensing, it is reasonable to expect that products will be written to allow the ACID database to accept information from other sources.

When it comes classifying vulnerabilities, one needs to look no further than The MITRE Corporation's Common Vulnerabilities and Exposures (CVE) dictionary. The CVE dictionary is a "list of standardized names for vulnerabilities and other information security exposures" according to the CVE website. The goal of the CVE dictionary is to replace names like "Code Red" and "Nimda" with standardized names.

Since the CVE dictionary doesn't list unknown vulnerabilities and it doesn't define a format for alerts, the CVE dictionary cannot be considered a complete event correlation system. However, since it would allow for alerts from disparate systems to use the same name for known vulnerabilities, the CVE dictionary could be one of the pieces to the event correlation puzzle.

Conclusion

Intrusion detection event correlation is crucial for the success in organizations with DIDS environments. Event correlation applies to nearly every organization since most organizations have either a non-classical DIDS environment (firewall logs and web server logs) or a classical DIDS environment (NIDS, HIDS, sniffers, firewalls, etc.). While event correlation is crucial to the success of a DIDS environment, organizations are compromised by the fact that event correlation is one of the biggest weaknesses in intrusion detection.

Event correlation, as it exists today, is mostly a manual or home grown process. This could change if more IDS and IDS-related systems begin adopting the

IDWG standards and reports with IDMEF alerts. As we all know, acceptance of standards usually takes longer than expected. However, as security companies like Silicon Defense become more involved with IDWG standards, it is likely only a matter of time before event correlation because a main stream reality.

References

Northcutt, Stephen and Novak, Judy. Network Intrusion Detection, An Analyst's Handbook, Second Edition. New Riders, 2001. p. 189. ISBN: 0-7357-1008-2.
Northcutt, Stephan, et. al. Intrusion Signatures and Analysis. New Riders, 2001. ISBN: 0-7357-1063-5.

Bruneau, Guy. What difficulties are associated on matching events with attacks. Why is event/data correlation important? SANS Institute, Intrusion Detection FAQ.
URL: http://ww.sans.org/newlook/resources/IDFAQ/matching.htm.

Shipley, Greg. Dragon Claws its Way to the Top. Network Computing; August 20, 2001.
URL: http://www.networkcomputing.com/1217/1217f2.html.

Curry, D. et. al. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition. IETF Intrusion Detection Working Group. Dec. 28, 2001.
URL: http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-06.txt.

Feinstein, B. et. al. The Intrusion Detection Exchange Protocol (IDXP). IETF Intrusion Detection Working Group. Sep. 11, 2001.
URL: http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-03.txt.

Shipley, Greg. Intrusion Detection, Take Two. Network Computing; November 15, 1999.
URL: http://www.networkcomputing.com/1023/1023f1.html.

ACID. CERT Coordination Center.
URL: http://www.cert.org/kb/acid.

Silicon Defense website.
URL: www.silicondefense.com

McAlerney, Joe. IDMEF XML Library version 0.6.3 Readme.
URL: http://www.silicondefense.com/idwg/libidmef/README.

The MITRE Corporation website.
URL: www.mitre.org

Assignment 2 – Network Detects

Detect 1 – Nimda Scan

Snort Packet Log:

```
01/29-00:19:12.533371 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:20691 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:19:15.530667 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:20931 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:19:21.539206 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:21768 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:19:33.581389 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:23989 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:19:57.601601 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:26942 IpLen:20 DgmLen:112 DF
```

```
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:20:42.844738 the.attack.net.106:3088 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33536 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x2AD11403  Ack: 0x5346A54F  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 63 2F 77 69 6E 6E 74 2F 73 79 73  GET /c/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

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

01/29-00:20:43.086140 the.attack.net.106:3102 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33577 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x2ADBD325  Ack: 0xA8919C23  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 64 2F 77 69 6E 6E 74 2F 73 79 73  GET /d/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

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

01/29-00:20:43.398588 the.attack.net.106:3115 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33627 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2AE6A1E5  Ack: 0xA1072883  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65  5c../winnt/syste
6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64  m32/cmd.exe?/c+d
69 72 20 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  ir r HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

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

01/29-00:20:43.661293 the.attack.net.106:3126 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33671 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x2AF0D852  Ack: 0xE684E55E  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 5F 76 74 69 5F 62 69 6E 2F 2E 2E  GET /_vti_bin/..
25 35 63 2E 2E 2F 2E 2E 25 35 63 2E 2E 2F 2E 2E  %5c../..%5c../..
25 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %5c../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 63 2B 64 69 72 20 48 54 54 50 2F 31  dir c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....

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

```
01/29-00:20:43.957840 the.attack.net.106:3141 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33720 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x2AFC752F  Ack: 0xB0D742E  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 5F 6D 65 6D 5F 62 69 6E 2F 2E 2E  GET /_mem_bin/..
25 35 63 2E 2E 2F 2E 2E 25 35 63 2E 2E 2F 2E 2E  %5c../..%5c../..
25 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %5c../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 63 2B 64 69 72 20 48 54 54 50 2F 31  dir c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....

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

01/29-00:20:44.317748 the.attack.net.106:3158 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33776 IpLen:20 DgmLen:185 DF
***AP*** Seq: 0x2B09AB6F  Ack: 0x36009632  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 35 63  GET /msadc/..%5c
2E 2E 2F 2E 2E 25 35 63 2E 2E 2F 2E 2E 25 35 63  ../..%5c../..%5c
2F 2E 2E 35 35 2E 2E 2F 2E 2E 63 31 2E 2E 2F 2E  /..55../..c1../.
2E 2F 2E 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  ./.../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  dir 32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

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

01/29-00:20:44.638550 the.attack.net.106:3177 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33860 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B1949A6  Ack: 0x9EDA6EA2  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  c../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  r dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

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

01/29-00:20:44.888771 the.attack.net.106:3193 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33901 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B26AA62  Ack: 0x8D263909  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  c../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  r dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

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

01/29-00:20:45.094986 the.attack.net.106:3202 -> my.innocent.net.14:80
```

```
TCP TTL:114 TOS:0x0 ID:33935 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B2E1ADD  Ack: 0xAD71306D  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  c../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  r dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

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

01/29-00:20:45.328942 the.attack.net.106:3211 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:33972 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B3568A9  Ack: 0x60FC788B  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  c../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  r dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

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

01/29-00:20:45.521271 the.attack.net.106:3228 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:34001 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x2B424EF3  Ack: 0x66529D9C  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65  5c../winnt/syste
6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64  m32/cmd.exe?/c+d
69 72 20 64 69 72 20 48 54 54 50 2F 31 2E 30 0D  ir dir HTTP/1.0.
0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E  .Host: www..Conn
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
0D 0A                                            ..

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

01/29-00:20:45.663869 the.attack.net.106:2769 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:34026 IpLen:20 DgmLen:112 DF
***AP**F Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

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

01/29-00:20:45.698318 the.attack.net.106:3235 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:34031 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2B48D352  Ack: 0xC616EC9A  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65  5c../winnt/syste
6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64  m32/cmd.exe?/c+d
69 72 20 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  ir r HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
```

```
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

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

01/29-00:20:45.935024 the.attack.net.106:3249 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:34069 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x2B53F207  Ack: 0x8FDF60BD  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65  5c../winnt/syste
6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64  m32/cmd.exe?/c+d
69 72 20 63 2B 64 69 72 20 48 54 54 50 2F 31 2E  ir c+dir HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F  0..Host: www..Co
6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  nnnection: close
0D 0A 0D 0A                                      ....

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

01/29-00:20:46.183626 the.attack.net.106:3259 -> my.innocent.net.14:80
TCP TTL:114 TOS:0x0 ID:34107 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2B5CDF1A  Ack: 0x130E632D  Win: 0x4510  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65  2f../winnt/syste
6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64  m32/cmd.exe?/c+d
69 72 20 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  ir r HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....
```

Snort Alert Log:

```
[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
01/29-00:19:12.533371 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:20691 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20

[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
01/29-00:19:15.530667 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:20931 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20

[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
01/29-00:19:21.539206 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:21768 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20

[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
```

```
01/29-00:19:33.581389 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:23989 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20

[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
01/29-00:19:57.601601 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:26942 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:42.844738 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x86
the.attack.net.106:3088 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33536 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x2AD11403  Ack: 0x5346A54F  Win: 0x4510  TcpLen: 20

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:43.086140 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x86
the.attack.net.106:3102 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33577 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x2ADBD325  Ack: 0xA8919C23  Win: 0x4510  TcpLen: 20

[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:43.398588 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x96
the.attack.net.106:3115 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33627 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2AE6A1E5  Ack: 0xA1072883  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:43.661293 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0xAB
the.attack.net.106:3126 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33671 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x2AF0D852  Ack: 0xE684E55E  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:43.957840 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0xAB
the.attack.net.106:3141 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33720 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x2AFC752F  Ack: 0xB0D742E  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]
```

```
[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:44.317748 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0xC7
the.attack.net.106:3158 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33776 IpLen:20 DgmLen:185 DF
***AP*** Seq: 0x2B09AB6F  Ack: 0x36009632  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:44.638550 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x97
the.attack.net.106:3177 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33860 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B1949A6  Ack: 0x9EDA6EA2  Win: 0x4510  TcpLen: 20

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:44.888771 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x97
the.attack.net.106:3193 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33901 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B26AA62  Ack: 0x8D263909  Win: 0x4510  TcpLen: 20

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:45.094986 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x97
the.attack.net.106:3202 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33935 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B2E1ADD  Ack: 0xAD71306D  Win: 0x4510  TcpLen: 20

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:45.328942 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x97
the.attack.net.106:3211 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:33972 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x2B3568A9  Ack: 0x60FC788B  Win: 0x4510  TcpLen: 20

[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:45.521271 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x98
the.attack.net.106:3228 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:34001 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x2B424EF3  Ack: 0x66529D9C  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:1257:1] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
01/29-00:20:45.663869 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x7E
the.attack.net.106:2769 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:34026 IpLen:20 DgmLen:112 DF
***AP**F Seq: 0x1CDDC85D  Ack: 0xC00AA076  Win: 0x4510  TcpLen: 20
```

```
[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:45.698318 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x96
the.attack.net.106:3235 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:34031 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2B48D352  Ack: 0xC616EC9A  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:970:1] WEB-IIS multiple decode attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:45.935024 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x9A
the.attack.net.106:3249 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:34069 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x2B53F207  Ack: 0x8FDF60BD  Win: 0x4510  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333]

[**] [1:1002:1] WEB-IIS cmd.exe access [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
01/29-00:20:46.183626 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x96
the.attack.net.106:3259 -> my.innocent.net.14:80 TCP TTL:114 TOS:0x0
ID:34107 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x2B5CDF1A  Ack: 0x130E632D  Win: 0x4510  TcpLen: 20
```

IIS 5.0 Log:

```
2002-01-29 08:19:34 the.attack.net.106 - my.innocent.net.14 80 GET
/MSADC/root.exe /c+dir 404 -
2002-01-29 08:19:34 the.attack.net.106 - my.innocent.net.14 80 GET
/c/winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:34 the.attack.net.106 - my.innocent.net.14 80 GET
/d/winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:34 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..%5c../winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:35 the.attack.net.106 - my.innocent.net.14 80 GET
/_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe /c+dir 500 -
2002-01-29 08:19:35 the.attack.net.106 - my.innocent.net.14 80 GET
/_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:35 the.attack.net.106 - my.innocent.net.14 80 GET
/msadc/..%5c../..%5c../..%5c/..Á ../..Á ../..Á ../winnt/system32/cmd.ex
e /c+dir 404 -
2002-01-29 08:19:35 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..Á ../winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:36 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:36 the.attack.net.106 - my.innocent.net.14 80 GET
/winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:36 the.attack.net.106 - my.innocent.net.14 80 GET
/winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:36 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..%5c../winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:36 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..%5c../winnt/system32/cmd.exe /c+dir 404 -
```

```
2002-01-29 08:19:37 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..%5c../winnt/system32/cmd.exe /c+dir 404 -
2002-01-29 08:19:37 the.attack.net.106 - my.innocent.net.14 80 GET
/scripts/..%2f../winnt/system32/cmd.exe /c+dir 404 -
```

Source of Trace

Corporate network

Detect Generated By

This detect information was generated from an instance of Snort v. 1.8.1-WIN32 (build 74) in NIDS mode using ruleset 1.8.0 and from IIS 5.0 logs. Snort was configured to log packets in binary format according to the ruleset and to generate an alert file, alert.ids. The Ethernet information is included in the Snort output because Snort was configured to capture the layer 2 information.

The Snort packet log information includes the date, time, source IP address, source port, destination IP address, destination port, transport layer protocol, TTL, TOS, fragment ID, IP header length, packet datagram length, fragment information, TCP flags, sequence number, acknowledgement number, TCP window size, TCP header length, and data.

The Snort alert log information includes alert title, classification, priority, date, time, MAC address of next-hop router, MAC address of destination, layer 2 type, frame length, source IP address, source port, destination IP address, destination port, protocol, TTL, TOS, ID, IP header length, datagram length, fragment information, TCP flags, sequence number, acknowledgement number, window size, TCP header length, cross reference (if available).

The IIS 5.0 log information includes date, time, source IP address, destination IP address, destination port, and protocol command.

Please note that the source and destination addresses were modified to protect the guilty and the innocent.

Probability The Source Address Was Spoofed

It is unlikely that the source address was spoofed. One of the intents of Nimda is to gain access to the exploited host so spoofing the source was be of little use. Had a packet logger been in place, the logs could have been examined for the three way TCP handshake.

Description of The Attack

The Nimda attack is a worm which attempts to exploit known vulnerabilities in Microsoft's IIS servers (including directory traversal vulnerabilities and back

doors left behind by the Code Red II worm) and Internet Explorer. CERT has an advisory at http://www.cert.org/advisories/CA-2001-26.html (CERT Advisory CA-2001-26 Nimda Worm).

Attack Mechanism

The Nimda worm was targeting port 80 on the web server. Specifically, the worm was first trying to utilize a back door left by the Code Red II worm. This is documented by the "WEB-IIS CodeRed v2 root.exe access" alerts listed above. Secondly, the worm was trying to exploit a known directory traversal vulnerability. This is documented by the "WEB-IIS multiple decode attempt" alerts listed above. The Nimda worm also attempts to exploit a known vulnerability in Internet Explorer which can manifest itself in MIME e-mail clients like Outlook and can be propagated with the malicious attachment, readme.exe.

The malicious code will infect a vulnerable host by writing copies of itself to .eml and .nws files and by inputting JavaScript code into web-related files (.htm, .html. .htt, etc.). The malicious code will also infect binary files by creating trojans with the malicious code. The code will also attempt to share the C:\ drive, enable or create the Guest account and add the Guest account to the Administrators group.

If the JavaScript code mentioned above is executed, the infected host attempts to propagate Nimda to other hosts. Nimda can be further propagated by copying the malicious code via TFTP to other systems, by scanning for other vulnerable IIS servers, and by a mass mailing e-mail mechanism.

Correlations

The Nimda worm and the relevant IIS/IE vulnerabilities are very well documented, including:

Nimda

http://www.cert.org/advisories/CA-2001-26.html
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/topics/nimda.asp

IIS Vulnerabilities
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0333
http://www.cert.org/advisories/CA-2001-12.html
http://www.cert.org/advisories/CA-2001-11.html
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

IE execution of embedded MIME types

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp
http://www.cert.org/advisories/CA-2001-06.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0154

Evidence of Active Targeting

The source IP address generated the same alerts to multiple hosts on our subnet so it is unlikely that this was a case of active targeting. This activity is typical of a host infected with the Nimda worm.

Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is: +2

Criticality: 5 (the corporate web server received the Nimda alerts)
Lethality: 4 (if the web server were to be exploited, the impact would have been very significant)
System Countermeasures: 5 (all security patches were installed)
Network Countermeasures: 2 (firewall and router were not configured to stop this type of traffic)

Defensive Recommendation

Block this type of traffic at the router using this guide from Cisco: http://www.cisco.com/warp/public/63/nimda.shtml. Also, continue to keep all systems up-to-date with security patches.

Multiple Choice Test Question

Which vulnerabilities does Nimda try to exploit:

A) Directory traversal vulnerabilities with Microsoft's IIS servers?
B) Buffer overflow in Universal Plug and Play service in Windows?
C) Microsoft Word macro vulnerability?
D) IE execution of embedded MIME types?
E) All of the above?

Answer: B & D

Detect 2 – ICMP Superscan Echo

Snort Alert Log:

```
[**] [1:474:1] ICMP superscan echo [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/29-01:21:34.942060 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.236 -> my.innocent.net.3 ICMP TTL:109 TOS:0x0 ID:48079
IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16507  ECHO

[**] [1:474:1] ICMP superscan echo [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/29-01:21:35.003999 AA:AA:BB:BB:CC:CC -> 0:B0:D0:79:17:5D type:0x800
len:0x3C
the.attack.net.236 -> my.innocent.net.4 ICMP TTL:109 TOS:0x0 ID:48847
IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16510  ECHO

[**] [1:474:1] ICMP superscan echo [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/29-01:21:35.059323 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.236 -> my.innocent.net.5 ICMP TTL:109 TOS:0x0 ID:49615
IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16513  ECHO

[**] [1:474:1] ICMP superscan echo [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/29-01:21:35.337637 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.236 -> my.innocent.net.10 ICMP TTL:109 TOS:0x0 ID:53455
IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16528  ECHO
```

These alerts continued and included the hosts: .12, .14, .20, .30, .39, .50, .51, .52, .53, .54, .61-.68, .70-.75, .80, .100-.105, and .125.

Snort Packet Log:

```
01/29-01:21:34.942060 the.attack.net.236 -> my.innocent.net.3
ICMP TTL:109 TOS:0x0 ID:48079 IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16507  ECHO
00 00 00 00 00 00 00 00                         ........

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

01/29-01:21:35.003999 the.attack.net.236 -> my.innocent.net.4
ICMP TTL:109 TOS:0x0 ID:48847 IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16510  ECHO
00 00 00 00 00 00 00 00                         ........

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

```
01/29-01:21:35.059323 the.attack.net.236 -> my.innocent.net.5
ICMP TTL:109 TOS:0x0 ID:49615 IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16513  ECHO
00 00 00 00 00 00 00 00                         ........

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

01/29-01:21:35.337637 the.attack.net.236 -> my.innocent.net.10
ICMP TTL:109 TOS:0x0 ID:53455 IpLen:20 DgmLen:36
Type:8  Code:0  ID:1   Seq:16528  ECHO
00 00 00 00 00 00 00 00                         ........

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

These logs continued and included the hosts: .12, .14, .20, .30, .39, .50, .51, .52, .53, .54, .61-.68, .70-.75, .80, .100-.105, and .125.

Source of Trace

Corporate network

Detect Generated By

This detect information was generated from an instance of Snort v. 1.8.1-WIN32 (build 74) in NIDS mode using ruleset 1.8.0. Snort was configured to log packets in binary format according to the ruleset and to generate an alert file, alert.ids. The Ethernet information is included in the Snort output because Snort was configured to capture the layer 2 information.

The Snort alert log information includes alert title, classification, priority, date, time, MAC address of next-hop router, MAC address of destination, layer 2 type, frame length, source IP address, destination IP address, protocol, TTL, TOS, ID, IP header length, datagram length, ICMP Type, ICMP Code, ID, sequence, and description.

The Snort packet log information includes the date, time, source IP address, destination IP address, protocol, TTL, TOS, fragment ID, IP header length, packet datagram length, ICMP Type, ICMP Code, ID, sequence number, description, and data.

Please note that the source and destination addresses were modified to protect the guilty and the innocent.

Probability The Source Address Was Spoofed

It is unlikely that the source address was spoofed since this was likely a reconnaissance probe to determine if hosts are active.

Description of The Attack

The port scanner SuperScan from Foundstone (www.foundstone.com) was likely used to run this ICMP scan for active systems on the network

Attack Mechanism

SuperScan is one of the many free scanners available on the Internet. The attacker had configured SuperScan to scan our network for active hosts. SuperScan used the ICMP protocol to scan for active hosts and this generated the alerts. The attacker could use the response information from the corporate hosts to map which IP addresses on the corporate subnet are active and then possibly perform some other attacks, including OS fingerprinting, port scans, etc.

Correlations

SuperScan information can be found at Foundstone at:
http://www.foundstone.com/knowledge/free_tools.html

A SuperScan scan detected by Laurie Zirkle is posted at Incidents.org at:
http://www.incidents.org/archives/intrusions/msg01221.html

Evidence of Active Targeting

This scan was unlikely a case of active targeting since all hosts on the subnet were scanned.

Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is: -2

Criticality: 4 (all hosts were scanned)
Lethality: 1 (this was an “active host” reconnaissance scan)
System Countermeasures: 4 (the systems replied but should be configured not to do so)
Network Countermeasures: 3 (the IDS detected the scan but was not configured to reset this type of connection)

Defensive Recommendation

Setup an overall solution which prevents replies to ICMP packets from untrusted sources.

Multiple Choice Test Question

The SuperScan scan in this detect used which protocol:

A) HTTP
B) FTP
C) TCP
D) ICMP
E) UDP

Answer: D

Detect 3 – Nmap scan

Snort Alert Log:

```
[**] [1:468:1] ICMP Nmap2.36BETA or HPING2 Echo  [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:07:46.260211 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162 -> my.innocent.net.3 ICMP TTL:34 TOS:0x0 ID:23560
IpLen:20 DgmLen:28
Type:8  Code:0  ID:12010   Seq:24366  ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [1:615:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:07:56.207080 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162:18565 -> my.innocent.net.3:1080 TCP TTL:33 TOS:0x0
ID:4676 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

[**] [1:615:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:07:57.224423 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162:18942 -> my.innocent.net.3:1080 TCP TTL:33 TOS:0x0
ID:29015 IpLen:20 DgmLen:40
******S* Seq: 0x14526E57  Ack: 0x0  Win: 0x800  TcpLen: 20

[**] [1:618:1] INFO - Possible Squid Scan [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:08:42.287539 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162:18565 -> my.innocent.net.3:3128 TCP TTL:33 TOS:0x0
ID:31078 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

[**] [1:620:1] SCAN Proxy attempt [**]
```

```
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:09:12.187969 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162:18565 -> my.innocent.net.3:8080 TCP TTL:33 TOS:0x0
ID:17535 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

[**] [1:620:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 3]
01/30-11:09:13.201069 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.162:18942 -> my.innocent.net.3:8080 TCP TTL:33 TOS:0x0
ID:33331 IpLen:20 DgmLen:40
******S* Seq: 0x14526E57  Ack: 0x0  Win: 0x800  TcpLen: 20

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.162:
27 connections across 1 hosts: TCP(26), UDP(1) [**]
01/30-11:09:15.405000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.162: 2
connections across 1 hosts: TCP(2), UDP(0) [**]
01/30-11:09:19.341000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.162: 2
connections across 1 hosts: TCP(1), UDP(1) [**]
01/30-11:09:23.266000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.162: 3
connections across 1 hosts: TCP(2), UDP(1) [**]
01/30-11:09:27.272000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.162: 1
connections across 1 hosts: TCP(1), UDP(0) [**]
01/30-11:09:46.720000
```

NOTE: The majority of the spp_portscan records were omitted for brevity.

Snort Portscan Log:

```
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:261 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:1400 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:6112 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:556 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:517 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:997 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18942 -> my.innocent.net.3:1067 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18942 -> my.innocent.net.3:1346 SYN
******S*
```

```
Jan 30 11:07:48 the.attack.net.162:18942 -> my.innocent.net.3:2019 SYN
******S*
Jan 30 11:07:47 the.attack.net.162:18565 -> my.innocent.net.3:2301 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18565 -> my.innocent.net.3:5978 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18565 -> my.innocent.net.3:524 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18565 -> my.innocent.net.3:1671 SYN
******S*
Jan 30 11:07:48 the.attack.net.162:18565 -> my.innocent.net.3:1385 SYN
******S*
Jan 30 11:07:49 the.attack.net.162:18942 -> my.innocent.net.3:1349 SYN
******S*
```

…….. (this continued on many more ports)

```
Jan 30 11:09:13 the.attack.net.162:20760 -> my.innocent.net.3:1 SYN
******S*
Jan 30 11:09:15 the.attack.net.162:21082 -> my.innocent.net.3:1 UDP
Jan 30 11:09:17 the.attack.net.162:20928 -> my.innocent.net.3:80 SYN
******S*
Jan 30 11:09:19 the.attack.net.162:20760 -> my.innocent.net.3:1 SYN
******S*
Jan 30 11:09:21 the.attack.net.162:21082 -> my.innocent.net.3:1 UDP
Jan 30 11:09:23 the.attack.net.162:18942 -> my.innocent.net.3:80 SYN
******S*
Jan 30 11:09:23 the.attack.net.162:20928 -> my.innocent.net.3:80 SYN
******S*
Jan 30 11:09:25 the.attack.net.162:20760 -> my.innocent.net.3:1 SYN
******S*
Jan 30 11:09:27 the.attack.net.162:21082 -> my.innocent.net.3:1 UDP
Jan 30 11:09:29 the.attack.net.162:20928 -> my.innocent.net.3:80 SYN
******S*
```

Snort Packet Log:

```
01/30-11:07:46.260211 the.attack.net.162 -> my.innocent.net.3
ICMP TTL:34 TOS:0x0 ID:23560 IpLen:20 DgmLen:28
Type:8  Code:0  ID:12010   Seq:24366  ECHO

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

01/30-11:07:56.207080 the.attack.net.162:18565 ->
my.innocent.net.3:1080
TCP TTL:33 TOS:0x0 ID:4676 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

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

01/30-11:07:57.224423 the.attack.net.162:18942 ->
my.innocent.net.3:1080
TCP TTL:33 TOS:0x0 ID:29015 IpLen:20 DgmLen:40
******S* Seq: 0x14526E57  Ack: 0x0  Win: 0x800  TcpLen: 20

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

```
01/30-11:08:42.287539 the.attack.net.162:18565 ->
my.innocent.net.3:3128
TCP TTL:33 TOS:0x0 ID:31078 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

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

01/30-11:09:12.187969 the.attack.net.162:18565 ->
my.innocent.net.3:8080
TCP TTL:33 TOS:0x0 ID:17535 IpLen:20 DgmLen:40
******S* Seq: 0x580C0895  Ack: 0x0  Win: 0x800  TcpLen: 20

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

01/30-11:09:13.201069 the.attack.net.162:18942 ->
my.innocent.net.3:8080
TCP TTL:33 TOS:0x0 ID:33331 IpLen:20 DgmLen:40
******S* Seq: 0x14526E57  Ack: 0x0  Win: 0x800  TcpLen: 20

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

Source of Trace

Corporate network

Detect Generated By

This detect information was generated from an instance of Snort v. 1.8.1-WIN32 (build 74) in NIDS mode using ruleset 1.8.0. Snort was configured to log packets in binary format according to the ruleset and to generate an alert file, alert.ids. The Ethernet information is included in the Snort output because Snort was configured to capture the layer 2 information.

The ICMP record from the Snort alert log includes the alert title, classification, priority, date, time, MAC address of next-hop router, MAC address of destination, layer 2 type, frame length, source IP address, destination IP address, protocol, TTL, TOS, ID, IP header length, datagram length, ICMP Type, ICMP Code, ID, sequence, description, and cross reference.

The TCP records from the Snort alert log include the alert title, classification, priority, date, time, MAC address of next-hop router, MAC address of destination, layer 2 type, frame length, source IP address, source port, destination IP address, destination port, protocol, TTL, TOS, ID, IP header length, datagram length, TCP flags, sequence number, acknowledgement number, window size, and TCP header length.

The portscan records from the Snort alert log include the portscan title, source IP address, connection attempts, time span or number of hosts, protocol(s) if applicable, date, and time.

The portscan records from the Snort portscan log include the date, time, source IP address, source port, destination IP address, destination port, and TCP options.

The Snort packet log information of the ICMP record includes the date, time, source IP address, destination IP address, protocol, TTL, TOS, ID, IP header length, packet datagram length, ICMP Type, ICMP Code, ID, sequence number, and description.

The Snort packet log information of the TCP records includes the date, time, source IP address, source port, destination IP address, destination port, transport layer protocol, TTL, TOS, ID, IP header length, packet datagram length, TCP flags, sequence number, acknowledgement number, TCP window size, and TCP header length.

Please note that the source and destination addresses were modified to protect the guilty and the innocent.

Probability The Source Address Was Spoofed

It is unlikely that the source address was spoofed since the attacker's goal was to obtain responses from the destination host.

Description of The Attack

The network mapping tool, Nmap, was used in an attempt to determine the operating system of the destination host and to scan for open ports.

Attack Mechanism

Nmap is a "network mapper" available at www.insecure.org. Nmap can be configured to do a number of things, including port scans, null scans, stealth scans, operating system fingerprinting, and more. It appears from the Snort data that Nmap attempted to determine the destination host's operating system and did a port scan on the destination host.

The Nmap port scan aspect of the attack was similar to other port scanners. Nmap was looking for responses from ports to determine whether or not they were open.

The Nmap operating system aspect of the attack uses the responses from the destination host in an attempt to determine what operating system is running on the destination host. This is explained in great detail on the Insecure.org site at: http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

The information from the Snort alert log file indicates that a number of different alerts occurred; yet, they are included here as part of a single Nmap scan. While this may seem a bit strange, it is important to note that Snort reported exactly what it is saw. Snort didn't post-process it's own alerts to determine that:

- All of the alerts were from the same source host
- All of the alerts were to the same destination host
- The alerts occurred in a very short duration

This is a good example of why IDS data needs to be evaluated by a security analyst. It would have been easy to say that the alerts were exactly what they appeared to be. However, in this case, the combination of the alert, portscan, and packet logging information indicated that this was more than just port scans, Squid scans, and Proxy scans.

Correlations

Nmap can be found at Insecure.org at:
http://www.insecure.org

"What is nmap and what can it do" is online at SANS at:
http://www.sans.org/newlook/resources/IDFAQ/What_is_nmap.htm

Evidence of Active Targeting

This scan was unlikely a case of active targeting since all hosts on the subnet were scanned.

Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is: -1

Criticality: 5 (the main corporate web server was targeted)
Lethality: 2 (this was a port and OS fingerprinting scan)
System Countermeasures: 4 (the web server is located behind a firewall)
Network Countermeasures: 4 (a firewall protects the web server and only allows HTTP connections)

Defensive Recommendation

Investigate a solution which would reset port scans and operating system fingerprinting traffic.

Multiple Choice Test Question

Nmap can be used for which purpose:

A) Determination of layer 2 protocol?
B) Password cracking?
C) Operating system fingerprinting?
D) Bandwidth utilization?

Answer: C

Network Detect 4 – SYN-FIN Scan

Snort Portscan Log:

```
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.3:22 SYNFIN
******SF
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.4:22 SYNFIN
******SF
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.5:22 SYNFIN
******SF
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.10:22 SYNFIN
******SF
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.12:22 SYNFIN
******SF
Dec  1 07:55:31 the.attack.net.231:22 -> my.innocent.net.14:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.20:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.30:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.39:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.50:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.51:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.52:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.53:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.54:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.61:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.62:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.63:22 SYNFIN
******SF
```

```
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.64:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.65:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.66:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.67:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.68:22 SYNFIN
******SF
Dec  1 07:55:32 the.attack.net.231:22 -> my.innocent.net.69:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.70:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.71:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.72:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.73:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.74:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.75:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.80:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.100:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.101:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.102:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.103:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.104:22 SYNFIN
******SF
Dec  1 07:55:33 the.attack.net.231:22 -> my.innocent.net.105:22 SYNFIN
******SF
Dec  1 07:55:34 the.attack.net.231:22 -> my.innocent.net.125:22 SYNFIN
******SF
```

Snort Alert Log:

```
[**] [111:13:1] spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
[**]
12/01-07:55:31.652537 AA:AA:BB:BB:CC:CC -> 01:23:45:67:89:AB type:0x800
len:0x3C
the.attack.net.231:22 -> my.innocent.net.3:22 TCP TTL:25 TOS:0x0
ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x23FF782  Ack: 0x28111CC5  Win: 0x404  TcpLen: 20
```

NOTE: These alerts occurred for each destination host listed in the portscan log listed above. The remaining alerts were omitted for brevity. It is important to note that the ID, sequence, and acknowledgement numbers were the same in all alerts.

```
[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from the.attack.net.231
(STEALTH) [**]
12/01-07:55:31.640000
```

Snort Packet Log:

```
12/01-07:55:31.652537 the.attack.net.231:22 -> my.innocent.net.3:22
TCP TTL:25 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x23FF782  Ack: 0x28111CC5  Win: 0x404  TcpLen: 20

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

NOTE: These packet log records occurred for each destination host listed in the portscan log listed above. The remaining records were omitted for brevity. As reported with the alert records, the ID, Seq, and Ack numbers were the same in all of these records.

Source of Trace

Corporate network

Detect Generated By

This detect information was generated from an instance of Snort v. 1.8.1-WIN32 (build 74) in NIDS mode using ruleset 1.8.0. Snort was configured to log packets in binary format according to the ruleset and to generate an alert file, alert.ids. The Ethernet information is included in the Snort output because Snort was configured to capture the layer 2 information.

The portscan records from the Snort portscan log include the date, time, source IP address, source port, destination IP address, destination port, and TCP options.

The TCP records from the Snort alert log include the alert title, date, time, MAC address of next-hop router, MAC address of destination, layer 2 type, frame length, source IP address, source port, destination IP address, destination port, protocol, TTL, TOS, ID, IP header length, datagram length, TCP flags, sequence number, acknowledgement number, window size, and TCP header length.

The portscan record from the Snort alert log includes the portscan title, source IP address, STEALTH marker, date, and time.

The records from the Snort packet log include the date, time, source IP address, source port, destination IP address, destination port, transport layer protocol, TTL, TOS, ID, IP header length, packet datagram length, TCP flags, sequence number, acknowledgement number, TCP window size, and TCP header length.

Please note that the source and destination addresses were modified to protect the guilty and the innocent.

Probability The Source Address Was Spoofed

It is unlikely that the source address was spoofed since in a SYN-FIN scan, the attacker is looking for a response.

Description of The Attack

This was a SYN-FIN scan for port 22, SSH Remote Login Protocol. Port 22 is commonly used for secure sessions into routers, firewalls, servers, etc. SYN is used to initiate the three-way TCP handshake and FIN is used to terminate a TCP session. When SYN and FIN are used together in the same packet, it is usually a sign of a crafted packet since they should not appear together in the same packet. Other signs indicating that these were crafted packets are that all packets have the same sequence numbers, the same acknowledgement numbers, and the same ID numbers.

Attack Mechanism

There are a couple of programs which could have been used for this scan. One program that is commonly used for scans like this is SynScan (http://www.psychoid.lam3rz.de/synscan.html). SynScan commonly uses 39426 for the ID and 0x404 for the window size, which is what was detected in this scan. The attacker using SynScan (or a similar tool) customized it to scan the corporate subnet for hosts with port 22 active. The scan took 3 seconds.

Correlations

SynScan can be found at:
http://www.psychoid.lam3rz.de/synscan.html

Snort-users newsgroup thread:
http://www.geocrawler.com/archives/3/4890/2000/11/0/4749307/

SANS GIAC, Current Report, 2/23/01 - 1600
http://www.sans.org/y2k/022301-1600.htm

SecurityFocus home infocus: Network Intrusion Detection Signatures, Part 1
http://www.securityfocus.com/infocus/1524

Evidence of Active Targeting

The scan was directed at the corporate subnet; however, it is likely that the corporate subnet was included as part of a wider scan. No traffic from the source IP address has been detected since this scan.

Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is: -3

Criticality: 4 (the corporate Internet subnet was targeted)
Lethality: 3 (if SSH access is obtained to vital resources, the effect could be significant)
System Countermeasures: 5 (these systems do not run SSH)
Network Countermeasures: 5 (the firewall dropped all of these packets)

Defensive Recommendation

Continue monitoring for this type of traffic and if SSH-enabled systems are implemented, ensure all security recommendations are followed.

Multiple Choice Test Question

SynScan commonly uses which ID number:

A) 34926
B) 0x404
C) 17
D) 6
E) 39426

Answer: E

Network Detect 5 – FTP Server Scan, Warez Vulnerability

Snort Portscan Log:

```
Jan 29 00:54:29 the.attack.net.10:1484 -> my.innocent.net.3:21 SYN
******S*
Jan 29 00:54:30 the.attack.net.10:1485 -> my.innocent.net.4:21 SYN
******S*
Jan 29 00:54:26 the.attack.net.10:1486 -> my.innocent.net.5:21 SYN
******S*
Jan 29 00:54:29 the.attack.net.10:1491 -> my.innocent.net.10:21 SYN
******S*
```

```
Jan 29 00:54:29 the.attack.net.10:1493 -> my.innocent.net.12:21 SYN
******S*
Jan 29 00:54:29 the.attack.net.10:1495 -> my.innocent.net.14:21 SYN
******S*
Jan 29 00:54:29 the.attack.net.10:1501 -> my.innocent.net.20:21 SYN
******S*
Jan 29 00:54:29 the.attack.net.10:1511 -> my.innocent.net.30:21 SYN
******S*
Jan 29 00:54:29 the.attack.net.10:1520 -> my.innocent.net.39:21 SYN
******S*
Jan 29 00:54:30 the.attack.net.10:1531 -> my.innocent.net.50:21 SYN
******S*
Jan 29 00:54:31 the.attack.net.10:1532 -> my.innocent.net.51:21 SYN
******S*
Jan 29 00:54:30 the.attack.net.10:1533 -> my.innocent.net.52:21 SYN
******S*
Jan 29 00:54:30 the.attack.net.10:1534 -> my.innocent.net.53:21 SYN
******S*
Jan 29 00:54:30 the.attack.net.10:1535 -> my.innocent.net.54:21 SYN
******S*
Jan 29 00:54:32 the.attack.net.10:1534 -> my.innocent.net.53:21 SYN
******S*
Jan 29 00:54:32 the.attack.net.10:1533 -> my.innocent.net.52:21 SYN
******S*
Jan 29 00:54:32 the.attack.net.10:1535 -> my.innocent.net.54:21 SYN
******S*
Jan 29 00:54:31 the.attack.net.10:1531 -> my.innocent.net.50:21 SYN
******S*
Jan 29 00:54:32 the.attack.net.10:1532 -> my.innocent.net.51:21 SYN
******S*
Jan 29 00:54:34 the.attack.net.10:1542 -> my.innocent.net.61:21 SYN
******S*
Jan 29 00:54:34 the.attack.net.10:1543 -> my.innocent.net.62:21 SYN
******S*
Jan 29 00:54:34 the.attack.net.10:1544 -> my.innocent.net.63:21 SYN
******S*
Jan 29 00:54:34 the.attack.net.10:1545 -> my.innocent.net.64:21 SYN
******S*
Jan 29 00:54:35 the.attack.net.10:1546 -> my.innocent.net.65:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1547 -> my.innocent.net.66:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1548 -> my.innocent.net.67:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1549 -> my.innocent.net.68:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1551 -> my.innocent.net.70:21 SYN
******S*
Jan 29 00:54:35 the.attack.net.10:1542 -> my.innocent.net.61:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1552 -> my.innocent.net.71:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1553 -> my.innocent.net.72:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1554 -> my.innocent.net.73:21 SYN
******S*
```

```
Jan 29 00:54:37 the.attack.net.10:1555 -> my.innocent.net.74:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1556 -> my.innocent.net.75:21 SYN
******S*
Jan 29 00:54:35 the.attack.net.10:1544 -> my.innocent.net.63:21 SYN
******S*
Jan 29 00:54:35 the.attack.net.10:1543 -> my.innocent.net.62:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1561 -> my.innocent.net.80:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1581 -> my.innocent.net.100:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1546 -> my.innocent.net.65:21 SYN
******S*
Jan 29 00:54:37 the.attack.net.10:1545 -> my.innocent.net.64:21 SYN
******S*
Jan 29 00:54:38 the.attack.net.10:1582 -> my.innocent.net.101:21 SYN
******S*
Jan 29 00:54:38 the.attack.net.10:1583 -> my.innocent.net.102:21 SYN
******S*
Jan 29 00:54:38 the.attack.net.10:1584 -> my.innocent.net.103:21 SYN
******S*
Jan 29 00:54:38 the.attack.net.10:1585 -> my.innocent.net.104:21 SYN
******S*
Jan 29 00:54:38 the.attack.net.10:1586 -> my.innocent.net.105:21 SYN
******S*
Jan 29 00:54:39 the.attack.net.10:1606 -> my.innocent.net.125:21 SYN
******S*
Jan 29 00:54:41 the.attack.net.10:1606 -> my.innocent.net.125:21 SYN
******S*
```

Snort Alert Log:

```
[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from the.attack.net.10
(THRESHOLD 4 connections exceeded in 1 seconds) [**]
01/29-00:54:27.035000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.10: 14
connections across 14 hosts: TCP(14), UDP(0) [**]
01/29-00:54:31.361000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.10: 10
connections across 10 hosts: TCP(10), UDP(0) [**]
01/29-00:54:35.006000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.10: 22
connections across 22 hosts: TCP(22), UDP(0) [**]
01/29-00:54:39.122000

[**] [100:2:1] spp_portscan: portscan status from the.attack.net.10: 1
connections across 1 hosts: TCP(1), UDP(0) [**]
01/29-00:54:44.971000

[**] [100:3:1] spp_portscan: End of portscan from the.attack.net.10:
TOTAL time(15s) hosts(44) TCP(47) UDP(0) [**]
01/29-00:54:48.706000
```

IIS 5.0 Log

```
08:45:49 the.attack.net.10 USER anonymous 331
08:45:49 the.attack.net.10 PASS guest@here.com 230
08:45:50 the.attack.net.10 MKD 020129095042p 550
08:45:53 the.attack.net.10 MKD 020129095044p 550
```

Source of Trace

Corporate network

Detect Generated By

This detect information was generated from an instance of Snort v. 1.8.1-WIN32 (build 74) in NIDS mode using ruleset 1.8.0. Snort was configured to log packets in binary format according to the ruleset and to generate an alert file, alert.ids. The Ethernet information is included in the Snort output because Snort was configured to capture the layer 2 information.

The Snort portscan log records include the date, time, source IP address, source port, destination IP address, destination port, and TCP options.

The Snort alert log portscan records include the portscan title, source IP address, connection attempts, time span or number of hosts contacted, protocol(s) if applicable, date, and time.

The IIS 5.0 log information includes the time, source IP address, FTP command, and result code.

Please note that the source and destination addresses were modified to protect the guilty and the innocent.

Probability The Source Address Was Spoofed

It is unlikely that the source address was spoofed since this scan was looking for FTP servers; specifically, the scan was looking for FTP servers with a null password for the anonymous account.

Description of The Attack

The Snort records show that this was a scan of the corporate subnet. When the Snort records were combined with the IIS log records, it became apparent that this was a scan for FTP servers with the anonymous account active. The information from these logs is typical of a script which looks for “open” FTP servers to be used as a warez site for the distribution of illegal copies of software.

Attack Mechanism

This FTP scan took twelve seconds and was targeted at the corporate subnet. This scan likely used a script which looked for FTP servers which have the anonymous account active. If the FTP server did have the anonymous account active, the script would then try to create directories on the FTP server. If this were successful, illegal copies of software would likely be uploaded and this server would be advertised within the warez community.

Correlations

Shelli Crocket wrote, "FTP and the Warez Scene"
http://rr.sans.org/threats/warez.php

CERT Advisory CA-1993-10 Anonymous FTP Activity
http://www.cert.org/advisories/CA-1993-10.html

Evidence of Active Targeting

The scan was directed at the corporate subnet. One FTP server did respond but it wasn't the response desired from the scan and no traffic from the external host has been detected since then. So, the likelihood of active targeting is fairly low.

Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is: -1

Criticality: 4 (the corporate Internet subnet was targeted)
Lethality: 4 (warez compromise machines can have all of their disk space consumed and the resultant software downloads from this machine can saturate the Internet link)
System Countermeasures: 5 (the contacted FTP server had it's security configuration setup to prevent this type of compromise)
Network Countermeasures: 4 (a firewall protects the corporate subnet and only allows FTP in to the one FTP server)

Defensive Recommendation

Continue monitoring for this type of traffic on the network. Also, continue monitoring the FTP logs and consider blocking source IP addresses if these

sources continue initiating scans. Also, consider contacting the ISP of the source IP addresses.

Multiple Choice Test Question

Warez scripts target which destination port:

A) 23
B) 80
C) 21
D) 22
E) 25

Answer: C

References

CERT Advisory CA-2001-26 Nimda Worm.
URL: http://www.cert.org/advisories/CA-2001-26.html

Information on the "Nimda" Worm.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/topics/nimda.asp

CVE-2001-033.
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0333

CERT Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS.
URL: http://www.cert.org/advisories/CA-2001-12.html

CERT Advisory CA-2001-11 sadmind/IIS Worm.
URL: http://www.cert.org/advisories/CA-2001-11.html

Microsoft Security Bulletin MS01-33.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Microsoft Security Bulletin (MS01-020).
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

CERT Advisory CA-2001-06 Automatic Execution of Embedded MIME Types.
URL: http://www.cert.org/advisories/CA-2001-06.html

CVE-2001-0154.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0154

Cisco - How to Protect Your Network Against the Nimda Virus.
URL: http://www.cisco.com/warp/public/63/nimda.shtml.

SuperScan.
URL: http://www.foundstone.com/knowledge/free_tools.html

Zirkle, Laurie. July 30, 2001 probes (part 2).
URL: http://www.incidents.org/archives/intrusions/msg01221.html

Insecure.org website.
URL: http://www.insecure.org

Remote OS Detection via TCP/IP Fingerprinting.
URL: http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

Green, John. What is nmap and what can it do?
URL: http://www.sans.org/newlook/resources/IDFAQ/What_is_nmap.htm

SynScan.
URL: http://www.psychoid.lam3rz.de/synscan.html

Snort-users newsgroup thread.
URL: http://www.geocrawler.com/archives/3/4890/2000/11/0/4749307/

SANS GIAC, Current Report, 2/23/01 – 1600.
URL: http://www.sans.org/y2k/022301-1600.htm

Frederick, Karen Kent. SecurityFocus home infocus: Network Intrusion Detection Signatures, Part 1.
URL: http://www.securityfocus.com/infocus/1524

Crocket, Shelli. FTP and the Warez Scene.
URL: http://rr.sans.org/threats/warez.php

CERT Advisory CA-1993-10 Anonymous FTP Activity.
URL: http://www.cert.org/advisories/CA-1993-10.html

Lajon, Gregory. GCIA Practical.
URL: http://www.giac.org/practical/Gregory_Lajon_GCIA.doc

Currie, Robert. GCIA Practical.
URL: http://www.giac.org/practical/Robert_Currie.doc

Yuen, Rick Wenkey. GCIA Practical.
URL: http://www.giac.org/practical/Rick_Yuen_GCIA.doc

Partee, Elvis Moe. GCIA Practical.
URL: http://www.giac.org/practical/Elvis_Moe_Partee_GCIA.zip

Goodwin, PJ. GCIA Practical.
URL: http://www.giac.org/practical/PJ_Goodwin_GCIA.doc

Jenkinson, John. GCIA Practical.
URL: http://www.giac.org/practical/John_Jenkinson_GCIA.doc

Woodroffe, Alan. GCIA Practical.
URL: http://www.giac.org/practical/Alan_Woodroffe_GCIA.doc

Assignment 3 – "Analyze This" Scenario

Overview/Executive Summary

A University has asked for a security audit of log files generated from their Snort implementation. Specifically, the data to be analyzed was from December 22 – 26, 2001. The log output during this time was separated into three different sets of files: alerts, scans, and out of specifications (OOS).

A summary and description of alerts, scans, and OOS data will be presented. Also presented in this report will be the top twenty alerts, the top ten alert talkers, the top fifteen scans, the top ten scan talkers, and registration information for certain external hosts. Finally, security recommendations will be presented at the end of this document.

As a disclaimer, the Snort version and rule sets have not been provided for this audit, nor has the network topology.

Alert Analysis

The alerts indicated that a lot of peer-to-peer file sharing and instant messaging was present on the network. The alerts also suggested that a significant portion of the network traffic could be classified as suspicious and that active targeting may have occurred. There is a high probability that some of the internal hosts have been exploited and were/are in a compromised state. Please note that the

portscan alerts were removed from this analysis since there is a separate Scan Analysis section below. There were 85,000 portscan records in the alert files.

The list of alert files that were used for this analysis were:

- alert_011222_gz.htm
- alert_011223_gz.htm
- alert_011224_gz.htm
- alert_011225_gz.htm
- alert_011226_gz.htm

Top 20 Alerts

Alert Rank	**Alert**	***Total***
1	Watchlist 000220 IL-ISDNNET-990517	62,318
2	MISC traceroute	32,793
3	CS WEBSERVER – external web traffic	18,080
4	MISC source port 53 to MY.NET.x.x:53 (this is a combination of multiple alerts to 13 hosts)	16,955
5	ICMP Echo Request BSDtype	11,550
6	INFO MSN IM Chat data	10,305
7	WEB-MISC prefix-get //	9,644
8	MISC Large UDP Packet	7,748
9	SCAN Proxy attempt	5,753
10	Queso fingerprint	5,132
11	ICMP Source Quench	5,111
12	SYN-FIN Scan!	5,026
13	BACKDOOR NetMetro (two alerts - File List & Incoming Traffic)	4,683
14	ICMP Destination Unreachable (Communication Administratively Prohibited)	4,681
15	ICMP Destination Unreachable (Host Unreachable)	3,447
16	ICMP Fragment Reassembly Time Exceeded	2,249
17	Watchlist 000222 NET-NCFC	1,980
18	External RPC call	1,256
19	ICMP Echo Request Nmap or HPING2	1,218
20	INFO FTP anonymous FTP	1,054

Top 10 Alert Talkers

Talker Rank	IP Address	Total Alerts	Top Alerts	Top Alert Total
1	212.179.35.118	61,327	Watchlist 000220 IL-ISDNNET-990517	61,327
2	24.0.28.234	5,027	SYN-FIN Scan!	5,026
3	MY.NET.5.13	5,026	ICMP Source Quench	5,026
4	206.65.191.129	4,908	Queso Fingerprint	4,895
5	65.165.14.43	4,668	SCAN Proxy Attempt	4,665
6	216.106.172.149	5,648	MISC Large UDP Packet	4,351
7	MY.NET.60.11	3,667	BACKDOOR NetMetro File List	3,586
8	65.207.94.30	3,661	ICMP Destination Unreachable (Communication Administratively Prohibited)	3,661
9	128.223.4.21	3,610	ICMP Echo Request BSDtype	3,475
10	141.213.11.120	3,460	ICMP Echo Request BSDtype	3,363

Alert Descriptions

Watchlist 000220 IL-ISDNNET-990517

These alerts were generated from traffic coming from Bezeq International, an ISP in Israel. Primarily, ninety-eight percent of the alerts came from 212.179.35.118. Since a watchset rule had been implemented for this network, it is likely that this network has been a source of interest in the past. Ninety-nine percent of the alerts were generated on December 25 & 26 to host MY.NET.70.70 on port 1214. This port is used by MusicCity's Morpheus (www.musiccity.com), a peer-to-peer file sharing application which, according the MusicCity, "allows users to search and find almost any type of digital file (audio, video, photos, reference data, reports, documents, etc.) through a secure peer-to-peer network unlike any other". This port is also used by KaZaA Media Desktop, a similar peer-to-peer file sharing application (www.kazaa.com).

Here is a sample from the alert file, alert_011225_gz.htm:

12/25-15:47:49.122291 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.35.118:60339 -> MY.NET.70.70:1214

MISC traceroute

The alerts were spread fairly evenly over the five days. Ninety-five percent of the alerts were to MY.NET.140.9 on ports 33450 to 33497 from a wide number of hosts. This port range is common for traceroutes. UNIX traceroute programs tend to start with UDP datagrams to port 33434 and increment by one for each successive packet. Since these programs usually send three packets, a destination host fifteen hops away would see packets at 33479 (33434 plus 45 (3 times 15)).

It's possible that the path to MY.NET.140.9 is being actively targeted. Or, it's possible that these ports are being used by some other programs or covert channels. Further investigation is warranted.

Here is a sample from the alert file, alert_011225_gz.htm:

12/25-00:01:10.945677 [**] MISC traceroute [**] 137.145.206.101:46735 -> MY.NET.140.9:33484

CS WEBSERVER – external web traffic

These alerts were likely triggered by normal HTTP traffic to the CS HTTP server. MY.NET.100.165. This host should be investigated to ensure that the traffic is normal and is not a port 80 exploit.

Here is a sample from the alert file, alert_011222_gz.htm:

12/22-00:01:56.824890 [**] CS WEBSERVER - external web traffic [**] 209.105.134.195:4132 -> MY.NET.100.165:80

MISC source port 53 to MY.NET.x.x:53

This is actually a combination of alerts to thirteen hosts on the MY.NET subnet. This could be normal traffic since port 53 to port 53 communications are common in DNS communications. These thirteen hosts should be investigated to ensure that no vulnerabilities have been exposed and that all security updates have been installed.

Here is a sample from the alert file, alert_011222_gz.htm:

12/22-00:01:45.247851 [**] MISC source port 53 to MY.NET.1.5:53

ICMP Echo Request BSDtype

This alert implied that ICMP echo requests from BSD systems were being detected. Similar detected are listed online at SANS (http://www.sans.org/y2k/090100.htm) and Netsys (http://www.netsys.com/suse-linux-security/2001/01/msg00227.html). The Netsys link describes bandwidth measuring traffic from companies to users. Some of the other alerts indicate that this was likely occurring. A number of the external hosts which generated these alerts, including 128.223.4.21 and 141.213.11.120, generated "MISC traceroute" alerts in conjunction with the "ICMP Echo Request BSDtype" alerts. It's likely that these hosts were measuring response times and hops to the internal hosts. These alerts could be further investigated if this type of traffic is of concern to the University.

Here is a sample from the alert file, alert_011222_gz.htm:

12/22-00:13:40.091776 [**] ICMP Echo Request BSDtype [**] 141.213.11.120 -> MY.NET.70.148

INFO MSN IM Chat data

The alerts were spread fairly evenly over the five days. The majority of the traffic involved the external hosts at 64.4.12.x which belongs to HotMail and is expected for MSN traffic.

Here is a sample from the alert file, alert_011223_gz.htm:

12/23-00:15:25.469643 [**] INFO MSN IM Chat data [**] 64.4.12.189:1863 -> MY.NET.97.202:4328

WEB-MISC prefix-get //

Ninety-three percent of this traffic was to MY.NET.253.114 on port 80. This host should be investigated to ensure that all patches are up to date and the logs should be analyzed to determine if any events appear to be suspicious.

Here is a sample from the alert file, alert_011223_gz.htm:

12/23-01:15:01.456242 [**] WEB-MISC prefix-get // [**] 196.40.43.219:46978 -> MY.NET.253.114:80

MISC Large UDP Packet

These alerts were mainly generated by two external hosts, 216.106.172.149 and 61.219.53.135, to MY.NET.153.210 on 12/22 and 12/23. The breakdown by these hosts is as follows:

Fifty-six percent of these alerts were from 216.106.172.149 to MY.NET.153.210:

- Two alerts were from port 0 to port 0
- 950 alerts were from port 2083 to port 3872 on 12/22 from 5:42:56 – 5:46:31 PM
- 3399 alerts were from port 54567 to port 1434 on 12/23 from 4:00:02 – 4:00:10 PM and from 4:16:02 – 5:21:49 PM

Twenty-five percent of these alerts were from 61.219.53.135 to MY.NET.153.210:

- Four alerts were from port 0 to port 0
- 1964 alerts were from port 1654 to port 3816 on 12/22 from 5:32:20 – 5:42:03 PM
- One alert was from port 39197 to port 51498 on 12/22 at 5:42:02 PM

This traffic appears to be suspicious and should be further investigated as should MY.NET.153.210.

Here is a sample from the alert file, alert_011222_gz.htm:

12/22-17:32:20.369527 [**] MISC Large UDP Packet [**] 61.219.53.135:1654 -> MY.NET.153.210:3816

SCAN Proxy attempt

The MY.NET network was being scanned for proxy servers. This is a fairly common scan as external hosts will look for proxy servers that can be used to mask their IP address. The external host 65.165.14.43 performed eighty-one percent of the scans, all of which occurred on 12/26. The internal hosts that were scanned the most were MY.NET.253.105 (fourteen percent of the scans) and MY.NET.98.202 (three percent of the scans). A deeper analysis is warranted to determine if any hosts on the MY.NET network are being improperly used as proxy servers.

Here is a sample from the alert file, alert_011226_gz.htm:

12/26-06:47:21.985513 [**] SCAN Proxy attempt [**] 65.165.14.43:4725 -> MY.NET.1.1:1080

The registration information for the host 65.165.14.43 from ARIN.NET is:

Sprint (NETBLK-SPRINTLINK-2-BLKS)
12502 Sunrise Valley Drive
Mailstop VARESA0104
Reston, VA 20196
US

Netname: SPRINTLINK-2-BLKS
Netblock: 65.160.0.0 - 65.174.255.255
Maintainer: SPRN

Coordinator:
Sprintlink (Sprint) (SPRINT-NOC-ARIN) NOC@SPRINT.NET
800-232-6895

SYSTEMS SOLUTIONS INC (NETBLK-FON-110133555275610)
2108 E THOMAS RD
PHOENIX, AZ 85016
US

Netname: FON-110133555275610
Netblock: 65.165.12.0 - 65.165.15.255

Coordinator:
Troxel, Dan (DT73-ARIN) dant@SYSPAC.COM
602-955-5566 (FAX) 6029550085

Record last updated on 05-Apr-2001.
Database last updated on 25-Jan-2002 19:56:21 EDT.

Queso fingerprint

Queso is tool which uses TCP fingerprinting to identify remote operating systems. It can be found at: http://www.apocalypseonline.com/security/tools/tools.asp?exp_category=Scanners. The host 206.65.191.129 generated ninety-five percent of the alerts on 12/26 and its primary target was MY.NET.98.177. Other alerts indicate the MY.NET.98.177 was using MSN's Instant Messenger and Gnuttella (a peer-to-peer file sharing program) so it's possible that this host peaked someone's interest, prompting them to run Queso. MY.NET.98.177 should be further investigated to determine if any compromises have occurred.

Here is a sample from the alert file, alert_011226_gz.htm:

12/26-02:33:01.293213 [**] Queso fingerprint [**] 206.65.191.129:46588 -> MY.NET.98.187:1000

The registration information for host 206.65.191.129 from ARIN.NET is:

UUNET Technologies, Inc. (NETBLK-NETBLK-UUNETCBLK64-67)
3060 Williams Drive, Suite 601
Fairfax, Virginia 22031

US

Netname: NETBLK-UUNETCBLK64-67
Netblock: 206.64.0.0 - 206.67.255.255
Maintainer: UU

Coordinator:
UUNET Postmaster (UUPM-ARIN) postmaster@uunet.uu.net
703-206-5440

Domain System inverse mapping provided by:

AUTH00.NS.UU.NET 198.6.1.65
AUTH01.NS.UU.NET 198.6.1.81

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 26-Sep-2001.
Database last updated on 25-Jan-2002 19:56:21 EDT.

ICMP Source Quench

A host will send ICMP Source Quench error messages when it is busy and is unable to keep up with the information it is receiving from other hosts. This error message asks to hosts to "please slow down". Ninety-eight percent of the ICMP Source Quench alerts were generated from MY.NET.5.13 to hosts on the MY.NET.200.0/24 subnet. MY.NET.5.13 should be investigated in an attempt to determine why it was sending the source quenches.

Here is a sample from the alert file, alert_011225_gz.htm:

12/25-00:01:09.960583 [**] ICMP Source Quench [**] MY.NET.5.13 -> MY.NET.200.23

SYN-FIN Scan!

All of the SYN-FIN Scan! alerts were generated on 12/25 by 24.0.28.234 on port 22. This host attempted a SYN-FIN Scan! to port 22 on many hosts on the MY.NET subnet, starting at MY.NET.1.2 and finishing at MY.NET.186.253. The alerts started at 9:50:40 PM and finished at 10:06:28 PM. Port 22 is commonly used for SSH logins.

Here is a sample from the alert file, alert_011225_gz.htm:

12/25-21:50:38.906742 [**] SYN-FIN scan! [**] 24.0.28.234:22 -> MY.NET.1.2:22

The registration information for 24.0.28.234 from ARIN.NET is:

@Home Network (NETBLK-ATHOME)
450 Broadway Street
Redwood City, CA 94063
US

Netname: ATHOME
Netblock: 24.0.0.0 - 24.23.255.255
Maintainer: HOME

Coordinator:
Operations, Network (HOME-NOC-ARIN) noc-abuse@noc.home.net
(650) 556-5599

This address is part of the network block used by cable modem subscribers in the @Home network. Since most @Home customers are DHCP clients, pinpointing the location of this host will require contacting @Home. @Home is currently in bankruptcy so it is unlikely that they will be willing to research the location of this host.

BACKDOOR NetMetro File List and BACKDOOR NetMetro Incoming Traffic

This description covers both the BACKDOOR NetMetro File List and BACKDOOR NetMetro Incoming Traffic alerts. BACKDOOR NetMetro is a trojan and its presence is definitely of concern. These internal hosts were listed in the alerts: MY.NET.130.123, MY.NET.60.11, and MY.NET.60.8. All hosts should be inspected for the existence of this and possibly other trojans. It should be noted that seventy-seven percent of the alerts occurred on 12/25.

Here are samples from the alert files, alert_011223_gz.htm and alert_011225_gz.htm:

12/23-14:41:01.829592 [**] BACKDOOR NetMetro Incoming Traffic [**] 193.252.200.136:5031 -> MY.NET.130.123:20
12/25-23:21:32.584622 [**] BACKDOOR NetMetro File List [**] MY.NET.60.11:20 -> 209.49.12.32:5032

ICMP Destination Unreachable (Communication Administratively Prohibited)

This alert usually occurs when a host is blocking this type of traffic due to certain rules. This is common on routers with access control lists blocking this type of

traffic. During these five days of alerts, over seventy-eight percent of the alerts were from 65.207.94.30 to MY.NET.137.7.

Here is a sample from the alert file, alert_011225_gz.htm:

12/25-00:02:00.316767 [**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**] 65.207.94.30 -> MY.NET.137.7

ICMP Destination Unreachable (Host Unreachable)

This alert usually occurs when a router receives a packet that it cannot deliver to the final destination because the router does not know the route to this destination. Host and host 63.146.1.33 had forty-five percent of the alerts, primarily to MY.NET.70.11, MY.NET.70.70, and MY.NET.137.7. Host 160.36.56.17 had thirty percent of the alerts, all to MY.NET.140.9.

Here is a sample from the alert file, alert_011226_gz.htm:

12/26-06:47:49.377047 [**] ICMP Destination Unreachable (Host Unreachable) [**] 63.146.1.33 -> MY.NET.70.11

ICMP Fragment Reassembly Time Exceeded

This alert occurs when a host reports that it cannot reassemble the fragments within the time limit. The host MY.NET.87.50 generated the majority of these alerts. This host was also involved in a number of port scans so more investigation needs to be performed with this host.

Here is a sample from the alert file, alert_011224_gz.htm:

12/24-04:34:38.210071 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.87.50 -> 195.249.246.249

Watchlist 000222 NET-NCFC

These alerts were generated from traffic coming from The Computer Network Center Chinese Academy of Sciences in Beijing, China. Since a watchset rule had been implemented for this network, it is likely that this network has been a source of interest in the past.

The majority of the traffic was to ports 80 (HTTP) and 25 (SMTP) on a number of hosts on the MY.NET network, with MY.NET.253.114, port 80 receiving eighty-six percent of the traffic. It's possible that this was normal traffic but the MY.NET hosts should be investigated to ensure that no vulnerabilities have been exploited and that all security patches are up-to-date.

Here is a sample from the alert file, alert_011222_gz.htm:

12/22-09:56:47.063994 [**] Watchlist 000222 NET-NCFC [**]
159.226.61.68:1852 -> MY.NET.253.114:80

External RPC call

The alerts indicate that many MY.NET systems were probed on 12/22 and 12/23 for the existence of the Remote Procedure Call (RPC) portmapper service. This service reports which services are running on the system. A number of vulnerabilities exist with this service so this issue should be further investigated. A comprehensive explanation can be found at http://www.sans.org/newlook/resources/IDFAQ/blocking.htm and a CERT advisory can be found at: http://www.cert.org/advisories/CA-2000-17.html.

Here is a sample from the alert file, alert_011223_gz.htm:

12/23-06:35:35.579960 [**] External RPC call [**] 208.7.170.44:111 ->
MY.NET.5.45:111

ICMP Echo Request Nmap or HPING2

Eighty-two percent of these alerts involved the external host 149.1.1.1. This should be further investigated since Nmap and HPING2 are OS fingerprinting and TCP scanning tools. Nmap can be found online at www.insecure.org and HPING2 can be found online at www.hping.org.

Here is a sample from the alert file, alert_011224_gz.htm:

12/24-01:30:54.901195 [**] ICMP Echo Request Nmap or HPING2 [**]
MY.NET.83.20 -> 149.1.1.1

INFO FTP anonymous FTP

These alerts indicate anonymous FTP traffic to a number of FTP hosts in the MY.NET network. The FTP servers should be investigated to ensure that they aren't being used as warez servers since it is common for anonymous FTP servers with no passwords to be compromised and used as warez sites.

Here is a sample from the alert file, alert_011223_gz.htm:

12/23-01:17:27.695448 [**] INFO FTP anonymous FTP [**]
24.249.181.184:10909 -> MY.NET.11.4:21

Scan Analysis

The scans indicate that a lot of gaming and peer-to-peer file sharing was present on this network. This correlates well with the information in the alert files. There are also a number of scans for HTTP, FTP, and DNS services which should be further investigated to determine if known vulnerabilities have been exploited and if trojan activity is present. The Stacheldraht distributed denial of service attack was also detected in these scan files.

The list of scan files used for this analysis were:

- scans_011222_gz.htm
- scans_011223_gz.htm
- scans_011224_gz.htm
- scans_011225_gz.htm
- scans_011226_gz.htm

The Top 15 Scans by Port

Scan Rank	Scanned Port	Scan Total	Description
1	27005	167,509	Port 27005/udp is the source (client) port used for the game Half-Life (www.sierra.com) and all of the scans were for port 27005/udp. The Autodesk network license manager (FLEXlm) runs on port 27005/tcp but there weren't any scans for this port.
2	1214	31,150	Port 1214/tcp is used by the peer-to-peer file sharing applications Morpheus (by MusicCity) and Media Desktop (by KaZaA). Ninety-eight percent of the scans were for port 1214/tcp.
3	6112	21,648	More than likely this scan was for some Internet games (like Battle.net) since all but twenty-eight of these scans were scanned for port 6112/udp. CERT advisory CA-2001-31 explains a vulnerability on port 6112/tcp with Sun Solaris systems running the CDE Subprocess Control Service so the hosts receiving this scan should be investigated for this vulnerability.
4	27500	20,311	All scans were for port 27500/udp and this is the default port for the game QuakeWorld (www.quakeworld.com).
5	22	18,353	Ports 22/udp and 22/tcp are the default ports

			for the SSH remote login protocol. Nearly twenty-five percent of these scans had both the SYN and FIN flags set.
6	21	18,233	Port 21/tcp received 18,232 scans and port 21/udp received one scan. Port 21/tcp scans are common since this port is the default port for FTP servers.
7	60001	7,952	Stacheldraht, a distributed denial of service tool, uses port 60001/tcp. All scans were to port 60001/tcp by 210.77.145.30 on port 46138. The scans were to sequential hosts on the MY.NET network starting at MY.NET.1.0 and ending at MY.NET.254.99. This entire scan occurred in 33 seconds.
8	1080	4,610	This was a scan for proxy servers and/or the WinHole trojan on port 1080/tcp.
9	53	4,174	This is the common DNS server scan.
10	4665	3,924	Port 4665/udp is used by eDonkey, a peer-to-peer file sharing program (www.edonkey2000.com).
11	6346	3,615	Port 6346/tcp and 6346/udp are used for Gnutella, a peer-to-peer file sharing program
12	27010	3,411	Port 27010 is the port of the Half-Life Master Server.
13	80	3,061	Port 80/tcp is the standard port for HTTP servers.
14	25	2,921	Port 25/tcp is the standard port for SMTP servers.
15	1025	2,722	Port 1025/ucp is used for the game network blackjack and for the trojan Remote Storm

Top 10 Scan Talkers

Talker Rank	IP Address	Scan Total	Top Ports(s) Scanned	Top Port(s) Scanned Total
1	MY.NET.87.50	331,649	27005, 27500, 27010	191,200
2	MY.NET.98.203	27,085	4901, 5401, 13201	6,679
3	211.248.231.10	9,876	22	9,876
4	65.165.14.43	9,508	1080, 21	9,112
5	210.77.145.30	7,952	60001	7,952
6	210.58.102.186	7,680	21	7,680
7	204.152.184.75	6,143	Scanned entire port range	N/A

			multiple times	
8	24.44.21.206	5,412	21	5,412
9	24.0.28.234	5,072	22	5,072
10	MY.NET.84.185	4,075	4665	3,275

The registration information from APNIC.NET for the host which initiated the Stacheldraht distributed denial of service attack, 210.77.145.30, is:

inetnum 210.77.128.0 - 210.77.159.255
netname A-1
descr A-1.Net China Inc.
country CN
admin-c SC142-AP, inverse
tech-c WH46-AP, inverse
mnt-by MAINT-CNNIC-AP, inverse
changed zwh@cnnic.net.cn 19991028
source APNIC

person Sheng Chen, inverse
address 20/F, Jingtai Tower, No.24, Jianguomenwai Avenue, Beijing, P.R.China
country CN
phone +86-010-65675678
fax-no +86-010-65674567
e-mail wkn@a-1.net.cn, inverse
nic-hdl SC142-AP, inverse
mnt-by MAINT-CN-WANGZJ, inverse
changed wangzj@staff.a-1.net 20000406
source APNIC

person Wei He, inverse
address 20/F,Jingtai Tower,No 24,Jianguomenwai Avenue
country CN
phone +86-10-65675678
fax-no +86-10-65674567
e-mail hhew@a-1.net.cn, inverse
nic-hdl WH46-AP, inverse
mnt-by MAINT-CN-WANGZJ, inverse
changed wangzj@staff.a-1.net 20000406
source APNIC

The APNIC.NET registration information for host 211.248.231.10, which initiated over 9,000 scans to port 22, is:

inetnum 211.232.0.0 - 211.255.255.255
netname KRNIC-KR
descr KRNIC
descr Korea Network Information Center
country KR
admin-c HM127-AP, inverse
tech-c HM127-AP, inverse
remarks **
remarks KRNIC is the National Internet Registry
remarks in Korea under APNIC. If you would like to
remarks find assignment information in detail
remarks please refer to the KRNIC Whois DB
remarks http://whois.nic.or.kr/english/index.html
remarks **
mnt-by APNIC-HM, inverse
mnt-lower MNT-KRNIC-AP, inverse
changed hostmaster@apnic.net 20000908
changed hostmaster@apnic.net 20010627
source APNIC

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

Out of Spec (OOS)

Over ninety-five percent of the OOS records were SYN-FIN scans. Over ninety-nine percent of these SYN-FIN scans occurred on 12/25 by 24.0.28.234. This is covered further in the SYN-FIN Scan! description in the Alerts section.

Of the remain five percent of OOS records, ninety percent had the two reserved, high-order TCP bits set and the Type of Service (TOS) set to 0x0. This is typical of an OS fingerprinting tool like Queso. While having these bits set is common in

environments using ECN (Explicit Congestion Notification), having a non-zero TOS indicates that these records were out of spec.

The list of OOS files used for this analysis were:

- oos_Dec_22_2001_gz.htm
- oos_Dec_23_2001_gz.htm
- oos_Dec_24_2001_gz.htm
- oos_Dec_25_2001_gz.htm
- oos_Dec_26_2001_gz.htm

Analysis Process Description

The process that I used to analyze the data was different than the other practicals that I read. Each file was first opened in Microsoft Word and the records were run through a couple of search-and-replace steps to delimit the date, time, the alert (in the alert files), the source, and the destination. This file was saved as a text file and then opened in Microsoft Excel to delimit the source ports and destination ports since delimiting these fields in Word would have resulted in delimiting the hour, minute, and second. While delimiting the hour, minute, and second would not have been bad, my desire was to keep the time field as just one field. It should be noted that Excel has a limit of 65535 rows so some files had to be split into multiple files. Each of the finished Excel files were saved as comma delimited files.

These comma delimited files were then imported into newly created databases in Microsoft's SQL Server. The delimited files from the alerts were imported into a single table in one database and the delimited files from the scans were imported into a single table in a different database. Importing the files into single tables was done to simplify the reporting and SQL queries that were soon to come.

The alert and scan totals listed in the tables above were all derived from Crystal Reports run against the alert table and scan table. The numerical analysis in the descriptions was determined by a couple of different methods. In most cases, more Crystal Reports were written. In other cases, data was exported from the SQL Server tables to text files for further analysis in Excel. And in some other cases, Windows Grep (www.wingrep.com) was used.

The OOS files didn't contain much data so extensive manipulation in Word, Excel, and SQL Server was not needed. The files were visually inspected and Windows Grep was used to generate record totals.

Security Recommendations

This University should install a firewall and a packet logger if these are not already in place. These devices should be configured so that their logs and the Snort logs can be correlated as best as possible (time synchronization is the first step). The firewall and router should be configured to pass traffic deemed acceptable in the University's security policy. If a security policy has not been written, one should be written immediately. Since gaming generated a huge number of alert and scan records, the University should evaluate if it deems this type of traffic as acceptable. After these systems are in place, the security policy, firewall, and router rules should be evaluated on a routine basis and updated as needed.

All systems run by the University should subject to a port scan and a vulnerability assessment if possible. Unnecessary services and ports should be removed or disabled. All systems run by the University should be evaluated to determine if the security patches are up-to-date. If a "system touch" log has not yet been implemented, one should be implemented immediately.

The SANS Institute (www.sans.org) has a number of articles and references on all of these recommendations.

References

O'Reilly Network: Morpheus Out of the Underworld.
URL: http://www.openp2p.com/lpt/a/p2p/2001/07/02/morpheus.html

MusicCity Morpheus
URL: http://www.musiccity.com

KaZaA Media Desktop
URL: http://www.kazaa.com

SANS Institute Resources, Global Incident Analysis Center, Detects Analyzed 9/1/00
URL: http://www.sans.org/y2k/090100.htm

NETSYS.COM SuSE Linux Security Mailing List Archives
URL: http://www.netsys.com/suse-linux-security/2001/01/msg00227.html

American Registry for Internet Numbers
URL: http://www.arin.net

Queso application on Apocalypse Online Security

URL:
http://www.apocalypseonline.com/security/tools/tools.asp?exp_category=Scanners

SANS Institute, Intrusion Detection FAQ, Is blocking port 111 sufficient to protect your systems from RPC attacks?
URL: http://www.sans.org/newlook/resources/IDFAQ/blocking.htm

CERT Advisory CA-2000-17 Input Validation Problem in rpc.statd
URL: http://www.cert.org/advisories/CA-2000-17.html

Insecure.Org -- Nmap Free Stealth Network Port Scanner, Linux/Windows/UNIX/Solaris Tools & Hacking
URL: http://www.insecure.org

Hping home page
URL: http://www.hping.org

Sierra Website (Half-Life game)
URL: http://www.sierra.com

Battle.net News Website
URL: http://www.battle.net

CERT Advisory CA-2001-31 Buffer Overflow in CDE Subprocess Control Service
URL: http://www.cert.org/advisories/CA-2001-31.html

PlanetQuake
URL: http://www.quakeworld.com

SANS Institute, Global Incident Analysis Center: Special Notice – TheStacheldraht Distributed Denial of Service Attack Tool.
URL: http://www.sans.org/y2k/stacheldraht.htm

G-Lock Software, Trojan List, WinHole.
URL: http://www.glocksoft.com/trojan_list/WinHole.htm

G-Lock Software, Trojan List, Remote Storm
URL: http://www.glocksoft.com/trojan_list/Remote_Storm.htm

eDonkey 2000.
URL: http://www.edonkey2000.com

Gnutella.com
URL: http://www.gnutella.com

Snort - The Open Source Network IDS
URL: http://www.snort.org

Asia Pacific Network Information Centre
URL: http://www.apnic.net

Cisco - Implementing Quality of Service Policies with DSCP
URL: http://www.cisco.com/warp/public/105/dscpvalues.html

Windows Grep
URL: http://www.wingrep.com

Lajon, Gregory. GCIA Practical.
URL: http://www.giac.org/practical/Gregory_Lajon_GCIA.doc

Currie, Robert. GCIA Practical.
URL: http://www.giac.org/practical/Robert_Currie.doc

Yuen, Rick Wenkey. GCIA Practical.
URL: http://www.giac.org/practical/Rick_Yuen_GCIA.doc

Partee, Elvis Moe. GCIA Practical.
URL: http://www.giac.org/practical/Elvis_Moe_Partee_GCIA.zip

Goodwin, PJ. GCIA Practical.
URL: http://www.giac.org/practical/PJ_Goodwin_GCIA.doc

Jenkinson, John. GCIA Practical.
URL: http://www.giac.org/practical/John_Jenkinson_GCIA.doc

Woodroffe, Alan. GCIA Practical.
URL: http://www.giac.org/practical/Alan_Woodroffe_GCIA.doc

Last Updated: October 18th, 2017

Upcoming Training

SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced