GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

SANS/GIAC Certifications:
Track 3 – Intrusion Detection In-Depth

Practical Assignment
Version 3.3

Submittted May 28th, 2003

By Andrew J. Patrick
In pursuit of GCIA Certification

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract:

This paper is submitted for the GCIA Version 3.3 Practical.

It consists of three parts:

1) Customized IDS Signature Creation: Why you aren't using your IDS to its full potential - One of the more under-utilized capabilities of most modern Intrusion Detection Systems (IDS) is the ability of the organization to "roll their own" customized network traffic patterns for the IDS to sniff for. This may not sound like much of an innovation to some of the more expert members of the Intrusion Detection Community, but after close examination of how IDS is implemented in several organizations, I have become convinced that this may be the single biggest "bang-for-buck" improvement available. By following the few simple and cost-effective steps I will outline in this paper, any reasonably competent IDS analyst should be able to greatly improve the value of intrusion intelligence that their IDS provides to their organization.

2) Three "10 step standard format" SANS/GIAC Intrusion Analysis detects:

Detect #1 – Front Page Extensions & Anonymous FTP

Detect #2 – A Visit from a Curious Friend

Detect # 3 – "It's Code Red! No, It's Nimda! No, it's, it's….???"

3) "Analyze This!" assignment. the University is confronted with three major issues with regard to its Intrusion Detection efforts: 1) There is far too much "noise" being generated by the IDS system. The majority of the alerts being generated appear to due to benign traffic, mis-configured hosts or IDS rules, and some customized alerts that do not appear to serve any useful function. This has the deleterious effect of swamping both the IDS sensors and the Analyst's bandwidth. 2) The use of peer-to-peer networks such as Gnutella, Morpheus, and Kazaa is obviously quite widespread at the University. Rampant uncontrolled use of P2P networks is becoming much more controversial and potentially costly, as the Recording Industry Association of America has recently begun mounting major legal challenged to educational institutions which turn a blind eye to the resulting inevitable theft of copyrighted material. This uncontrolled file-sharing also constitutes a serious abuse of the University's Internet capacity, which is quite likely to be interfering with much more legitimate bandwidth demands.
3) There are indications that several University systems may have been compromised by worms and/or external attackers. These should be examined immediately for any signs of potential compromise by the University's InfoSec personnel.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 1:
Customized IDS Signature Creation:
Why you aren't using your IDS to its full potential

One of the more under-utilized capabilities of most modern Intrusion Detection Systems (IDS) is the ability of the organization to "roll their own" customized network traffic patterns for the IDS to sniff for. This may not sound like much of an innovation to some of the more expert members of the Intrusion Detection Community, but after close examination of how IDS is implemented in several organizations, I have become convinced that this may be the single biggest "bang-for-buck" improvement available. By following the few simple and cost-effective steps I will outline in this paper, any reasonably competent IDS analyst should be able to greatly improve the value of intrusion intelligence that their IDS provides to their organization.

For motivation, I would first like to consider the reasons we would want to customize our own IDS in the first place. I believe that the single most significant obstacle to the proper use of IDS technology in Corporate America is the tendency to treat it (and, indeed, many forms of information technology) as a "black box" – i.e., plug it in, turn it on and wait for it to do its thing. In general, this is a poor way to implement technology, and it is an extremely poor way to implement IDS technologies. IDS excels at identifying unique threat patterns in massive amounts of data whizzing by its sensors, so why not train your IDS to look for those unique patterns that pose the greatest threat to your particular organization? (This is not something a "black box" will ever be capable of doing. The bad news is that we have to do a little bit of work here)

For example, suppose there is an evil competitor or disgruntled former employee you suspect may be seeking to do you harm. Also suppose that you are aware of some unique pattern that an attack from this evil entity would possess (say, a source IP address or the employee's former userid). Why not program this info into your IDS system as a customized alert? Isn't this exactly the sort of function your IDS is supposed to serve?

Some critics may argue that this would be an undue invasion of privacy, or that by doing this, we may generate a lot of bogus alerts. To the first point, I argue that this is conceptually no different from looking at the signature for Code Red, Nimda or any of the numerous other nasties that we know to be bona fide threats to the information security of our organizations. The second criticism is a much better point, as IDS are very prone to false positives, and that is precisely why I am emphasizing that that the signatures in question need to be UNIQUE to the threat involved. As Intrusion Analysts, we've become quite familiar with the experience of wading through large numbers of false positive alerts. However, my experience is that there are in fact unique signatures that can be utilized (and sometimes even self-generated!) that can alert to real threats whilst keeping false positives to a bare minimum.

Let's examine some situations where customized IDS alerts prove useful.

Example 1 – Major new threat emerges, IDS vendor does not yet have signature available:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In this case, the organization becomes aware of the new threat via the news media, or perhaps a distribution list such as BugTraq. The IDS Analyst checks for an updated signature from the vendor, but it has not yet been released (it is not unusual for several days to pass before the major commercial IDS vendors release signatures for major new threats, and even longer for lesser threats).

Not to fear. All our intrepid IDS analyst requires is some unique set of characteristics describing the new threat and she can easily fabricate her own customized signature. The recently discovered SendMail vulnerability is an excellent example. As of this writing, many commercial IDS vendors have not yet released a detect signature for this particular vulnerability, even though the existence of published exploit code has been reported in the mass media (MSNBC, Cnet, etc).

This sounds very worrisome, but the fact that there is published exploit code is actually a boon to the creative IDS analyst who is willing to create her own alerts! The exploit code should give us the exact pattern we need to build our custom signature.

A very recent (and quite amusing example) of how quickly the Intrusion Detection community can respond to the emergence of new information was seen on April 1st, 2003 with the release of "RFC 3514: The Security Flag in the IPv4 Header" by S. Bellovin of AT&T Labs Research. (ftp://ftp.rfc-editor.org/in-notes/rfc3514.txt). While the entire RFC is clearly intended as a tongue-in-cheek April Fool's prank, the immediate responses from various IDS practitioners were stunning in their ingenuity (and humor). My personal favorite was the following customized Snort signature, posted by Edward Southcote-Want southcotewant@yahoo.co.uk, within a few hours of the time the original "RFC" was made public on April 1st.

```
alert tcp $EXTERNAL_NET 80 -> $ANY_NET
(msg:"Here PigE, PigE; Here PigE, PigE"; flags: E+; content:"Evil";
reference:arachnids,03; sid:666; classtype:bad-unknown; rev:3;)
```

Example 2 – Detecting Self-Generated Coded Signals from Home Grown Applications:

IDS are a relatively new technology in the corporate world, so it is not all that surprising that application development has largely ignored their existence. But, what if our organization's applications and automated scripts were designed to be "IDS aware"?

Quite recently, an Application Security Analyst colleague brought an interesting question to me. It appeared that a proposed new application would likely have very weak passwords, and he had a (very valid) concern that it would be highly vulnerable to brute-force attacks. He asked me to verify that if this application was designed to send out a very unique data string upon a certain number of bad passwords attempts, could we then program our IDS to detect that same string and alert us when a potential brute-force attack is in progress. By making the data string as unique as possible, we could reduce the likelihood of false positive to be virtually nil. My response was something along the lines of: "Sure, that's simple!"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In order to simulate this process, we generated a random string of sixteen hex characters, which we then incorporated into one of our Real Secure sensors. The beauty of this concept is that, provided we have the ability to program our applications to generate a specific pattern, we can tune our IDS systems to be on the alert for that exact same string. We can (and should) make this pattern something that would be virtually impossible to occur solely by random chance.

We assumed that the application would be sending this custom string as part of a URL data-stream to a web-server on one of our IDS monitored subnets. The actual destination is really not important; all that really matters here is that the IDS sensor see the ASCII string on the wire.

Note that this is not a theoretical discussion by any means, we have **actually implemented** this on a Real Secure sensor responsible for monitoring activity on the internal network segment in my organization. It has yet to produce a single false positive, but has correctly fired on the sixteen character string every time we have tested it.

A customized Snort rule incorporating this same technique looks like this:

```
alert tcp $DMZ_NET 80 -> $DMZ_SENSOR
(msg "TAT_App: Possible Brute Force Attack !";
content: "22f867a5d4d488417b47a0bbbbe80863bdec569e";
classtype: custom; rev:1;)
```

Here, “TAT” is the name of the internal application, which lives on a web-server on the DMZ_NET subnet. The application is programmed to automatically send a packet containing the hex string "22f867a5d4d488417b47a0bbbbe80863bdec569e" to the existing IDS sensor located on the same DMZ, upon the detection of possible brute force attacks. The IDS will take it from there, sending out the appropriate alerts and logging the attack to the database.

Through this process, we demonstrate that, by generating a totally random string of sufficient length, it is possible to design “IDS aware” alerts into home-grown applications and scripts that are effective warning mechanisms and have extremely low probability of generating false positives.

Example 3 – Detecting Potential Attacks from Organization-Specific Threats:
Each organization faces its own unique set of information security risks. This could take the form of a disgruntled former employee, a major competitor set on corporate espionage, or even an irate customer trying to deface a website. By molding our customized IDS alerts to match the profile of the threats affecting our organization, we can much more accurately detect the relevant events of interest.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In the case of the disgruntled former employee, we are likely to know a bit about what an attempted logon attempt from this individual would look like. We certainly know her userid (hopefully now disabled!), and may have other relevant information in our logs, such as home IP address(es), and home computer name(s). Since we have this information, why not use it? It is trivial to program these few facts into a set of customized alerts in our IDS, yet it could potentially provide us with extremely valuable warning that an attack was in progress. Additionally, the IDS logs of any trespass by this individual could prove to be bona fide evidence in a subsequent criminal prosecution.

For example, consider the following customized Snort rule:

```
alert tcp $ANY_NET -> $WIN_DOM_CONTROLLER
(msg "Disgruntled Ex-Employee Logon Attempt!";
content: " joe_angry [Windows user-id of employee]";
classtype: custom; rev:1;)
```

Summary –

Customized IDS signatures represent an extememely powerful detection enhancement, allowing the IDS analyst to tailor their systems to the unique needs of their organization. The astute IDS analyst should become adept at writing and implementing customized rules in order to maximize their organization's return on investment in their intrusions detection systems.

Customized signatures can detect brand new or emerging threats for which the IDS vendor has not yet released a signature. They can be used to detect organization-specific threats, such as access attempts generated by a disgruntled former employee or a competitor. They can even be used to enhance the security of internal applications if such applications can be designed and developed in an "IDS-aware" manner.

Clearly, the ability to customize IDS signatures brings many benefits to the table. The wise IDS analyst will cultivate their signature customization skill set to take advantage of these benefits.

References for Assignment #1:

1) *Snort Users Manual, Snort Release: 2.0.0,* Roesch & Green, http://www.snort.org/docs/writing_rules/

2) "Writing rules and understanding alerts for Snort, a network intrusion detection system", http://www.cert.org/security-improvement/implementations/i042.14.html

3) "Snort Installation & Usage, Part 2", Coddington, for SecurityFocus.Com – http://www.securityfocus.com/infocus/1422

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4) *Incident Response*, van Wyk & Forno, August 2001, O'Reilly Press.

5) *Network Intrusion Detection, 2nd Edition*, Northcutt & Novak, September 2000, New Riders Press.

6) *Intrusion Signatures and Analysis*, Northcutt, Cooper, et.al., January, 2001, New Riders Press.

© SANS Institute 2003, Author retains full rights.

Assignment # 2 –
Analysis of Three IDS Detects:

Detect #1 –
Front Page Extensions & Anonymous FTP:

```
07:41:39.834488 IP adsl-211-78-179-19.TYON.sparqnet.net.64874 > 46.5.180.133.21: P
557163300:557163316(16) ack 424442759 win 64208 (DF)
0x0000  4500 0038 4a0a 4000 6906 64cf d34e b313      E..8J.@.i.d..N..
0x0010  2e05 b485 fd6a 0015 2135 a324 194c 7b87      .....j..!5.$.L{.
0x0020  5018 fad0 737b 0000 5553 4552 2061 6e6f      P...s{..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

08:47:48.554488 IP 207.178.214.186.3157 > 46.5.180.133.21: P 3660070479:3660070495(16)
ack 337602424 win 16497 (DF)
0x0000  4500 0038 685b 4000 6e06 2173 cfb2 d6ba      E..8h[@.n.!s....
0x0010  2e05 b485 0c55 0015 da28 3e4f 141f 6778      .....U...(>O..gx
0x0020  5018 4071 c403 0000 5553 4552 2061 6e6f      P.@q....USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:11.584488 IP 207.178.214.168.4010 > 46.5.180.133.21: P 2039960623:2039960639(16)
ack 1623707048 win 8217 (DF)
0x0000  4500 0038 f5e0 4000 6e06 93ff cfb2 d6a8      E..8..@.n.......
0x0010  2e05 b485 0faa 0015 7997 542f 60c7 cda8      ........y.T/`...
0x0020  5018 2019 78f1 0000 5553 4552 2061 6e6f      P...x...USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:12.674488 IP 207.178.214.220.3911 > 46.5.180.133.21: P 1093920734:1093920750(16)
ack 1628754634 win 16497 (DF)
0x0000  4500 0038 3dfd 4000 6e06 4baf cfb2 d6dc      E..8=.@.n.K.....
0x0010  2e05 b485 0f47 0015 4133 e7de 6114 d2ca      .....G..A3..a...
0x0020  5018 4071 f80d 0000 5553 4552 2061 6e6f      P.@q....USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:13.284488 IP 207.178.214.156.4749 > 46.5.180.133.21: P 993837810:993837826(16)
ack 1625276195 win 8217 (DF)
0x0000  4500 0038 e1f3 4000 6e06 a7f8 cfb2 d69c      E..8..@.n.......
0x0010  2e05 b485 128d 0015 3b3c c2f2 60df bf23      ........;<..`..#
0x0020  5018 2019 541f 0000 5553 4552 2061 6e6f      P...T...USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:16.914488 IP 207.178.214.223.3593 > 46.5.180.133.21: P 1617729588:1617729604(16)
ack 1636177237 win 8217 (DF)
0x0000  4500 0038 ce63 4000 6e06 bb45 cfb2 d6df      E..8.c@.n..E....
0x0010  2e05 b485 0e09 0015 606c 9834 6186 1555      ........`l.4a..U
0x0020  5018 2019 0716 0000 5553 4552 2061 6e6f      P.......USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:18.454488 IP 207.178.214.228.2801 > 46.5.180.133.21: P 1442445886:1442445902(16)
ack 1637249967 win 8217 (DF)
0x0000  4500 0038 67fa 4000 6e06 21aa cfb2 d6e4      E..8g.@.n.!.....
0x0010  2e05 b485 0af1 0015 55f9 fa3e 6196 73af      ........U..>a.s.
0x0020  5018 2019 5427 0000 5553 4552 2061 6e6f      P...T'..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

09:08:26.904488 IP 207.178.214.186.1052 > 46.5.180.133.21: P 3249564905:3249564921(16)
ack 1637741999 win 16497 (DF)
0x0000  4500 0038 ed90 4000 6e06 9c3d cfb2 d6ba      E..8..@.n..=....
0x0010  2e05 b485 041c 0015 c1b0 6ce9 619d f5af      ..........l.a...
0x0020  5018 4071 da64 0000 5553 4552 2061 6e6f      P.@q.d..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
10:02:57.614488 IP eatkyo187118.adsl.ppp.infoweb.ne.jp.1480 > 46.5.180.133.21: P
3707753065:3707753081(16) ack 754907336 win 64177 (DF)
0x0000  4500 0038 3b81 4000 2a06 e961 dae2 7476      E..8;.@.*..a..tv
0x0010  2e05 b485 05c8 0015 dcff d269 2cfe f8c8      ...........i,...
0x0020  5018 fab1 2643 0000 5553 4552 2061 6e6f      P...&C..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

11:22:07.554488 IP pD955A17C.dip.t-dialin.net.2852 > 46.5.180.133.21: P
5766169:5766185(16) ack 1507047257 win 9936 (DF)
0x0000  4500 0038 a681 4000 1306 69e8 d955 a17c      E..8..@...i..U.|
0x0010  2e05 b485 0b24 0015 0057 fc19 59d3 b759      .....$...W..Y..Y
0x0020  5018 26d0 90e2 0000 5553 4552 2061 6e6f      P.&.....USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

11:22:16.714488 IP pD955A17C.dip.t-dialin.net.2854 > 46.5.180.133.21: P
5775336:5775352(16) ack 1526466325 win 9936 (DF)
0x0000  4500 0038 bb81 4000 1306 54e8 d955 a17c      E..8..@...T..U.|
0x0010  2e05 b485 0b26 0015 0058 1fe8 5afc 0715      .....&...X..Z...
0x0020  5018 26d0 1c2d 0000 5553 4552 2061 6e6f      P.&..-..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

18:34:49.644488 IP 203.241.151.50.60592 > 46.5.180.133.80: P
3832713821:3832714083(262) ack 2125416356 win 65535 <nop,nop,timestamp 4461199
7368629>
0x0000  4500 013a 4178 0000 3006 089e cbf1 9732      E..:Ax..0......2
0x0010  2e05 b485 ecb0 0050 e472 925d 7eaf 47a4      .......P.r.]~.G.
0x0020  8018 ffff 502d 0000 0101 080a 0044 128f      ....P-.......D..
0x0030  0070 6fb5 4745 5420 2f5f 7674 695f 696e      .po.GET./_vti_in
0x0040  662e 6874 6d6c 2048 5454 502f 312e 300d      f.html.HTTP/1.0.
0x0050  0a44 6174 653a 2053 6174 2c20 3133 204a      .Date:.Sat,.13.J
0x0060  756c 2032 3030 3220 3031 3a34 353a 3432      ul.2002.01:45:42
0x0070  2047 4d54 0d0a 4d49 4d45 2d56 6572 7369      .GMT..MIME-Versi
0x0080  6f6e 3a20 312e 300d 0a41 6363 6570 743a      on:.1.0..Accept:
0x0090  202a 2f2a 0d0a 5573 6572 2d41 6765 6e74      .*/*..User-Agent
0x00a0  3a20 4d6f 7a69 6c6c 612f 322e 3020 2863      :.Mozilla/2.0.(c
0x00b0  6f6d 7061 7469 626c 653b 204d 5320 4672      ompatible;.MS.Fr
0x00c0  6f6e 7450 6167 6520 342e 3029 0d0a 486f      ontPage.4.0)..Ho
0x00d0  7374 3a20 7777 772e 5858 5858 2e63 6f6d      st:.www.XXXX.com
0x00e0  0d0a 4163 6365 7074 3a20 6175 7468 2f73      ..Accept:.auth/s
0x00f0  6963 696c 790d 0a43 6f6e 7465 6e74 2d4c      icily..Content-L
0x0100  656e 6774 683a 2030 0d0a 5072 6167 6d61      ength:.0..Pragma
0x0110  3a20 6e6f 2d63 6163 6865 0d0a 4361 6368      :.no-cache..Cach
0x0120  652d 436f 6e74 726f 6c3a 206d 6178 2d73      e-Control:.max-s
0x0130  7461 6c65 3d30 0d0a 0d0a                     tale=0....

18:34:50.944488 IP 203.241.151.50.61193 > 46.5.180.133.80: P
3390767304:3390767693(389) ack 2126797398 win 65535 <nop,nop,timestamp 4461202
7368758>
0x0000  4500 01b9 5e6c 0000 3006 eb2a cbf1 9732      E...^l..0..*...2
0x0010  2e05 b485 ef09 0050 ca1b 00c8 7ec4 5a56      .......P....~.ZV
0x0020  8018 ffff 9b37 0000 0101 080a 0044 1292      .....7.......D..
0x0030  0070 7036 504f 5354 202f 5f76 7469 5f62      .pp6POST./_vti_b
0x0040  696e 2f73 6874 6d6c 2e65 7865 2f5f 7674      in/shtml.exe/_vt
0x0050  695f 7270 6320 4854 5450 2f31 2e30 0d0a      i_rpc.HTTP/1.0..
0x0060  4461 7465 3a20 5361 742c 2031 3320 4a75      Date:.Sat,.13.Ju
0x0070  6c20 3230 3032 2030 313a 3435 3a34 3320      l.2002.01:45:43.
0x0080  474d 540d 0a4d 494d 452d 5665 7273 696f      GMT..MIME-Versio
0x0090  6e3a 2031 2e30 0d0a 5573 6572 2d41 6765      n:.1.0..User-Age
0x00a0  6e74 3a20 4d53 4672 6f6e 7450 6167 652f      nt:.MSFrontPage/
0x00b0  342e 300d 0a48 6f73 743a 2077 7777 2e58      4.0..Host:.www.X
0x00c0  5858 582e 636f 6d0d 0a41 6363 6570 743a      XXX.com..Accept:
0x00d0  2061 7574 682f 7369 6369 6c79 0d0a 436f      .auth/sicily..Co
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x00e0  6e74 656e 742d 4c65 6e67 7468 3a20 3431       ntent-Length:.41
0x00f0  0d0a 436f 6e74 656e 742d 5479 7065 3a20       ..Content-Type:.
0x0100  6170 706c 6963 6174 696f 6e2f 782d 7777       application/x-ww
0x0110  772d 666f 726d 2d75 726c 656e 636f 6465       w-form-urlencode
0x0120  640d 0a58 2d56 6572 6d65 6572 2d43 6f6e       d..X-Vermeer-Con
0x0130  7465 6e74 2d54 7970 653a 2061 7070 6c69       tent-Type:.appli
0x0140  6361 7469 6f6e 2f78 2d77 7777 2d66 6f72       cation/x-www-for
0x0150  6d2d 7572 6c65 6e63 6f64 6564 0d0a 5072       m-urlencoded..Pr
0x0160  6167 6d61 3a20 6e6f 2d63 6163 6865 0d0a       agma:.no-cache..
0x0170  4361 6368 652d 436f 6e74 726f 6c3a 206d       Cache-Control:.m
0x0180  6178 2d73 7461 6c65 3d30 0d0a 0d0a 6d65       ax-stale=0....me
0x0190  7468 6f64 3d73 6572 7665 722b 7665 7273       thod=server+vers
0x01a0  696f 6e25 3361 3425 3265 3025 3265 3225       ion%3a4%2e0%2e2%
0x01b0  3265 3236 3131 0a0d 0a                        2e2611...

18:44:18.214488 IP 203.241.151.50.60802 > 46.5.180.133.80: P 475005787:475006049(262)
ack 2726606846 win 65535 <nop,nop,timestamp 4462337 7425481>
0x0000  4500 013a 2bb1 0000 3006 1e65 cbf1 9732       E..:+...0..e...2
0x0010  2e05 b485 ed82 0050 1c50 035b a284 b7fe       .......P.P.[....
0x0020  8018 ffff 32cb 0000 0101 080a 0044 1701       ....2........D..
0x0030  0071 4dc9 4745 5420 2f5f 7674 695f 696e       .qM.GET./_vti_in
0x0040  662e 6874 6d6c 2048 5454 502f 312e 300d       f.html.HTTP/1.0.
0x0050  0a44 6174 653a 2053 6174 2c20 3133 204a       .Date:.Sat,.13.J
0x0060  756c 2032 3030 3220 3031 3a35 353a 3130       ul.2002.01:55:10
0x0070  2047 4d54 0d0a 4d49 4d45 2d56 6572 7369       .GMT..MIME-Versi
0x0080  6f6e 3a20 312e 300d 0a41 6363 6570 743a       on:.1.0..Accept:
0x0090  202a 2f2a 0d0a 5573 6572 2d41 6765 6e74       .*/*..User-Agent
0x00a0  3a20 4d6f 7a69 6c6c 612f 322e 3020 2863       :.Mozilla/2.0.(c
0x00b0  6f6d 7061 7469 626c 653b 204d 5320 4672       ompatible;.MS.Fr
0x00c0  6f6e 7450 6167 6520 342e 3029 0d0a 486f       ontPage.4.0)..Ho
0x00d0  7374 3a20 7777 772e 5858 5858 2e63 6f6d       st:.www.XXXX.com
0x00e0  0d0a 4163 6365 7074 3a20 6175 7468 2f73       ..Accept:.auth/s
0x00f0  6963 696c 790d 0a43 6f6e 7465 6e74 2d4c       icily..Content-L
0x0100  656e 6774 683a 2030 0d0a 5072 6167 6d61       ength:.0..Pragma
0x0110  3a20 6e6f 2d63 6163 6865 0d0a 4361 6368       :.no-cache..Cach
0x0120  652d 436f 6e74 726f 6c3a 206d 6178 2d73       e-Control:.max-s
0x0130  7461 6c65 3d30 0d0a 0d0a                      tale=0....

18:44:19.334488 IP 203.241.151.50.61384 > 46.5.180.133.80: P
1493364766:1493365155(389) ack 2720916284 win 65535 <nop,nop,timestamp 4462339
7425594>
0x0000  4500 01b9 5216 0000 3006 f780 cbf1 9732       E...R...0......2
0x0010  2e05 b485 efc8 0050 5902 f01e a22d e33c       .......PY....-.<
0x0020  8018 ffff 8d78 0000 0101 080a 0044 1703       .....x.......D..
0x0030  0071 4e3a 504f 5354 202f 5f76 7469 5f62       .qN:POST./_vti_b
0x0040  696e 2f73 6874 6d6c 2e65 7865 2f5f 7674       in/shtml.exe/_vt
0x0050  695f 7270 6320 4854 5450 2f31 2e30 0d0a       i_rpc.HTTP/1.0..
0x0060  4461 7465 3a20 5361 742c 2031 3320 4a75       Date:.Sat,.13.Ju
0x0070  6c20 3230 3032 2030 313a 3535 3a31 3220       l.2002.01:55:12.
0x0080  474d 540d 0a4d 494d 452d 5665 7273 696f       GMT..MIME-Versio
0x0090  6e3a 2031 2e30 0d0a 5573 6572 2d41 6765       n:.1.0..User-Age
0x00a0  6e74 3a20 4d53 4672 6f6e 7450 6167 652f       nt:.MSFrontPage/
0x00b0  342e 300d 0a48 6f73 743a 2077 7777 2e58       4.0..Host:.www.X
0x00c0  5858 582e 636f 6d0d 0a41 6363 6570 743a       XXX.com..Accept:
0x00d0  2061 7574 682f 7369 6369 6c79 0d0a 436f       .auth/sicily..Co
0x00e0  6e74 656e 742d 4c65 6e67 7468 3a20 3431       ntent-Length:.41
0x00f0  0d0a 436f 6e74 656e 742d 5479 7065 3a20       ..Content-Type:.
0x0100  6170 706c 6963 6174 696f 6e2f 782d 7777       application/x-ww
0x0110  772d 666f 726d 2d75 726c 656e 636f 6465       w-form-urlencode
0x0120  640d 0a58 2d56 6572 6d65 6572 2d43 6f6e       d..X-Vermeer-Con
0x0130  7465 6e74 2d54 7970 653a 2061 7070 6c69       tent-Type:.appli
0x0140  6361 7469 6f6e 2f78 2d77 7777 2d66 6f72       cation/x-www-for
0x0150  6d2d 7572 6c65 6e63 6f64 6564 0d0a 5072       m-urlencoded..Pr
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0160  6167 6d61 3a20 6e6f 2d63 6163 6865 0d0a       agma:.no-cache..
0x0170  4361 6368 652d 436f 6e74 726f 6c3a 206d       Cache-Control:.m
0x0180  6178 2d73 7461 6c65 3d30 0d0a 0d0a 6d65       ax-stale=0....me
0x0190  7468 6f64 3d73 6572 7665 722b 7665 7273       thod=server+vers
0x01a0  696f 6e25 3361 3425 3265 3025 3265 3225       ion%3a4%2e0%2e2%
0x01b0  3265 3236 3131 0a0d 0a                        2e2611...

18:44:56.054488 IP 203.241.151.50.15763 > 46.5.180.133.80: P
3203231433:3203231695(262) ack 2760327168 win 65535 <nop,nop,timestamp 4462412
7429266>
0x0000  4500 013a 87df 0000 3006 c236 cbf1 9732       E..:....0..6...2
0x0010  2e05 b485 3d93 0050 beed 6ec9 a487 4000       ....=..P..n...@.
0x0020  8018 ffff 388e 0000 0101 080a 0044 174c       ....8........D.L
0x0030  0071 5c92 4745 5420 2f5f 7674 695f 696e       .q\.GET./_vti_in
0x0040  662e 6874 6d6c 2048 5454 502f 312e 300d       f.html.HTTP/1.0.
0x0050  0a44 6174 653a 2053 6174 2c20 3133 204a       .Date:.Sat,.13.J
0x0060  756c 2032 3030 3220 3031 3a35 353a 3438       ul.2002.01:55:48
0x0070  2047 4d54 0d0a 4d49 4d45 2d56 6572 7369       .GMT..MIME-Versi
0x0080  6f6e 3a20 312e 300d 0a41 6363 6570 743a       on:.1.0..Accept:
0x0090  202a 2f2a 0d0a 5573 6572 2d41 6765 6e74       .*/*..User-Agent
0x00a0  3a20 4d6f 7a69 6c6c 612f 322e 3020 2863       :.Mozilla/2.0.(c
0x00b0  6f6d 7061 7469 626c 653b 204d 5320 4672       ompatible;.MS.Fr
0x00c0  6f6e 7450 6167 6520 342e 3029 0d0a 486f       ontPage.4.0)..Ho
0x00d0  7374 3a20 7777 772e 5858 5858 2e63 6f6d       st:.www.XXXX.com
0x00e0  0d0a 4163 6365 7074 3a20 6175 7468 2f73       ..Accept:.auth/s
0x00f0  6963 696c 790d 0a43 6f6e 7465 6e74 2d4c       icily..Content-L
0x0100  656e 6774 683a 2030 0d0a 5072 6167 6d61       ength:.0..Pragma
0x0110  3a20 6e6f 2d63 6163 6865 0d0a 4361 6368       :.no-cache..Cach
0x0120  652d 436f 6e74 726f 6c3a 206d 6178 2d73       e-Control:.max-s
0x0130  7461 6c65 3d30 0d0a 0d0a                      tale=0....

18:44:57.184488 IP 203.241.151.50.16446 > 46.5.180.133.80: P
3511070194:3511070583(389) ack 2769305419 win 65535 <nop,nop,timestamp 4462415
7429379>
0x0000  4500 01b9 abc8 0000 3006 9dce cbf1 9732       E.......0......2
0x0010  2e05 b485 403e 0050 d146 adf2 a510 3f4b       ....@>.P.F....?K
0x0020  8018 ffff 91e1 0000 0101 080a 0044 174f       .............D.O
0x0030  0071 5d03 504f 5354 202f 5f76 7469 5f62       .q].POST./_vti_b
0x0040  696e 2f73 6874 6d6c 2e65 7865 2f5f 7674       in/shtml.exe/_vt
0x0050  695f 7270 6320 4854 5450 2f31 2e30 0d0a       i_rpc.HTTP/1.0..
0x0060  4461 7465 3a20 5361 742c 2031 3320 4a75       Date:.Sat,.13.Ju
0x0070  6c20 3230 3032 2030 313a 3535 3a34 3920       l.2002.01:55:49.
0x0080  474d 540d 0a4d 494d 452d 5665 7273 696f       GMT..MIME-Versio
0x0090  6e3a 2031 2e30 0d0a 5573 6572 2d41 6765       n:.1.0..User-Age
0x00a0  6e74 3a20 4d53 4672 6f6e 7450 6167 652f       nt:.MSFrontPage/
0x00b0  342e 300d 0a48 6f73 743a 2077 7777 2e58       4.0..Host:.www.X
0x00c0  5858 582e 636f 6d0d 0a41 6363 6570 743a       XXX.com..Accept:
0x00d0  2061 7574 682f 7369 6369 6c79 0d0a 436f       .auth/sicily..Co
0x00e0  6e74 656e 742d 4c65 6e67 7468 3a20 3431       ntent-Length:.41
0x00f0  0d0a 436f 6e74 656e 742d 5479 7065 3a20       ..Content-Type:.
0x0100  6170 706c 6963 6174 696f 6e2f 782d 7777       application/x-ww
0x0110  772d 666f 726d 2d75 726c 656e 636f 6465       w-form-urlencode
0x0120  640d 0a58 2d56 6572 6d65 6572 2d43 6f6e       d..X-Vermeer-Con
0x0130  7465 6e74 2d54 7970 653a 2061 7070 6c69       tent-Type:.appli
0x0140  6361 7469 6f6e 2f78 2d77 7777 2d66 6f72       cation/x-www-for
0x0150  6d2d 7572 6c65 6e63 6f64 6564 0d0a 5072       m-urlencoded..Pr
0x0160  6167 6d61 3a20 6e6f 2d63 6163 6865 0d0a       agma:.no-cache..
0x0170  4361 6368 652d 436f 6e74 726f 6c3a 206d       Cache-Control:.m
0x0180  6178 2d73 7461 6c65 3d30 0d0a 0d0a 6d65       ax-stale=0....me
0x0190  7468 6f64 3d73 6572 7665 722b 7665 7273       thod=server+vers
0x01a0  696f 6e25 3361 3425 3265 3025 3265 3225       ion%3a4%2e0%2e2%
0x01b0  3265 3236 3131 0a0d 0a                        2e2611...
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
18:47:41.584488 IP 211.48.105.46.1437 > 46.5.180.133.21: P 4061913411:4061913427(16)
ack 2929597909 win 17457 (DF)
0x0000  4500 0038 32ef 4000 6c06 c2ed d330 692e      E..82.@.l....0i.
0x0010  2e05 b485 059d 0015 f21b e143 ae9e 1dd5      ...........C....
0x0020  5018 4431 2546 0000 5553 4552 2061 6e6f      P.D1%F..USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

20:24:21.944488 IP 168.103.106.145.43860 > 46.5.180.133.21: P
1548250402:1548250418(16) ack 447186845 win 8760 (DF)
0x0000  4500 0038 0360 4000 ee06 99e2 a867 6a91      E..8.`@......gj.
0x0010  2e05 b485 ab54 0015 5c48 6d22 1aa7 879d      .....T..\Hm"....
0x0020  5018 2238 ff11 0000 5553 4552 2061 6e6f      P."8....USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..

20:47:33.824488 IP 218.17.234.225.38236 > 46.5.180.133.80: P 6700137:6700377(240) ack
1929180817 win 7788 (DF)
0x0000  4500 0118 c20b 4000 6906 ad5c da11 eae1      E.....@.i..\....
0x0010  2e05 b485 955c 0050 0066 3c69 72fc f691      .....\.P.f<ir...
0x0020  5018 1e6c b6e5 0000 4745 5420 2f5f 7674      P..l....GET./_vt
0x0030  695f 696e 662e 6874 6d6c 2048 5454 502f      i_inf.html.HTTP/
0x0040  312e 310d 0a44 6174 653a 2053 6174 2c20      1.1..Date:.Sat,.
0x0050  3133 204a 756c 2032 3030 3220 3033 3a34      13.Jul.2002.03:4
0x0060  383a 3333 2047 4d54 0d0a 4d49 4d45 2d56      8:33.GMT..MIME-V
0x0070  6572 7369 6f6e 3a20 312e 300d 0a41 6363      ersion:.1.0..Acc
0x0080  6570 743a 202a 2f2a 0d0a 5573 6572 2d41      ept:.*/*..User-A
0x0090  6765 6e74 3a20 4d6f 7a69 6c6c 612f 322e      gent:.Mozilla/2.
0x00a0  3020 2863 6f6d 7061 7469 626c 653b 204d      0.(compatible;.M
0x00b0  5320 4672 6f6e 7450 6167 6520 342e 3029      S.FrontPage.4.0)
0x00c0  0d0a 486f 7374 3a20 7777 772e 5858 5858      ..Host:.www.XXXX
0x00d0  2e63 6f6d 0d0a 4163 6365 7074 3a20 6175      .com..Accept:.au
0x00e0  7468 2f73 6963 696c 790d 0a43 6f6e 7465      th/sicily..Conte
0x00f0  6e74 2d4c 656e 6774 683a 2030 0d0a 436f      nt-Length:.0..Co
0x0100  6e6e 6563 7469 6f6e 3a20 4b65 6570 2d41      nnection:.Keep-A
0x0110  6c69 7665 0d0a 0d0a                          live....

20:47:34.644488 IP 218.17.234.225.38237 > 46.5.180.133.80: P 6701699:6702064(365) ack
1930933751 win 8484 (DF)
0x0000  4500 0195 d80b 4000 6906 96df da11 eae1      E.....@.i.......
0x0010  2e05 b485 955d 0050 0066 4283 7317 b5f7      .....].P.fB.s...
0x0020  5018 2124 ae62 0000 504f 5354 202f 5f76      P.!$.b..POST./_v
0x0030  7469 5f62 696e 2f73 6874 6d6c 2e65 7865      ti_bin/shtml.exe
0x0040  2f5f 7674 695f 7270 6320 4854 5450 2f31      /_vti_rpc.HTTP/1
0x0050  2e31 0d0a 4461 7465 3a20 5361 742c 2031      .1..Date:.Sat,.1
0x0060  3320 4a75 6c20 3230 3032 2030 333a 3438      3.Jul.2002.03:48
0x0070  3a33 3320 474d 540d 0a4d 494d 452d 5665      :33.GMT..MIME-Ve
0x0080  7273 696f 6e3a 2031 2e30 0d0a 5573 6572      rsion:.1.0..User
0x0090  2d41 6765 6e74 3a20 4d53 4672 6f6e 7450      -Agent:.MSFrontP
0x00a0  6167 652f 342e 300d 0a48 6f73 743a 2077      age/4.0..Host:.w
0x00b0  7777 2e58 5858 582e 636f 6d0d 0a41 6363      ww.XXXX.com..Acc
0x00c0  6570 743a 2061 7574 682f 7369 6369 6c79      ept:.auth/sicily
0x00d0  0d0a 436f 6e74 656e 742d 4c65 6e67 7468      ..Content-Length
0x00e0  3a20 3431 0d0a 436f 6e74 656e 742d 5479      :.41..Content-Ty
0x00f0  7065 3a20 6170 706c 6963 6174 696f 6e2f      pe:.application/
0x0100  782d 7777 772d 666f 726d 2d75 726c 656e      x-www-form-urlen
0x0110  636f 6465 640d 0a58 2d56 6572 6d65 6572      coded..X-Vermeer
0x0120  2d43 6f6e 7465 6e74 2d54 7970 653a 2061      -Content-Type:.a
0x0130  7070 6c69 6361 7469 6f6e 2f78 2d77 7777      pplication/x-www
0x0140  2d66 6f72 6d2d 7572 6c65 6e63 6f64 6564      -form-urlencoded
0x0150  0d0a 436f 6e6e 6563 7469 6f6e 3a20 4b65      ..Connection:.Ke
0x0160  6570 2d41 6c69 7665 0d0a 0d0a 6d65 7468      ep-Alive....meth
0x0170  6f64 3d73 6572 7665 722b 7665 7273 696f      od=server+versio
0x0180  6e25 3361 3425 3265 3025 3265 3225 3265      n%3a4%2e0%2e2%2e
0x0190  3236 3131 0a                                 2611.
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
07:13:19.714488 IP 81.28.32.103.1331 > 46.5.180.133.80: P 4121934171:4121934427(256)
ack 2943193079 win 8760 (DF)
0x0000  4500 0128 0e2a 4000 6c06 b19e 511c 2067      E..(.*@.l...Q..g
0x0010  2e05 b485 0533 0050 f5af b95b af6d 8ff7      .....3.P...[.m..
0x0020  5018 2238 1936 0000 4745 5420 2f5f 7674      P."8.6..GET./_vt
0x0030  695f 6269 6e2f 6f77 7373 7672 2e64 6c6c      i_bin/owssvr.dll
0x0040  3f55 4c3d 3126 4143 543d 3426 4255 494c      ?UL=1&ACT=4&BUIL
0x0050  443d 3236 3134 2653 5452 4d56 4552 3d34      D=2614&STRMVER=4
0x0060  2643 4150 5245 513d 3020 4854 5450 2f31      &CAPREQ=0.HTTP/1
0x0070  2e31 0d0a 4163 6365 7074 3a20 2a2f 2a0d      .1..Accept:.*/*.
0x0080  0a41 6363 6570 742d 456e 636f 6469 6e67      .Accept-Encoding
0x0090  3a20 677a 6970 2c20 6465 666c 6174 650d      :.gzip,.deflate.
0x00a0  0a55 7365 722d 4167 656e 743a 204d 6f7a      .User-Agent:.Moz
0x00b0  696c 6c61 2f34 2e30 2028 636f 6d70 6174      illa/4.0.(compat
0x00c0  6962 6c65 3b20 4d53 4945 2036 2e30 3b20      ible;.MSIE.6.0;.
0x00d0  5769 6e64 6f77 7320 4e54 2035 2e31 290d      Windows.NT.5.1).
0x00e0  0a48 6f73 743a 2077 7777 2e58 5858 582e      .Host:.www.XXXX.
0x00f0  636f 6d0d 0a43 6f6e 6e65 6374 696f 6e3a      com..Connection:
0x0100  204b 6565 702d 416c 6976 650d 0a43 6163      .Keep-Alive..Cac
0x0110  6865 2d43 6f6e 7472 6f6c 3a20 6e6f 2d63      he-Control:.no-c
0x0120  6163 6865 0d0a 0d0a                          ache....

07:13:23.254488 IP 81.28.32.103.1333 > 46.5.180.133.80: P 4122666454:4122666710(256)
ack 2947503828 win 8760 (DF)
0x0000  4500 0128 0e3b 4000 6c06 b18d 511c 2067      E..(.;@.l...Q..g
0x0010  2e05 b485 0535 0050 f5ba e5d6 afaf 56d4      .....5.P......V.
0x0020  5018 2238 258f 0000 4745 5420 2f5f 7674      P."8%...GET./_vt
0x0030  695f 6269 6e2f 6f77 7373 7672 2e64 6c6c      i_bin/owssvr.dll
0x0040  3f55 4c3d 3126 4143 543d 3426 4255 494c      ?UL=1&ACT=4&BUIL
0x0050  443d 3236 3134 2653 5452 4d56 4552 3d34      D=2614&STRMVER=4
0x0060  2643 4150 5245 513d 3020 4854 5450 2f31      &CAPREQ=0.HTTP/1
0x0070  2e31 0d0a 4163 6365 7074 3a20 2a2f 2a0d      .1..Accept:.*/*.
0x0080  0a41 6363 6570 742d 456e 636f 6469 6e67      .Accept-Encoding
0x0090  3a20 677a 6970 2c20 6465 666c 6174 650d      :.gzip,.deflate.
0x00a0  0a55 7365 722d 4167 656e 743a 204d 6f7a      .User-Agent:.Moz
0x00b0  696c 6c61 2f34 2e30 2028 636f 6d70 6174      illa/4.0.(compat
0x00c0  6962 6c65 3b20 4d53 4945 2036 2e30 3b20      ible;.MSIE.6.0;.
0x00d0  5769 6e64 6f77 7320 4e54 2035 2e31 290d      Windows.NT.5.1).
0x00e0  0a48 6f73 743a 2077 7777 2e58 5858 582e      .Host:.www.XXXX.
0x00f0  636f 6d0d 0a43 6f6e 6e65 6374 696f 6e3a      com..Connection:
0x0100  204b 6565 702d 416c 6976 650d 0a43 6163      .Keep-Alive..Cac
0x0110  6865 2d43 6f6e 7472 6f6c 3a20 6e6f 2d63      he-Control:.no-c
0x0120  6163 6865 0d0a 0d0a                          ache....

11:34:47.744488 IP hnllhi1-ar1-4-65-052-124.hnllhi1.dsl-verizon.net.2114 >
46.5.180.133.80: P 4824952:4825217(265) ack 2314464474 win 8064 (DF)
0x0000  4500 0131 5c4a 4000 6c06 9c3b 0441 347c      E..1\J@.l..;.A4|
0x0010  2e05 b485 0842 0050 0049 9f78 89f3 ecda      .....B.P.I.x....
0x0020  5018 1f80 05d9 0000 4745 5420 2f5f 7674      P.......GET./_vt
0x0030  695f 696e 662e 6874 6d6c 2048 5454 502f      i_inf.html.HTTP/
0x0040  312e 310d 0a44 6174 653a 2053 6174 2c20      1.1..Date:.Sat,.
0x0050  3133 204a 756c 2032 3030 3220 3138 3a33      13.Jul.2002.18:3
0x0060  343a 3033 2047 4d54 0d0a 4d49 4d45 2d56      4:03.GMT..MIME-V
0x0070  6572 7369 6f6e 3a20 312e 300d 0a41 6363      ersion:.1.0..Acc
0x0080  6570 743a 202a 2f2a 0d0a 5573 6572 2d41      ept:.*/*..User-A
0x0090  6765 6e74 3a20 4d6f 7a69 6c6c 612f 322e      gent:.Mozilla/2.
0x00a0  3020 2863 6f6d 7061 7469 626c 653b 204d      0.(compatible;.M
0x00b0  5320 4672 6f6e 7450 6167 6520 342e 3029      S.FrontPage.4.0)
0x00c0  0d0a 486f 7374 3a20 7777 772e 5858 5858      ..Host:.www.XXXX
0x00d0  2e63 6f6d 0d0a 4163 6365 7074 3a20 6175      .com..Accept:.au
0x00e0  7468 2f73 6963 696c 790d 0a43 6f6e 7465      th/sicily..Conte
0x00f0  6e74 2d4c 656e 6774 683a 2030 0d0a 436f      nt-Length:.0..Co
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0100  6e6e 6563 7469 6f6e 3a20 4b65 6570 2d41       nnection:.Keep-A
0x0110  6c69 7665 0d0a 4361 6368 652d 436f 6e74       live..Cache-Cont
0x0120  726f 6c3a 206e 6f2d 6361 6368 650d 0a0d       rol:.no-cache...
0x0130  0a                                            .

11:34:48.304488 IP hnllhi1-ar1-4-65-052-124.hnllhi1.dsl-verizon.net.2120 >
46.5.180.133.80: P 4831330:4831720(390) ack 2321404685 win 8760 (DF)
0x0000  4500 01ae 674a 4000 6c06 90be 0441 347c       E...gJ@.l....A4|
0x0010  2e05 b485 0848 0050 0049 b862 8a5d d30d       .....H.P.I.b.]..
0x0020  5018 2238 a581 0000 504f 5354 202f 5f76       P."8....POST./_v
0x0030  7469 5f62 696e 2f73 6874 6d6c 2e65 7865       ti_bin/shtml.exe
0x0040  2f5f 7674 695f 7270 6320 4854 5450 2f31       /_vti_rpc.HTTP/1
0x0050  2e31 0d0a 4461 7465 3a20 5361 742c 2031       .1..Date:.Sat,.1
0x0060  3320 4a75 6c20 3230 3032 2031 383a 3334       3.Jul.2002.18:34
0x0070  3a30 3420 474d 540d 0a4d 494d 452d 5665       :04.GMT..MIME-Ve
0x0080  7273 696f 6e3a 2031 2e30 0d0a 5573 6572       rsion:.1.0..User
0x0090  2d41 6765 6e74 3a20 4d53 4672 6f6e 7450       -Agent:.MSFrontP
0x00a0  6167 652f 342e 300d 0a48 6f73 743a 2077       age/4.0..Host:.w
0x00b0  7777 2e58 5858 582e 636f 6d0d 0a41 6363       ww.XXXX.com..Acc
0x00c0  6570 743a 2061 7574 682f 7369 6369 6c79       ept:.auth/sicily
0x00d0  0d0a 436f 6e74 656e 742d 4c65 6e67 7468       ..Content-Length
0x00e0  3a20 3431 0d0a 436f 6e74 656e 742d 5479       :.41..Content-Ty
0x00f0  7065 3a20 6170 706c 6963 6174 696f 6e2f       pe:.application/
0x0100  782d 7777 772d 666f 726d 2d75 726c 656e       x-www-form-urlen
0x0110  636f 6465 640d 0a58 2d56 6572 6d65 6572       coded..X-Vermeer
0x0120  2d43 6f6e 7465 6e74 2d54 7970 653a 2061       -Content-Type:.a
0x0130  7070 6c69 6361 7469 6f6e 2f78 2d77 7777       pplication/x-www
0x0140  2d66 6f72 6d2d 7572 6c65 6e63 6f64 6564       -form-urlencoded
0x0150  0d0a 436f 6e6e 6563 7469 6f6e 3a20 4b65       ..Connection:.Ke
0x0160  6570 2d41 6c69 7665 0d0a 4361 6368 652d       ep-Alive..Cache-
0x0170  436f 6e74 726f 6c3a 206e 6f2d 6361 6368       Control:.no-cach
0x0180  650d 0a0d 0a6d 6574 686f 643d 7365 7276       e....method=serv
0x0190  6572 2b76 6572 7369 6f6e 2533 6134 2532       er+version%3a4%2
0x01a0  6530 2532 6532 2532 6532 3631 310a            e0%2e2%2e2611.

15:47:51.294488 IP cs242716-158.austin.rr.com.2201 > 46.5.180.133.80: P
740893643:740893908(265) ack 1163455894 win 63167 <nop,nop,timestamp 145194 6366772>
(DF)
0x0000  4500 013d 7993 4000 6e06 8cea 181b 109e       E..=y.@.n.......
0x0010  2e05 b485 0899 0050 2c29 23cb 4558 ed96       .......P,)#.EX..
0x0020  8018 f6bf ff3e 0000 0101 080a 0002 372a       .....>........7*
0x0030  0061 2634 4745 5420 2f5f 7674 695f 6269       .a&4GET./_vti_bi
0x0040  6e2f 6f77 7373 7672 2e64 6c6c 3f55 4c3d       n/owssvr.dll?UL=
0x0050  3126 4143 543d 3426 4255 494c 443d 3236       1&ACT=4&BUILD=26
0x0060  3134 2653 5452 4d56 4552 3d34 2643 4150       14&STRMVER=4&CAP
0x0070  5245 513d 3020 4854 5450 2f31 2e31 0d0a       REQ=0.HTTP/1.1..
0x0080  4163 6365 7074 3a20 2a2f 2a0d 0a41 6363       Accept:.*/*..Acc
0x0090  6570 742d 456e 636f 6469 6e67 3a20 677a       ept-Encoding:.gz
0x00a0  6970 2c20 6465 666c 6174 650d 0a55 7365       ip,.deflate..Use
0x00b0  722d 4167 656e 743a 204d 6f7a 696c 6c61       r-Agent:.Mozilla
0x00c0  2f34 2e30 2028 636f 6d70 6174 6962 6c65       /4.0.(compatible
0x00d0  3b20 4d53 4945 2036 2e30 3b20 5769 6e64       ;.MSIE.6.0;.Wind
0x00e0  6f77 7320 4e54 2035 2e31 3b20 5133 3132       ows.NT.5.1;.Q312
0x00f0  3436 3129 0d0a 486f 7374 3a20 7777 772e       461)..Host:.www.
0x0100  5858 5858 2e63 6f6d 0d0a 436f 6e6e 6563       XXXX.com..Connec
0x0110  7469 6f6e 3a20 4b65 6570 2d41 6c69 7665       tion:.Keep-Alive
0x0120  0d0a 4361 6368 652d 436f 6e74 726f 6c3a       ..Cache-Control:
0x0130  206e 6f2d 6361 6368 650d 0a0d 0a              .no-cache....
```

1. Source of Trace -

I've purposely chosen the raw data file "2002.6.13", available from the Incidents.Org website at http://www.incidents.org/logs/Raw/, due to the fact that there has been relatively little analysis

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

performed on it to date. The output above consists of relevant packets for my analysis which I have output using tcpdump hex and ascii formatting (-X switch enabled).

2. Detect was generated by –

The Snort IDS sensors on this network are detecting traffic to and from the Class B 46.5.xxx.yyy IP address space (these are not the actual IP addresses, as they have been sanitized in these log files). Note that ALL the packets in this raw file triggered a Snort alert of some kind, or else they would not have been logged.

The Snort rules that generated these alerts are:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-IIS _vti_inf access";flags:A+; uricontent:"_vti_inf.html";
nocase; classtype:web-application-activity; sid:990; rev:5;)
```

and:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-FRONTPAGE _vti_rpc
access"; flags:A+; uricontent:"/_vti_rpc"; nocase; reference:bugtraq,2144; classtype:web-application-activity;
sid:937; rev:6;)
```

I have chosen to focus solely on traffic directed to the IIS/FTP server located at IP address 46.5.180.133, and that falls into one of two categories: they are either Anonymous FTP logons to the server, or they are part of a Front Page publishing attempt directed at this same server.

3. Probability the source address was spoofed –

It is extremely unlikely that the source IP addresses were spoofed. We see numerous tcp connections occurring in the raw data file, including several anonymous FTP logons and connections to the Front Page Extensions that are running on this web server. For a complete tcp "3 way connection" to occur, IP spoofing is almost certainly out of the question, unless we are dealing with a highly skilled hacker capable of pulling off some sort of Man in the Middle attack.

It is extremely likely, however, that the attacker(s) may be using open anonymous proxy servers and/or previously compromised hosts to mask the IP address from which they are basing their operations.

4. Description of attack –

The IIS web server located at IP address 46.5.180.133 appears to be allowing both Front Page publishing access as well as Anonymous FTP. This can be inferred from the numerous packets of both types directed toward it. These are targeted toward this server; we do not see any other such traffic directed at any other IP address being monitored by this IDS system. Unfortunately, since we have access only to the packets that actually triggered Snort alerts, a rigorous analysis of the entire tcp stream in question is not possible.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Captain John M. Melvin has written an excellent and comprehensive analysis of the Front Page-specific detects in this data file. Please refer to his analysis at http://cert.uni-stuttgart.de/archive/intrusions/2002/09/msg00265.html for a detailed description of the Front Page vulnerabilities present on this server.

We observe numerous anonymous FTP logons to the server from 11 distinct IP addresses. Virtually all of these logons originated from DSL connections with major ISPs. Interestingly, we see these anonymous FTP connections originating in several different nations on three continents: Germany, Japan, Korea, and the US.

The Front Page connections to the server originate from 5 distinct IP addresses, 2 of which have recent complaints lodged against them at www.Dshield.org:

IP Address: 218.17.234.225
HostName: 218.17.234.225
DShield Profile: Country:
Contact E-mail:
Total Records against IP: 204
Number of targets: 76
Date Range: 2003-02-15 to 2003-02-17

Fightback: not sent
Whois: inetnum: 218.13.0.0 - 218.18.255.255
netname: CHINANET-GD
country: CN
descr: CHINANET Guangdong province network
Data Communication Division
China Telecom
admin_c: CH93-AP
tech_c: WM12-AP
remarks:
mnt_by: MAINT-CHINANET
changed: hostmaster@ns.chinanet.cn.net 20010528
status: ALLOCATED PORTABLE
source: APNIC
notify:
mnt_lower: MAINT-CHINANET-GD
rev_srv:
start: 3658285056
end: 3658678271
diff: 393215
person: WU MIAN
address: NO.1,RO.DONGYUANHENG,YUEXIUNAN,GUANGZHOU
country: CN
phone: +086-20-83877223
fax_no: +86-20-83877223
e_mail: ipadm@gddc.com.cn
nic_hdl: WM12-AP
mnt_by: MAINT-CHINANET-GD
changed: ipadm@gddc.com.cn 20010820
source: APNIC

From this, we see that this individual is using an IP address belonging to China Telecom, located in Gaungdong province. We also see that that this IP address has over 200 prior complaint records logged against it in Dshield. These prior complaints are based on prior suspicious traffic from this user's current IP to 76 different hosts. While there is a good possibility that the ISP

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

uses DHCP to assign IP addresses, and that our user may have obtained a "Dshield tainted" IP address completely by chance, this is still evidence of malfeasance sufficient to raise our suspicions regarding traffic from this IP address.

5. Attack mechanism –

There is significant evidence that the IIS service in question has been set in a very permissive and lenient manner. Captain John Melvin has performed an exhaustive examination of the possible attack vectors against these exact same Front Page Extensions in his excellent analysis (available at http://cert.uni-stuttgart.de/archive/intrusions/2002/09/msg00265.html).

However, I draw a very different conclusion from Captain Melvin regarding the intent of the Front Page traffic. He concluded that the repeated accesses to the Front Page extensions were valid traffic from authorized users making changes to the web server's content. I propose that a more malicious intent is behind this traffic.

My conclusion is that this web server is being used as a Warez repository (i.e., a storage location hackers use to store and exchange illegally obtained software). In support of this conclusion, I offer the following observations:

1) The fact we see numerous anonymous FTP connections from DSL lines all over the world are consistent with this being a Warez server. If it truly is a Warez server, its IP address is likely to be disseminated via hacker websites and IRC chat rooms. This would explain why we are seeing so many anonymous connections from so many disparate geographic locations.

2) The Front Page authoring connections to the server could be the mechanism by which new files are transferred to the server. Remember that two of the source IP addresses have prior complaints against them at Dshield.org. This is consistent with the theory that these IP addresses belong to nefarious individuals who might well be trafficking in warez.

3) Warezers have been widely known to utilize the Front Page Extensions as a convenient mechanism for managing hordes of pirated software. This is due to a combination of ease-of-use and subterfuge. Publishing files to an IIS web server with Front Page Extensions is extremely easy, while the convoluted directory structure created by Front Page makes a great place to hide files away from prying SysAdmin eyes. I have personally witnessed this firsthand on compromised IIS servers that I have had the pleasure of rehabilitating. A Google search of "_vti" and "warez" yields 41 hits, many of which are actual warez sites with subdirectories named _vti.

6. Correlations –

Captain John Melvin's analysis of the Front Page configuration issues on this same server: http://cert.uni-stuttgart.de/archive/intrusions/2002/09/msg00265.html).

Dshield.Org analysis of IP Address:
http://www.dshield.org/ipinfo.php

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Corroborating evidence of this type of Warezer behavior can be found in the following FTP log at http://www.incidents.org/archives/intrusions/msg02584.html:

```
WAREZ Obfuscation on World-Writable FTP [LOGS]
-----------------------------------------------------------------------------
Date: Mon, 7 Jan 2002 16:44:07 -0600
From: "James Crossman" <jcrossman@xxxxxxxxxxxxxx>
Subject: WAREZ Obfuscation on World-Writable FTP [LOGS]
-----------------------------------------------------------------------------
My partner is busy fighting these WAREZ and wants to be left alone while
he works on the files, so let me share with you a couple of log extracts
I pieced together....  The tricks they tried include renaming files and
directories after they were made and one renamed a directory to a .DOC
extension and locked up windows explorer every time....

Log #1 - Uncopyable (or deletable) Nirvana
ex011226.log:19:16:21 200.180.178.28 [83]USER anonymous 331
ex011226.log:19:16:21 200.180.178.28 [83]PASS guest@xxxxxx 230
ex011226.log:19:16:38 200.180.178.28 [83]MKD _vti 257
ex011226.log:19:16:48 200.180.178.28 [83]MKD m 257
ex011226.log:19:16:56 200.180.178.28 [83]MKD p 257
ex011226.log:19:17:06 200.180.178.28 [83]MKD 3 257
ex011226.log:19:17:27 200.180.178.28 [83]MKD by 257
ex011226.log:19:17:36 200.180.178.28 [83]MKD danger 257
ex011226.log:19:17:50 200.180.178.28 [83]MKD nirvana-nevermind 257
ex011226.log:19:24:04 200.180.178.28 [83]created
01+-+Nirvana+-+Smell+Like+Teen+Spirit.mp3 226
ex011226.log:19:28:11 200.180.178.28 [84]RNFR
/_vti/m/p/3/by/danger/nirvana-nevermind/01+-+Nirvana+-+Smell+Like+Teen+S
pirit.mp3 350
ex011226.log:19:28:11 200.180.178.28 [84]RNTO
/_vti/m/p/3/by/danger/nirvana-nevermind/01+-+Nirvana+-+Smell+Like+Teen+S
pirit.mp3+.+/++ 250
ex011226.log:19:28:31 200.180.178.28 [84]DELE
01+-+Nirvana+-+Smell+Like+Teen+Spirit.mp3+.+ 550
ex011226.log:19:29:47 200.180.178.28 [84]RNFR
/_vti/m/p/3/by/danger/nirvana-nevermind/01+-+Nirvana+-+Smell+Like+Teen+S
pirit.mp3+.+ 550
ex011226.log:19:35:27 200.180.178.28 [84]RNFR
/_vti/m/p/3/by/danger/nirvana-nevermind/01+-+Nirvana+-+Smell+Like+Teen+S
pirit.mp3+.+ 550
ex011226.log:20:08:37 200.180.178.28 [83]RNFR /_vti 350
ex011226.log:20:08:37 200.180.178.28 [83]RNTO /_vti++/++ 250
ex011226.log:20:09:07 200.180.178.28 [83]RNFR /_vti++ 550
ex011226.log:20:09:16 200.180.178.28 [83]RNFR /_vti++ 550
ex011226.log:20:09:46 200.180.178.28 [83]RNFR /_vti++ 550
```

7. Evidence of Active Targeting –

There is ample evidence of active targeting here. The Front Page accesses are directed solely at the IP address of this web server; we do not see any attempts to access any Front Page components on any other IP address in the data file. The same is true of the anonymous FTP connections - these are also directed solely at the web server at IP 46.5.180.133. We do not witness any other anonymous FTP connection attempts directed at any other IP address in the 2002.6.13 raw data file.

I conclude that some of the Front Page accesses we see in the raw data file are potentially publications of new Warez files to the compromised server, probably by the individual(s) who

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

originally performed the compromise. The anonymous FTP accesses are downloads of these Warez files by the end user hackers, who probably learned of its IP address through a hacker web site or chat room.

8. Severity –
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: importance of the targeted system. The IIS web server in question is open to web traffic from all over the world, and is likely housed in a DMZ. It is therefore likely that no highly sensitive data is stored on this server. I will assign a rating of 3 here.

Lethality: How severe would the damage be if the attack succeeds. Having your server used as a Warez repository is obviously a major nuisance, and there are certainly liability issues that could arise from this scenario. However, there is no evidence that there has been any significant damage to the server itself (indeed, it appears to be serving its warez in a very robust fashion, nor does it seem likely that a total system compromise is likely). I will assign a 3, primarily due to the potential liability issues that could arise from this scenario, and also due to the potential theft of bandwidth and server resources.

System Countermeasures: We have no way of knowing which service patches and hot-fixes have been applied to this server, but it does appear that the configuration of the Front Page extensions and anonymous FTP access are quite lenient. Anonymous FTP should only be allowed if it is absolutely essential for some business function. I will assign a 2 in this category.

Network Countermeasures: Port 80 is wide open at the firewall by necessity (this is a publicly-accessible web server, after all). All IP addresses appear to be allowed access, regardless of geographic location. An IDS is obviously in place, or we would not be analyzing this detect in the first place. I will assign a rating of 2 here.

Severity = (3 + 3) – (2 + 2) = 2

9. Defensive Recommendation –
The SysAdmin for this server should **immediately** examine it for any evidence that it is being used as a Warez repository. A file-system search on all local logical drives for the most recently modified files should answer this question posthaste. If the server really is being used as a Warez repository, this needs to be addressed ASAP by deleting all the illegal software and tightening up the Front Page exposures that allowed this situation to emerge in the first place.

I would recommend completely disabling both the Front Page Extensions and the Anonymous FTP access, unless they are absolutely needed. If they are needed, it is essential to ensure that they are fully patched with all the latest service packs and hot-fixes. Accounts using the Front Page extensions should be subjected to rigorous password auditing

As with any IIS web server, the SysAdmin would be wise to run the IIS Lockdown Tool and install the URLScan ISAPI filter as documented by Microsoft at these URLs:

IIS Lockdown Tool:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b325864

URLscan:
http://www.microsoft.com/technet//security/tools/tools/urlscan.asp

10. Multiple Choice Question –

What is this user up to?

```
ex011226.log:19:16:21 200.180.178.28 [83]USER anonymous 331
ex011226.log:19:16:21 200.180.178.28 [83]PASS guest@xxxxxx 230
ex011226.log:19:16:38 200.180.178.28 [83]MKD _vti 257
ex011226.log:19:16:48 200.180.178.28 [83]MKD m 257
ex011226.log:19:16:56 200.180.178.28 [83]MKD p 257
ex011226.log:19:17:06 200.180.178.28 [83]MKD 3 257
ex011226.log:19:17:27 200.180.178.28 [83]MKD by 257
ex011226.log:19:17:36 200.180.178.28 [83]MKD danger 257
ex011226.log:19:17:50 200.180.178.28 [83]MKD nirvana-nevermind 257
ex011226.log:19:24:04 200.180.178.28 [83]created
01+-+Nirvana+-+Smell+Like+Teen+Spirit.mp3 226
ex011226.log:19:28:11 200.180.178.28 [84]RNFR
/_vti/m/p/3/by/danger/nirvana-nevermind/01+-+Nirvana+-+Smell+Like+Teen+S
pirit.mp3 350
```

a) downloading a Nirvana song from a commercial music service.
b) creating a hidden storage repository for illegally-obtained copyrighted materials.
c) sharing his own Nirvana music collection on the Gnutella network.
d) playing "Smells Like Teen Sprit" on his MP3 player.

Correct answer –
B – each "MKD" command is making a subdirectory on the FTP server. The user is attempting to hide his or her stash of copyrighted MP3s in an obscure location deep within a subdirectory structure that looks ostensibly like a normal Front Page "_vti" subdirectory.

Note:
Detect #1 was submitted to the "incidents.org" mailing list on March 28th, and is publicly accessible here in the mailing list archives:
http://cert.uni-stuttgart.de/archive/intrusions/2003/03/msg00378.html

I received one public response from Andrew Rucker Jones, it is also available here:
http://cert.uni-stuttgart.de/archive/intrusions/2003/03/msg00385.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Detect #2 –
A Visit from a Curious Friend:

```
[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:15:28.145975 66.77.73.84:2019 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:51084 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x35157923  Ack: 0x54B502E  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:16:58.730474 66.77.73.84:3254 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:5525 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x51A0AA09  Ack: 0x54B507E  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:18:31.737326 66.77.73.84:4373 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:21836 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x9F46D5B6  Ack: 0x54B50BE  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:19:32.395718 66.77.73.84:1274 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:34649 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x85E69E2D  Ack: 0x54B50ED  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:20:01.852392 66.77.73.84:1777 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:43066 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0xC5308CCF  Ack: 0x54B5117  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:20:31.972895 66.77.73.84:2166 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:49342 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x365314FD  Ack: 0x54B512F  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:24:26.938248 66.77.73.84:4580 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:23578 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x3D0E47B2  Ack: 0x54B5184  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:26:58.947784 66.77.73.84:2575 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:54548 IpLen:20 DgmLen:285 DF
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
***AP*** Seq: 0xE5902EB  Ack: 0x54B520E  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:28:44.503150 66.77.73.84:3725 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:7111 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x10C03339  Ack: 0x54B525E  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:35:37.267730 66.77.73.84:1111 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:25823 IpLen:20 DgmLen:284 DF
***AP*** Seq: 0x707B6EE  Ack: 0x54B5411  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:38:07.669492 66.77.73.84:2988 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:53858 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x5373E3F5  Ack: 0x54B5536  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]

[**] [1:895:5] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/28-03:38:37.977493 66.77.73.84:3335 -> xxx.yyy.zzz.142:80
TCP TTL:50 TOS:0x0 ID:59533 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x9DD72B54  Ack: 0x54B553A  Win: 0xFFFF  TcpLen: 20
[Xref => cve CVE-2000-0382][Xref => bugtraq 1179]
```

1. Source of Trace -

For the past month, I have been capturing the first 300 bytes of every packet passing through the Internet-facing subnet on my home network. This is being accomplished with a Linux server running tcpdump in promiscuous mode on eth0. Periodically, I run the captured traffic through a default Snort configuration using the default rule set.

2. Detect was generated by –

The network detect is from a Snort intrusion detection system with a standard 1.9.1 rule set.

The Snort rule that generated the alert was:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI
redirect access";flags: A+; uricontent:"/redirect";
nocase;reference:bugtraq,1179; reference:cve,CVE-2000-0382;
classtype:attempted-recon; sid:895; rev:2;)
```

3. Probability the source address was spoofed –

It is extremely unlikely that the source IP address was spoofed. This alert is triggered by an automated reconnaissance probe against a web server that is co-located on my network. In order to get worthwhile information back, the “attacker” must complete the 3-way tcp handshake and supply a valid IP address under her control.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I will present more information regarding the attackers motivations in the following discussion.

4. Description of "attack" –

These CGI Redirect packets are being sent to a co-located web server on my network that hosts a very popular hobbyist bulletin board and chat room. There is substantial evidence that this is a benign reconnaissance probe being conducted by an automated "web-bot" that has been programmed to search out and catalog web content.

A lookup of the source IP address in Dshield yields up the following:

```
IP Address: 66.77.73.84
HostName: cr045r01-2.sac2.fastsearch.net
DShield Profile: Country: US
Contact E-mail: ip-admin@qis.qwest.net
Total Records against IP:  36
Number of targets:  2
Date Range: 2003-01-19 to 2003-02-02
Ports Attacked (up to 10):
Port   Attacks      Start        End
80     155          2003-02-27   2003-03-26

Fightback:  not sent
Whois:
CustName:   Fast Search, Inc.
Address:    93 Worcester Street, 4th Floor
City:       Wellesley
StateProv:  MA
PostalCode: 02481
Country:    US
RegDate:    2002-01-10
Updated:    2002-01-10

NetRange:   66.77.73.0 - 66.77.73.255
CIDR:       66.77.73.0/24
NetName:    QWEST-MCC-FASTSRCH3
NetHandle:  NET-66-77-73-0-1
Parent:     NET-66-77-0-0-1
NetType:    Reassigned
Comment:
RegDate:    2002-01-10
Updated:    2002-01-10
```

Clearly, ours is not the only server on the WWW that the folks at Fast Search, Inc. have been checking out. A quick check on their website at http://www.fastsearch.net/products/websearch/index.asp yields some very relevant information concerning one of their products:

```
The FAST Web Search index powers portals that reach the majority of European searches
and over a quarter of all US searches--over 100 million users worldwide. Unlike other
search engines, every query we receive is submitted across the entire catalog and
results are returned in less than half a second. In addition to our industry-leading
relevancy algorithms, we are committed to providing our users with the largest and
freshest catalog on the Net.
```

© SANS Institute 2003, Author retains full rights.

5. "Attack" mechanism –

First, we see the FastSearch Web Bot making a normal TCP connection to the web server on port 80, with completion of the 3-way handshake (Syn, Syn Ack, Ack are bolded):

```
21:40:57.256310 IP 66.77.73.84.1138 > xxx.yyy.zzz.142.80: S 2236556219:2236556219(0) win 65535 <mss 1380,nop,wscale
1,nop,nop,timestamp 2483146531 0> (DF)
0x0000   4500 003c 4606 4000 3206 bb34 424d 4954    E..<F.@.2..4BMIT
0x0010   d151 ea8e 0472 0050 854f 23bb 0000 0000    .Q...r.P.O#.....
0x0020   a002 ffff f2e3 0000 0204 0564 0103 0301    ...........d....
0x0030   0101 080a 9401 cf23 0000 0000              .......#....
21:40:57.256590 IP xxx.yyy.zzz.142.80 > 66.77.73.84.1138: S 85585584:85585584(0) ack 2236556220 win 8280 <mss 1460>
(DF)
0x0000   4500 002c 6b8c 4000 8006 47be d151 ea8e    E..,k.@...G..Q..
0x0010   424d 4954 0050 0472 0519 eeb0 854f 23bc    BMIT.P.r.....O#.
0x0020   6012 2058 8ea5 0000 0204 05b4 0000         `..X..........
21:40:57.359989 IP 66.77.73.84.1138 > xxx.yyy.zzz.142.80: . ack 1 win 65535 (DF)
0x0000   4500 0028 464e 4000 3206 bb00 424d 4954    E..(FN@.2...BMIT
0x0010   d151 ea8e 0472 0050 854f 23bc 0519 eeb1    .Q...r.P.O#.....
0x0020   5010 ffff c6ba 0000 0204 0564 0103         P...........d..
```

This Web Bot does not waste any time!! It already knows what files what files it wants, and it only wants them if they have not changed since February 28 (probably the last time it paid a visit to this web-site). The current visit occurred in the wee hours March 28th, exactly one month later. I doubt this is a coincidence. Evidently, FastSearch's web bots update their content on a monthly basis.

```
21:40:57.383937 IP 66.77.73.84.1138 > xxx.yyy.zzz.142.80: P 1:210(209) ack 1 win 65535 (DF)
0x0000   4500 00f9 464f 4000 3206 ba2e 424d 4954    E...FO@.2...BMIT
0x0010   d151 ea8e 0472 0050 854f 23bc 0519 eeb1    .Q...r.P.O#.....
0x0020   5018 ffff ac57 0000 4745 5420 2f20 4854    P....W..GET./.HT
0x0030   5450 2f31 2e30 0d0a 4966 2d4d 6f64 6966    TP/1.0..If-Modif
0x0040   6965 642d 5369 6e63 653a 2046 7269 2c20    ied-Since:.Fri,.
0x0050   3238 2046 6562 2032 3030 3320 3233 3a32    28.Feb.2003.23:2
0x0060   353a 3237 2047 4d54 0d0a 486f 7374 3a20    5:27.GMT..Host:.
0x0070   7777 772e 6272 6577 7261 7473 2e6f 7267    www.xxxxxxxx.org
0x0080   0d0a 436f 6e6e 6563 7469 6f6e 3a20 636c    ..Connection:.cl
0x0090   6f73 650d 0a55 7365 722d 4167 656e 743a    ose..User-Agent:
0x00a0   2046 4153 542d 5765 6243 7261 776c 6572    .FAST-WebCrawler
0x00b0   2f33 2e38 2028 6174 772d 6372 6177 6c65    /3.8.(atw-crawle
0x00c0   7220 6174 2066 6173 7420 646f 7420 6e6f    r.at.fast.dot.no
0x00d0   3b20 6874 7470 3a2f 2f66 6173 742e 6e6f    ;.http://fast.no
0x00e0   2f73 7570 706f 7274 2f63 7261 776c 6572    /support/crawler
0x00f0   2e61 7370 290d 0a0d 0a                     .asp)....
21:40:57.923835 IP 66.77.73.84.1158 > xxx.yyy.zzz.142.80: P 1:170(169) ack 1 win 65535 (DF)
0x0000   4500 00d1 4766 4000 3206 b93f 424d 4954    E...Gf@.2..?BMIT
0x0010   d151 ea8e 0486 0050 f4cc a694 0519 eebd    .Q.....P........
0x0020   5018 ffff 56ae 0000 4745 5420 2f69 6e74    P...V...GET./int
0x0030   726f 2e68 746d 6c20 4854 5450 2f31 2e30    ro.html.HTTP/1.0
0x0040   0d0a 486f 7374 3a20 7777 772e 6272 6577    ..Host:.www.yyyy
0x0050   7261 7473 2e6f 7267 0d0a 436f 6e6e 6563    yyyy.org..Connec
0x0060   7469 6f6e 3a20 636c 6f73 650d 0a55 7365    tion:.close..Use
0x0070   722d 4167 656e 743a 2046 4153 542d 5765    r-Agent:.FAST-We
0x0080   6243 7261 776c 6572 2f33 2e38 2028 6174    bCrawler/3.8.(at
0x0090   772d 6372 6177 6c65 7220 6174 2066 6173    w-crawler.at.fas
0x00a0   7420 646f 7420 6e6f 3b20 6874 7470 3a2f    t.dot.no;.http:/
0x00b0   2f66 6173 742e 6e6f 2f73 7570 706f 7274    /fast.no/support
0x00c0   2f63 7261 776c 6572 2e61 7370 290d 0a0d    /crawler.asp)...
0x00d0   0a
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
21:40:58.447202 IP 66.77.73.84.1190 > xxx.yyy.zzz.142.80: P 1:169(168) ack 1 win 65535 (DF)
0x0000   4500 00d0 48ab 4000 3206 b7fb 424d 4954   E...H.@.2...BMIT
0x0010   d151 ea8e 04a6 0050 3045 6077 0519 eecc   .Q.....P0E`w....
0x0020   5018 ffff 05f8 0000 4745 5420 2f6d 656e   P.......GET./men
0x0030   752e 6874 6d6c 2048 5454 502f 312e 300d   u.html.HTTP/1.0.
0x0040   0a48 6f73 743a 2077 7777 2e62 7265 7772   .Host:.www.yyyyy
0x0050   6174 732e 6f72 670d 0a43 6f6e 6e65 6374   yyy.org..Connect
0x0060   696f 6e3a 2063 6c6f 7365 0d0a 5573 6572   ion:.close..User
0x0070   2d41 6765 6e74 3a20 4641 5354 2d57 6562   -Agent:.FAST-Web
0x0080   4372 6177 6c65 722f 332e 3820 2861 7477   Crawler/3.8.(atw
0x0090   2d63 7261 776c 6572 2061 7420 6661 7374   -crawler.at.fast
0x00a0   2064 6f74 206e 6f3b 2068 7474 703a 2f2f   .dot.no;.http://
0x00b0   6661 7374 2e6e 6f2f 7375 7070 6f72 742f   fast.no/support/
0x00c0   6372 6177 6c65 722e 6173 7029 0d0a 0d0a   crawler.asp)....
21:40:58.466444 IP xxx.yyy.zzz.142.80 > 66.77.73.84.1190: P 1:82(81) ack 169 win 8112 (DF)
0x0000   4500 0079 768c 4000 8006 3c71 d151 ea8e   E..yv.@...<q.Q..
0x0010   424d 4954 0050 04a6 0519 eecc 3045 611f   BMIT.P......0Ea.
0x0020   5018 1fb0 42c6 0000 4854 5450 2f31 2e31   P...B...HTTP/1.1
0x0030   2032 3030 204f 4b0d 0a53 6572 7665 723a   .200.OK..Server:
0x0040   204d 6963 726f 736f 6674 2d49 4953 2f34   .Microsoft-IIS/4
0x0050   2e30 0d0a 4461 7465 3a20 4672 692c 2032   .0..Date:.Fri,.2
0x0060   3820 4d61 7220 3230 3033 2030 333a 3335   8.Mar.2003.03:35
0x0070   3a32 3320 474d 540d 0a                    :23.GMT..
21:40:59.408512 IP xxx.yyy.zzz.142.80 > 66.77.73.84.1218: P 1:605(604) ack 170 win 8111 (DF)
0x0000   4500 0284 7a8c 4000 8006 3666 d151 ea8e   E...z.@...6f.Q..
0x0010   424d 4954 0050 04c2 0519 eed6 400c 06df   BMIT.P......@...
0x0020   5018 1faf cdf9 0000 4854 5450 2f31 2e31   P.......HTTP/1.1
0x0030   2034 3034 204f 626a 6563 7420 4e6f 7420   .404.Object.Not.
0x0040   466f 756e 640d 0a53 6572 7665 723a 204d   Found..Server:.M
0x0050   6963 726f 736f 6674 2d49 4953 2f34 2e30   icrosoft-IIS/4.0
0x0060   0d0a 4461 7465 3a20 4672 692c 2032 3820   ..Date:.Fri,.28.
0x0070   4d61 7220 3230 3033 2030 333a 3335 3a32   Mar.2003.03:35:2
0x0080   3420 474d 540d 0a43 6f6e 7465 6e74 2d4c   4.GMT..Content-L
0x0090   656e 6774 683a 2034 3631 0d0a 436f 6e74   ength:.461..Cont
0x00a0   656e 742d 5479 7065 3a20 7465 7874 2f68   ent-Type:.text/h
0x00b0   746d 6c0d 0a0d 0a3c 6874 6d6c 3e3c 6865   tml....<html><he
0x00c0   6164 3e3c 7469 746c 653e 4572 726f 7220   ad><title>Error.
0x00d0   3430 343c 2f74 6974 6c65 3e0d 0a0d 0a3c   404</title>....<
0x00e0   6d65 7461 206e 616d 653d 2272 6f62 6f74   meta.name="robot
0x00f0   7322 2063 6f6e 7465 6e74 3d22 6e6f 696e   s".content="noin
0x0100   6465 7822 3e0d 0a3c 4d45 5441 2048 5454   dex">..<META.HTT
0x0110   502d 4551 5549 563d 2243 6f6e 7465        P-EQUIV="Conte
```

Here the web bot is double-checking for instructions in a “robots” META file. These files are used by savvy webmasters to express their preferences for content inclusion in the web bots’ index. In general, this is a well-behaved web-bot, following the standard conventions and Netiquette expected of an automated web content update agent.

The original purpose of the “WEB-CGI redirect access” Snort rule was to warn of potential attempts to exploit a known vulnerability in older versions of Allaire’s ClusterCats load balancer and ColdFusion products. Detailed information regarding this vulnerability is available here: http://online.securityfocus.com/bid/1179/info/

Note that this rule will fire an **any** http request containing the text string “/redirect”. Given that the webserver in question uses http redirects by necessity, and does not run any of the vulnerable Allaire products, this particular Snort rule will likely yield nothing but false positives, at least with regard to this particular web server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

6. Correlations –
Description of the FAST "Web Search" product:
http://www.fastsearch.net/products/websearch/index.asp

Advisories regarding the original vulnerabilities in Allaire ColdFusion and ClusterCats:
http://online.securityfocus.com/bid/1179/info/

David Leadston's Practical Detect posting to the Incidents.Org mailing list regarding a ClusterCats detect:
http://cert.uni-stuttgart.de/archive/intrusions/2002/10/msg00049.html

7. Evidence of Active Targeting –
There is ample evidence of active targeting here. Out of 14 routable IP addresses on my network, this "attack" was only directed at ONLY ONE address, namely xxx.yyy.zzz.241. This is especially clear when one consider that there are other active web servers on the network that were not targeted at all. The "attacker" clearly has selected this particular IP address with some very specific goal in mind. That goal is to update their catalog of information regarding the web content of this server.

8. Severity –
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: Importance of the targeted system. This is a co-located web-server on the Internet facing-DMZ of my home network. While it does not contain any highly sensitive data, it is the home base of a very popular hobbyist bulletin-board and chat room frequented by avid home-brewers. These hobbyists would suffer significant disappointment if the server were negatively impacted. I will assign a **2** to Criticality.

Lethality: How severe is the damage if the attack succeeds? In this particular case, a successful "attack" is actually something rather positive: It results in up-to-date information regarding the hobbyist web-site and its services being made available to a broader audience. I will assign a **1** here.

System Countermeasures: The web-server's System Administrators are extremely security conscious, and apply any patches relevant to major new vulnerabilities immediately upon notification. However, sometimes they are too busy to immediately address vulnerabilities receiving lower levels of notoriety. I assign a **4** for System Countermeasures.

Network Countermeasures: Port 80 is wide open at the firewall by necessity (this is a publicly-accessible web-server, after all). All IP addresses are allowed access, regardless of geographic location. An IDS is obviously in place, or we would not be analyzing this detect in the first place. I will assign a rating of **2** here.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Severity = (2 + 1) – (4 + 2) = -3

9. Defensive Recommendation –

Existing system & network countermeasures are adequate. Given that there are no vulnerable Allaire products at this site, this Snort rule can be safely disabled without ill effect.

However, SysAdmins should continue to monitor for new service packs and patches relevant to the server.

10. Multiple Choice Question –

What is the most likely explanation for the trace below?

```
21:40:59.408512 IP xxx.yyy.zzz.142.80 > 66.77.73.84.1218: P 1:605(604) ack 170 win
8111 (DF)
0x0000  4500 0284 7a8c 4000 8006 3666 d151 ea8e          E...z.@...6f.Q..
0x0010  424d 4954 0050 04c2 0519 eed6 400c 06df          BMIT.P......@...
0x0020  5018 1faf cdf9 0000 4854 5450 2f31 2e31          P.......HTTP/1.1
0x0030  2034 3034 204f 626a 6563 7420 4e6f 7420          .404.Object.Not.
0x0040  466f 756e 640d 0a53 6572 7665 723a 204d          Found..Server:.M
0x0050  6963 726f 736f 6674 2d49 4953 2f34 2e30          icrosoft-IIS/4.0
0x0060  0d0a 4461 7465 3a20 4672 692c 2032 3820          ..Date:.Fri,.28.
0x0070  4d61 7220 3230 3033 2030 333a 3335 3a32          Mar.2003.03:35:2
0x0080  3420 474d 540d 0a43 6f6e 7465 6e74 2d4c          4.GMT..Content-L
0x0090  656e 6774 683a 2034 3631 0d0a 436f 6e74          ength:.461..Cont
0x00a0  656e 742d 5479 7065 3a20 7465 7874 2f68          ent-Type:.text/h
0x00b0  746d 6c0d 0a0d 0a3c 6874 6d6c 3e3c 6865          tml....<html><he
0x00c0  6164 3e3c 7469 746c 653e 4572 726f 7220          ad><title>Error.
0x00d0  3430 343c 2f74 6974 6c65 3e0d 0a0d 0a3c          404</title>....<
0x00e0  6d65 7461 206e 616d 653d 2272 6f62 6f74          meta.name="robot
0x00f0  7322 2063 6f6e 7465 6e74 3d22 6e6f 696e          s".content="noin
0x0100  6465 7822 3e0d 0a3c 4d45 5441 2048 5454          dex">..<META.HTT
0x0110  502d 4551 5549 563d 2243 6f6e 7465               P-EQUIV="Conte
```

a) a hacker is searching this web server for "warez", without success.
b) Code Red has tried and failed to infect this web server.
c) An automated web content indexing agent is doing its job.
d) A vulnerability scanner is being run against this web server.

Correct answer:
c) An automated web content indexing agent is doing its job.
(the "meta.name='robots'.content='noindex'" text is a very strong indication this is an automated web-indexing agent at work, cataloging web content).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Detect # 3 –
"It's Code Red! No, It's Nimda! No, it's, it's….???"

```
[**] [1:1256:7] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:25.552753 202.136.189.51:3389 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:47201 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x171A0707  Ack: 0xBC7D52  Win: 0x2238  TcpLen: 20
[Xref => url www.cert.org/advisories/CA-2001-19.html]

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:26.238232 202.136.189.51:3390 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:52577 IpLen:20 DgmLen:150 DF
***AP*** Seq: 0x819EE1D9  Ack: 0xBC7D67  Win: 0x2238  TcpLen: 20

[**] [1:1256:7] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:29.239814 202.136.189.51:3404 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:6242 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0xD1CD659C  Ack: 0xBC7D93  Win: 0x2238  TcpLen: 20
[Xref => url www.cert.org/advisories/CA-2001-19.html]

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:29.870857 202.136.189.51:3394 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:10594 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0xE63DB0D1  Ack: 0xBC7D74  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:29.947750 202.136.189.51:3407 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:11362 IpLen:20 DgmLen:150 DF
***AP*** Seq: 0xD09AF715  Ack: 0xBC7D9D  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:30.548233 202.136.189.51:3409 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:16482 IpLen:20 DgmLen:156 DF
***AP*** Seq: 0xC96A9158  Ack: 0xBC7DB0  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:30.623451 202.136.189.51:3411 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:16994 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0x265DDBF6  Ack: 0xBC7DB4  Win: 0x2238  TcpLen: 20

[**] [1:1945:1] WEB-IIS unicode directory traversal attempt [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:31.240974 202.136.189.51:3412 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:21602 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0xDC5A2460  Ack: 0xBC7DBA  Win: 0x2238  TcpLen: 20
[Xref => cve CVE-2000-0884]

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:31.394290 202.136.189.51:3414 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:23138 IpLen:20 DgmLen:156 DF
***AP*** Seq: 0xAC25C5CD  Ack: 0xBC7DC9  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
03/29-06:27:31.915149 202.136.189.51:3418 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:28002 IpLen:20 DgmLen:145 DF
***AP*** Seq: 0xA3DAFDC4  Ack: 0xBC7DDA  Win: 0x2238  TcpLen: 20

[**] [1:1945:1] WEB-IIS unicode directory traversal attempt [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:32.076022 202.136.189.51:3419 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:28514 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0x2A236276  Ack: 0xBC7DEE  Win: 0x2238  TcpLen: 20
[Xref => cve CVE-2000-0884]

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:32.650665 202.136.189.51:3423 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:35170 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0xCBB0FFFA  Ack: 0xBC7E02  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:32.791266 202.136.189.51:3425 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:36450 IpLen:20 DgmLen:145 DF
***AP*** Seq: 0x2D1B1B17  Ack: 0xBC7E07  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:33.336628 202.136.189.51:3426 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:41570 IpLen:20 DgmLen:151 DF
***AP*** Seq: 0xFB962C66  Ack: 0xBC7E10  Win: 0x2238  TcpLen: 20

[**] [1:1002:5] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:33.683365 202.136.189.51:3428 -> xxx.yyy.zzz.142:80
TCP TTL:113 TOS:0x0 ID:44642 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x59C34B71  Ack: 0xBC7E14  Win: 0x2238  TcpLen: 20

[**] [1:1945:1] WEB-IIS unicode directory traversal attempt [**]
[Classification: Web Application Attack] [Priority: 1]
03/29-06:27:34.140866 202.136.189.51:3431 -> xxx.yyy.zzz.141:80
TCP TTL:113 TOS:0x0 ID:49506 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x380E5209  Ack: 0xBC7E1A  Win: 0x2238  TcpLen: 20
[Xref => cve CVE-2000-0884]
```

[this pattern of alerts continues repeatedly at this very rapid pace until 6:40am – a total attack window of almost 13 solid minutes, hundreds of alerts were generated during this timeframe!]

1. Source of Trace -

For the past month I have been capturing the first 300 bytes of every packet passing through the Internet-facing subnet on my home network. This is being accomplished with a Linux server in my DMZ running tcpdump in promiscuous mode on 'eth0'. Periodically, I run all the captured traffic through a Snort configurations using the default rule set.

2. Detect was generated by –

The network detect is from a Snort intrusion detection system with a standard default 1.9.1 rule set.

The Snort rules that generated these alerts were:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

"WEB-IIS CodeRed v2 root.exe access" alert:
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase; classtype:web-application-attack; reference:url,www.cert.org/advisories/CA-2001-19.html; sid:1256; rev:7;)

"WEB-IIS cmd.exe access" alert:
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; flow:to_server,established; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:5;)

"WEB-IIS unicode directory traversal attempt" alert:
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS unicode directory traversal attempt"; flow:to_server,established; content:"/..%c0%af../"; nocase; classtype:web-application-attack; reference:cve,CVE-2000-0884; sid:981; rev:6;)

3. Probability the source address was spoofed –

It is very unlikely that the source IP address was spoofed. These types of web application exploits are explicitly directed at obtaining a root shell on a vulnerable IIS web-server. In order to do this, the attacker would need to somehow establish a successful three-way tcp handshake with the web-server in question, and would need access to the system that originated the connection.

However, there is an excellent probability that the attacking system is a previously root-compromised system under the attacker's direct control that he or she is using as an "attack host" to direct any resulting scrutiny elsewhere.

4. Description of the attack –

Here is what we know about the attacking IP address (from www.Dshield.Org):

IP Address: 202.136.189.51
HostName: mail.glorymhm.com.sg
Total Records against IP: 1372
Number of targets: 2
Ports Attacked (up to 10):

Port	Attacks	Start	End
80	2058	2003-03-25	2003-03-25

Whois: inetnum: 202.136.160.0 - 202.136.191.255
netname: NTTS
country: SG
descr: NTT Singapore Pte.Ltd.
20 Cecil Street #11-03/06 Singapore Exchange Singapore
admin_c: OO2-AP
tech_c: OO2-AP
remarks: NTT Signapore plans to start internet data center
service and internet access service on April. 1st.
mnt_by: APNIC-HM
changed: hostmaster@apnic.net 20010222
status: ALLOCATED PORTABLE
source: APNIC
mnt_lower: MAINT-SG-NTTS
start: 3397951488
end: 3397959679
diff: 8191

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

person: Osamu Ono
address: NTT International Singapore
20 Cecil Street
#11-03/06 The Exchange
Singapore 049705
phone: +65 2314119
fax_no: +65 4383012
e_mail: ono@ntti.com.sg
nic_hdl: OO2-AP
mnt_by: MAINT-NULL
changed: shafiah1@singnet.com.sg 19990517
source: APNIC
notify: hostmaster@singnet.com.sg

Clearly, this host has been used to mount significant suspicious activities against web-servers before! Further investigation is definitely warranted.

At first glance this network traffic pattern could easily be mistaken as a routine automated probe of my network by a web-server infected with the Nimda worm. The attempted exploits shown in the trace above are the exact same ones used by Nimda in its efforts to compromise any IIS web-servers it may find in its random searches of routable Internet IP space.

However, upon closer examination, this traffic is not consistent with Nimda (at least not any incarnation of Nimda that I have seen to date). Nimda is not this persistent. It will generally hit a target server with several unicode and cmd.exe attempts in extremely short order (under one minute). It will either infect the server within this time or not, but either way it will be moving on to its next target much more quickly than we see here. This makes sense; it could certainly not have become one of the more successful and notorious worms in Internet history if it spent multiple minutes trying to infect servers that are not vulnerable.

But if it's not Nimda, what is it? Probably some kind of automated attack script or maybe even a commercial vulnerability scanning tool, but we need to perform more analysis to say anything conclusive.

5. Attack Mechanism –

Further investigation is definitely warranted, so let's have a close look at some to the tcpdump capture files from this timeframe:

```
tcpdump -r capturefile -X -n 'host 202.136.189.51' > textfile
```

Looking through the resulting textfile, we can easily how the attack began:

```
06:26:14.003387 IP 202.136.189.51 > xxx.yyy.zzz.128: icmp 17: echo request seq 2897
0x0000  4500 0025 225b 0000 7101 e3ee ca88 bd33       E..%"[..q......3
0x0010  d151 ea80 0800 297d 0100 0b51 6865 6c6c       .Q....)}...Qhell
0x0020  6f20 3f3f 3f00 0000 0000 0000 0000            o.???.........
06:26:14.003960 IP xxx.yyy.zzz.133 > 202.136.189.51: icmp 17: echo reply seq 2897
0x0000  4500 0025 26de 0000 ff01 5166 d151 ea85       E..%&.....Qf.Q..
0x0010  ca88 bd33 0000 317d 0100 0b51 6865 6c6c       ...3..1}...Qhell
0x0020  6f20 3f3f 3f00 0000 0000 0000 0000            o.???.........
06:26:14.005830 IP xxx.yyy.zzz.139 > 202.136.189.51: icmp 17: echo reply seq 2897
0x0000  4500 0025 8bdd 0000 4001 ab61 d151 ea8b       E..%....@..a.Q..
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0010  ca88 bd33 0000 317d 0100 0b51 6865 6c6c       ...3..1}...Qhell
0x0020  6f20 3f3f 3f                                  o.???
```

First, the attacking host sends an icmp echo request packet to the target IP address in a fairly typical (and not always effective) attempt to identify whether a host exists at this address at all. But it gets two replies, from two different IP addresses. Why is this? In this case, the .128 IP address is actually a host network broadcast address, as my /28 subnet of routable IP space begins at .128 and ends at .144, with the endpoint addresses being reserved for host net and broadcast purposes. This automated tool appears to be oblivious to this fact, however, and actually ignores the source IP addresses in the replies that are sent back. It then proceeds to send **two** SYN connection attempt to port 80 on the original IP it probed. Neither of these is successful. Luckily, neither of my chatty hosts that feels the need to respond to broadcast pings has anything running on tcp port 80.

```
06:26:14.339235 IP 202.136.189.51.3155 > xxx.yyy.zzz.128.80: S
2137122782:2137122782(0) win 8192 <mss 1460> (DF)
0x0000  4500 002c 285b 4000 7106 9de2 ca88 bd33       E..,([@.q......3
0x0010  d151 ea80 0c53 0050 7f61 e7de 0000 0000       .Q...S.P.a......
0x0020  6002 2000 c0b4 0000 0204 05b4 7e7e            `...........~~
06:26:15.125456 IP 202.136.189.51.3155 > xxx.yyy.zzz.128.80: S
2993082321:2993082321(0) win 8192 <mss 1460> (DF)
0x0000  4500 002c 3d5b 4000 7106 88e2 ca88 bd33       E..,=[@.q......3
0x0010  d151 ea80 0c53 0050 b266 cfd1 0000 0000       .Q...S.P.f......
0x0020  6002 2000 a5bc 0000 0204 05b4 7e7e            `...........~~
```

That's it for traffic directed at .128; now the process repeats against other IP addresses:

```
06:26:24.356285 IP 202.136.189.51 > xxx.yyy.zzz.130: icmp 17: echo request seq 18001
0x0000   4500 0025 fc5b 0000 7101 09ec ca88 bd33     E..%.[..q......3
0x0010   d151 ea82 0800 ee7c 0100 4651 6865 6c6c     .Q.....|..FQhell
0x0020   6f20 3f3f 3f00 0000 0000 0000 0000          o.???........
06:26:24.356544 IP xxx.yyy.zzz.130 > 202.136.189.51: icmp 17: echo reply seq 18001
0x0000   4500 0025 5643 0000 8001 a104 d151 ea82     E..%VC.......Q..
0x0010   ca88 bd33 0000 f67c 0100 4651 6865 6c6c     ...3...|..FQhell
0x0020   6f20 3f3f 3f00 0000 0000 0000 0000          o.???........
06:26:24.716254 IP 202.136.189.51.3182 > xxx.yyy.zzz.130.80: S 3899983219:3899983219(0) win 8192
<mss 1460> (DF)
0x0000   4500 002c 0b5c 4000 7106 badf ca88 bd33     E..,.\@.q......3
0x0010   d151 ea82 0c6e 0050 e875 0573 0000 0000     .Q...n.P.u.s....
0x0020   6002 2000 39ef 0000 0204 05b4 0000          `...9........
06:26:24.716519 IP xxx.yyy.zzz.130.80 > 202.136.189.51.3182: S 369797678:369797678(0) ack
3899983220 win 8760 <mss 1460> (DF)
0x0000   4500 002c 5743 4000 8006 5ff8 d151 ea82     E..,WC@..._..Q..
0x0010   ca88 bd33 0050 0c6e 160a aa2e e875 0574     ...3.P.n.....u.t
0x0020   6012 2238 776d 0000 0204 05b4 0000          `."8wm........
06:26:25.023626 IP 202.136.189.51.3182 > xxx.yyy.zzz.130.80: . ack 1 win 8760 (DF)
0x0000   4500 0028 0d5c 4000 7106 b8e3 ca88 bd33     E..(.\@.q......3
0x0010   d151 ea82 0c6e 0050 e875 0574 160a aa2f     .Q...n.P.u.t.../
0x0020   5010 2238 8f2a 0000 0204 05b4 0000          P."8.*........
```

Uh OH!! Syn, Syn-Ack, ACK! The 3 way handshake is now complete, a tcp connection is made, and my web-server at .130 may be in for some big trouble! Let's see what happens next:

```
06:26:25.028708 IP 202.136.189.51.3182 > xxx.yyy.zzz.130.80: P 1:42(41) ack 1 win 8760
(DF)
0x0000  4500 0051 0e5c 4000 7106 b7ba ca88 bd33       E..Q.\@.q......3
0x0010  d151 ea82 0c6e 0050 e875 0574 160a aa2f       .Q...n.P.u.t.../
0x0020  5018 2238 45c3 0000 4845 4144 202f 2048       P."8E...HEAD./.H
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0030  5454 502f 312e 300d 0a48 6f73 743a 2032      TTP/1.0..Host:.2
0x0040  3039 2e38 312e 3233 342e 3133 300d 0a0d      09.81.234.130...
0x0050  0a                                           .
```

A simple HTTP 1.0 HEAD request to the root directory of the web server. My stalwart web-server at .130 replies:

```
06:26:25.031949 IP xxx.yyy.zzz.130.80 > 202.136.189.51.3182: P 1:149(148) ack
42 win 8719 (DF)
0x0000       4500 00bc 5843 4000 8006 5e68 d151 ea82  E...XC@...^h.Q..
0x0010       ca88 bd33 0050 0c6e 160a aa2f e875 059d  ...3.P.n.../.u..
0x0020       5018 220f e87f 0000 4854 5450 2f31 2e31  P."....HTTP/1.1
0x0030       2034 3031 2041 6363 6573 7320 4465 6e69  .401.Access.Deni
0x0040       6564 0d0a 5757 572d 4175 7468 656e 7469  ed..WWW-Authenti
0x0050       6361 7465 3a20 4e54 4c4d 0d0a 5757 572d  cate:.NTLM..WWW-
0x0060       4175 7468 656e 7469 6361 7465 3a20 4261  Authenticate:.Ba
0x0070       7369 6320 7265 616c 6d3d 2232 3039 2e38  sic.realm="209.8
0x0080       312e 3233 342e 3133 3022 0d0a 436f 6e74  1.234.130"..Cont
0x0090       656e 742d 4c65 6e67 7468 3a20 3634 340d  ent-Length:.644.
0x00a0       0a43 6f6e 7465 6e74 2d54 7970 653a 2074  .Content-Type:.t
0x00b0       6578 742f 6874 6d6c 0d0a 0d0a            ext/html....
06:26:25.032510 IP xxx.yyy.zzz.130.80 > 202.136.189.51.3182: F 149:149(0) ack
42 win 8719 (DF)
0x0000       4500 0028 5943 4000 8006 5dfc d151 ea82  E..(YC@...]..Q..
0x0010       ca88 bd33 0050 0c6e 160a aac3 e875 059d  ...3.P.n.....u..
0x0020       5011 220f 8e95 0000 0000 0000 0000       P."...........
06:26:25.354392 IP 202.136.189.51.3182 > xxx.yyy.zzz.130.80: . ack 150 win
8612 (DF)
0x0000       4500 0028 175c 4000 7106 aee3 ca88 bd33  E..(.\@.q......3
0x0010       d151 ea82 0c6e 0050 e875 059d 160a aac4  .Q...n.P.u......
0x0020       5010 21a4 8f00 0000 0204 05b4 0a0d       P.!...........
06:26:25.360930 IP 202.136.189.51.3182 > xxx.yyy.zzz.130.80: F 42:42(0) ack
150 win 8612 (DF)
0x0000       4500 0028 185c 4000 7106 ade3 ca88 bd33  E..(.\@.q......3
0x0010       d151 ea82 0c6e 0050 e875 059d 160a aac4  .Q...n.P.u......
0x0020       5011 21a4 8eff 0000 0204 05b4 0a0d       P.!...........
06:26:25.361152 IP xxx.yyy.zzz.130.80 > 202.136.189.51.3182: . ack 43 win
8719 (DF)
0x0000       4500 0028 5a43 4000 8006 5cfc d151 ea82  E..(ZC@...\..Q..
0x0010       ca88 bd33 0050 0c6e 160a aac4 e875 059e  ...3.P.n.....u..
0x0020       5010 220f 8e94 0000 0000 0000 0000       P."...........
```

"Hey, you need some NTLM logon credentials to get anything outta me, d00d!! Have a nice day!" Good job, .130! .130 has told the attacker what he can do with his automated attack script. Our attacker is not yet done with .130 though:

```
06:26:25.371984 IP 202.136.189.51.3184 > xxx.yyy.zzz.130.57: S
4193413308:4193413308(0) win 8192 <mss 1460> (DF)
0x0000       4500 002c 195c 4000 7106 acdf ca88 bd33  E..,.\@.q......3
0x0010       d151 ea82 0c70 0039 f9f2 68bc 0000 0000  .Q...p.9..h.....
0x0020       6002 2000 c53d 0000 0204 05b4 0a0d       `....=........
06:26:25.372171 IP xxx.yyy.zzz.130.57 > 202.136.189.51.3184: R 0:0(0) ack
4193413309 win 0
0x0000       4500 0028 5b43 0000 8006 9bfc d151 ea82  E..([C.......Q..
0x0010       ca88 bd33 0039 0c70 0000 0000 f9f2 68bd  ...3.9.p......h.
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0020       5014 0000 fce6 0000 0000 0000 0000       P.............
```

[This pattern repeats 3 times]

No dice here;, we don't speak no tcp port 57 round these parts. From the timing of the packets, I believe the repetitions are due to tcp retries at the stack level. I had to look up the significance of tcp port 57. It is a Mail Transfer Protocol (MTP) described in RFC 772 and 780

```
06:26:28.083056 IP 202.136.189.51.3193 > xxx.yyy.zzz.130.21: S
2781711404:2781711404(0) win 8192 <mss 1460> (DF)
0x0000  4500 002c 565c 4000 7106 6fdf ca88 bd33      E..,V\@.q.o....3
0x0010  d151 ea82 0c79 0015 a5cd 8c2c 0000 0000      .Q...y.....,....
0x0020  6002 2000 f60d 0000 0204 05b4 0a0d           `.............
06:26:28.083220 IP xxx.yyy.zzz.130.21 > 202.136.189.51.3193: R 0:0(0) ack 2781711405
win 0
0x0000  4500 0028 5f43 0000 8006 97fc d151 ea82      E..(_C.......Q..
0x0010  ca88 bd33 0015 0c79 0000 0000 a5cd 8c2d      ...3...y.......-
0x0020  5014 0000 2db7 0000 0000 0000 0000           P...-.........
```

He's also looking for FTP servers. Again, no dice on this host.

Undaunted, our attacker (or his automated minion) moves on. Since we are quite familiar with the sequence 1) ICMP echo request, 2) SYN connect to port 80, 3) HTTP 1.0 HEAD request, 4) probe tcp ports 57 and 21, I will not show these packets in the subsequent analysis. Our automated attacker continues upward with this now very familiar pattern sequentially upward through the IP address space of my network. Nothing interesting happens until we get to IP .141, port 80:

```
06:27:24.860147 IP xxx.yyy.zzz.141.80 > 202.136.189.51.3382: P 1:245(244) ack
42 win 8719 (DF)
0x0000       4500 011c e6a4 4000 8006 cf9b d151 ea8d  E.....@......Q..
0x0010       ca88 bd33 0050 0d36 00bc 7d4a 0e89 0ad2  ...3.P.6..}J....
0x0020       5018 220f b7fd 0000 4854 5450 2f31 2e31  P."....HTTP/1.1
0x0030       2033 3032 204f 626a 6563 7420 4d6f 7665  .302.Object.Move
0x0040       640d 0a4c 6f63 6174 696f 6e3a 2073 6b6f  d..Location:.xxx
0x0050       7472 6174 0d0a 5365 7276 6572 3a20 4d69  xxxx..Server:.Mi
0x0060       6372 6f73 6f66 742d 4949 532f 342e 300d  crosoft-IIS/4.0.
0x0070       0a43 6f6e 7465 6e74 2d54 7970 653a 2074  .Content-Type:.t
0x0080       6578 742f 6874 6d6c 0d0a 436f 6e74 656e  ext/html..Conten
0x0090       742d 4c65 6e67 7468 3a20 3132 330d 0a0d  t-Length:.123...
0x00a0       0a3c 6865 6164 3e3c 7469 746c 653e 446f  .<head><title>Do
0x00b0       6375 6d65 6e74 204d 6f76 6564 3c2f 7469  cument.Moved</ti
0x00c0       746c 653e 3c2f 6865 6164 3e0a 3c62 6f64  tle></head>.<bod
0x00d0       793e 3c68 313e 4f62 6a65 6374 204d 6f76  y><h1>Object.Mov
0x00e0       6564 3c2f 6831 3e54 6869 7320 646f 6375  ed</h1>This.docu
0x00f0       6d65 6e74 206d 6179 2062 6520 666f 756e  ment.may.be.foun
0x0100       6420 3c61 2048 5245 463d 2273 6b6f 7472  d.<a.HREF="xxxxx
0x0110       6174 223e 6865 7265 3c2f 613e            xx">here</a>
```

Uh oh, – an "HTTP 302 – Object moved message". This is actually an open, publicly accessible web-server. How will our automated attack buddy react?

Like this:

```
06:27:25.552753 IP 202.136.189.51.3389 > xxx.yyy.zzz.141.80: P 1:67(66) ack 1 win 8760
(DF)
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0000  4500 006a b861 4000 7106 0d91 ca88 bd33      E..j.a@.q......3
0x0010  d151 ea8d 0d3d 0050 171a 0707 00bc 7d52      .Q...=.P......}R
0x0020  5018 2238 e501 0000 4845 4144 202f 4d53      P."8....HEAD./MS
0x0030  4144 432f 726f 6f74 2e65 7865 3f2f 632b      ADC/root.exe?/c+
0x0040  6469 722b 633a 5c20 4854 5450 2f31 2e30      dir+c:\.HTTP/1.0
0x0050  0d0a 486f 7374 3a20 3230 392e 3831 2e32      ..Host:.209.81.2
0x0060  3334 2e31 3431 0d0a 0d0a                     34.141....
```

and like this:

```
06:27:26.238232 IP 202.136.189.51.3390 > xxx.yyy.zzz.141.80: P 1:111(110) ack 1 win
8760 (DF)
0x0000  4500 0096 cd61 4000 7106 f864 ca88 bd33      E....a@.q..d...3
0x0010  d151 ea8d 0d3e 0050 819e e1d9 00bc 7d67      .Q...>.P......}g
0x0020  5018 2238 d5a9 0000 4845 4144 202f 5042      P."8....HEAD./PB
0x0030  5365 7276 6572 2f2e 2e25 2533 3525 3633      Server/..%%35%63
0x0040  2e2e 2525 3335 2536 332e 2e25 2533 3525      ..%%35%63..%%35%
0x0050  3633 7769 6e6e 742f 7379 7374 656d 3332      63winnt/system32
0x0060  2f63 6d64 2e65 7865 3f2f 632b 6469 722b      /cmd.exe?/c+dir+
0x0070  633a 5c20 4854 5450 2f31 2e30 0d0a 486f      c:\.HTTP/1.0..Ho
0x0080  7374 3a20 3230 392e 3831 2e32 3334 2e31      st:.xxx.yyy.zzz.1
0x0090  3431 0d0a 0d0a                               41....
```

and like this:

```
06:27:31.915149 IP 202.136.189.51.3418 > xxx.yyy.zzz.141.80: P 1:106(105) ack 1 win
8760 (DF)
0x0000  4500 0091 6d62 4000 7106 5869 ca88 bd33      E...mb@.q.Xi...3
0x0010  d151 ea8d 0d5a 0050 a3da fdc4 00bc 7dda      .Q...Z.P......}.
0x0020  5018 2238 4e27 0000 4845 4144 202f 5270      P."8N'..HEAD./Rp
0x0030  632f 2e2e 2525 3335 2536 332e 2e25 2533      c/..%%35%63..%%3
0x0040  3525 3633 2e2e 2525 3335 2536 3377 696e      5%63..%%35%63win
0x0050  6e74 2f73 7973 7465 6d33 322f 636d 642e      nt/system32/cmd.
0x0060  6578 653f 2f63 2b64 6972 2b63 3a5c 2048      exe?/c+dir+c:\.H
0x0070  5454 502f 312e 300d 0a48 6f73 743a 2032      TTP/1.0..Host:.2
0x0080  3039 2e38 312e 3233 342e 3134 310d 0a0d      09.81.234.141...
0x0090  0a                                           .
```

and another:

```
06:39:37.340330 IP 202.136.189.51.3117 > xxx.yyy.zzz.141.80: P 1:126(125) ack 1 win
8760 (DF)
0x0000  4500 00a5 40bc 4000 7106 84fb ca88 bd33      E...@.@.q......3
0x0010  d151 ea8d 0c2d 0050 bb39 f701 00d8 1182      .Q...-.P.9......
0x0020  5018 2238 5f82 0000 4845 4144 202f 6578      P."8_...HEAD./ex
0x0030  6368 616e 6765 2f63 6865 636b 2e62 6174      change/check.bat
0x0040  2f2e 2e25 6331 2531 632e 2e25 6331 2531      /..%c1%1c..%c1%1
0x0050  632e 2e25 6331 2531 6377 696e 6e74 2f73      c..%c1%1cwinnt/s
0x0060  7973 7465 6d33 322f 636d 642e 6578 653f      ystem32/cmd.exe?
0x0070  2f63 2b64 6972 203f 2f63 2b64 6972 2b63      /c+dir.?/c+dir+c
0x0080  3a5c 2048 5454 502f 312e 300d 0a48 6f73      :\.HTTP/1.0..Hos
0x0090  743a 2032 3039 2e38 312e 3233 342e 3134      t:.xxx.yyy.zzz.14
0x00a0  310d 0a0d 0a                                 1....
```

Not nice!! The minute the attack tool smells a web server that might be vulnerable, it starts throwing several well-known IIS exploits at the server, not just once, but in a systematic effort to test every possible permutation of subdirectory locations that might possibly used to get at cmd.exe! (There are **literally hundreds** of attempts to exploit cmd.exe through the MDAC, Unicode, and Double-Decode vulnerabilities in these logs. I will spare the gentle reader all of the gory details).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Luckily, in this particular case the web-server in question was up the latest patch levels, and was not vulnerable to this exploit. Had the web-servers in question not been patched, they would certainly have been completely compromised by this automated attack.

But web-servers are not the only type of system this automated tool is seeking to exploit. We've seen that it also probes tcp ports 21 and 57. Can we learn anything further about what its intentions might be toward any FTP or MTP servers that it might encounter in its automated travels?

tcpdump -r capturefile -X -n host 202.136.1 89.51 and port 21 > ftpfile.txt

yields the following sobering exchange:

```
06:27:52.088223 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 1:55(54) ack 1 win 5840
(DF)
0x0000  4500 005e 0ce1 4000 4006 ea1f d151 ea8b      E..^..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bb11 3743 08cb      ...3.....,..7C..
0x0020  5018 16d0 df3c 0000 3232 3020 6761 6c61      P....<..220.gala
0x0030  6472 6965 6c20 4654 5020 7365 7276 6572      driel.FTP.server
0x0040  2028 5665 7273 696f 6e20 7775 2d32 2e36      .(Version.wu-2.6
0x0050  2e32 2d38 2920 7265 6164 792e 0d0a           .2-8).ready...
06:27:52.401561 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 1:17(16) ack 55 win
8706 (DF)
0x0000  4500 0038 2d65 4000 7106 98c1 ca88 bd33      E..8-e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 08cb a92c bb47      .Q......7C...,.G
0x0020  5018 2202 0fea 0000 5553 4552 2061 6e6f      P."....USER.ano
0x0030  6e79 6d6f 7573 0d0a                          nymous..
06:27:52.401740 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: . ack 17 win 5840 (DF)
0x0000  4500 0028 0ce2 4000 4006 ea54 d151 ea8b      E..(..@.@..T.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bb47 3743 08db      ...3.....,.G7C..
0x0020  5010 16d0 a300 0000                          P.......
06:27:52.404221 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 55:123(68) ack 17 win
5840 (DF)
0x0000  4500 006c 0ce3 4000 4006 ea0f d151 ea8b      E..l..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bb47 3743 08db      ...3.....,.G7C..
0x0020  5018 16d0 b90f 0000 3333 3120 4775 6573      P.......331.Gues
0x0030  7420 6c6f 6769 6e20 6f6b 2c20 7365 6e64      t.login.ok,.send
0x0040  2079 6f75 7220 636f 6d70 6c65 7465 2065      .your.complete.e
0x0050  2d6d 6169 6c20 6164 6472 6573 7320 6173      -mail.address.as
0x0060  2070 6173 7377 6f72 642e 0d0a                .password...
06:27:52.718373 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 17:35(18) ack 123 win
8638 (DF)
0x0000  4500 003a 3065 4000 7106 95bf ca88 bd33      E..:0e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 08db a92c bb8b      .Q......7C...,..
0x0020  5018 21be 0ba4 0000 5041 5353 2061 6e6f      P.!.....PASS.ano
0x0030  4061 6e6f 2e63 6f6d 0d0a                     @ano.com..
```

Whoa! The attack tool has logged onto my DMZ Linux server via anonymous FTP!! Not good! Let's see what it did: (commands sent by the tool are in **bold** in the ascii dump on the right)

```
06:27:53.035359 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 35:43(8) ack 171 win
8590 (DF)
0x0000  4500 0030 3565 4000 7106 90c9 ca88 bd33      E..05e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 08ed a92c bbbb      .Q......7C...,..
0x0020  5018 218e c5ba 0000 5459 5045 2049 0d0a      P.!.....TYPE.I..
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
06:27:53.035570 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 171:191(20) ack 43 win
5840 (DF)
0x0000  4500 003c 0ce5 4000 4006 ea3d d151 ea8b      E..<..@.@..=.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bbbb 3743 08f5      ...3.....,..7C..
0x0020  5018 16d0 0f73 0000 3230 3020 5479 7065      P....s..200.Type
0x0030  2073 6574 2074 6f20 492e 0d0a                .set.to.I...
06:27:53.335252 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 43:51(8) ack 191 win
8570 (DF)
0x0000  4500 0030 3f65 4000 7106 86c9 ca88 bd33      E..0?e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 08f5 a92c bbcf      .Q......7C...,..
0x0020  5018 217a c4aa 0000 5354 5255 2046 0d0a      P.!z....STRU.F..
06:27:53.335461 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 191:207(16) ack 51 win
5840 (DF)
0x0000  4500 0038 0ce6 4000 4006 ea40 d151 ea8b      E..8..@.@..@.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bbcf 3743 08fd      ...3.....,..7C..
0x0020  5018 16d0 e156 0000 3230 3020 5354 5255      P....V..200.STRU
0x0030  2046 206f 6b2e 0d0a                          .F.ok...
06:27:53.663663 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 51:59(8) ack 207 win
8554 (DF)
0x0000  4500 0030 4665 4000 7106 7fc9 ca88 bd33      E..0Fe@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 08fd a92c bbdf      .Q......7C...,..
0x0020  5018 216a d8aa 0000 4d4f 4445 2053 0d0a      P.!j....MODE.S..
06:27:53.663825 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 207:223(16) ack 59 win
5840 (DF)
0x0000  4500 0038 0ce7 4000 4006 ea3f d151 ea8b      E..8..@.@..?.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bbdf 3743 0905      ...3.....,..7C..
0x0020  5018 16d0 f546 0000 3230 3020 4d4f 4445      P....F..200.MODE
0x0030  2053 206f 6b2e 0d0a                          .S.ok...
06:27:53.969825 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 59:67(8) ack 223 win
8538 (DF)
0x0000  4500 0030 4d65 4000 7106 78c9 ca88 bd33      E..0Me@.q.x....3
0x0010  d151 ea8b 0dc3 0015 3743 0905 a92c bbef      .Q......7C...,..
0x0020  5018 215a c4c0 0000 5245 5354 2030 0d0a      P.!Z....REST.0..
06:27:53.970046 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 223:290(67) ack 67 win
5840 (DF)
0x0000  4500 006b 0ce8 4000 4006 ea0b d151 ea8b      E..k..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bbef 3743 090d      ...3.....,..7C..
0x0020  5018 16d0 c730 0000 3335 3020 5265 7374      P....0..350.Rest
0x0030  6172 7469 6e67 2061 7420 302e 2053 656e      arting.at.0..Sen
0x0040  6420 5354 4f52 4520 6f72 2052 4554 5249      d.STORE.or.RETRI
0x0050  4556 4520 746f 2069 6e69 7469 6174 6520      EVE.to.initiate.
0x0060  7472 616e 7366 6572 2e0d 0a                  transfer...
06:27:54.281907 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 67:75(8) ack 290 win
8471 (DF)
0x0000  4500 0030 5665 4000 7106 6fc9 ca88 bd33      E..0Ve@.q.o....3
0x0010  d151 ea8b 0dc3 0015 3743 090d a92c bc32      .Q......7C...,.2
0x0020  5018 2117 c4b7 0000 5245 5354 2031 0d0a      P.!.....REST.1..
06:27:54.282219 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 290:357(67) ack 75 win
5840 (DF)
0x0000  4500 006b 0ce9 4000 4006 ea0a d151 ea8b      E..k..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bc32 3743 0915      ...3.....,.27C..
0x0020  5018 16d0 c5e5 0000 3335 3020 5265 7374      P.......350.Rest
0x0030  6172 7469 6e67 2061 7420 312e 2053 656e      arting.at.1..Sen
0x0040  6420 5354 4f52 4520 6f72 2052 4554 5249      d.STORE.or.RETRI
0x0050  4556 4520 746f 2069 6e69 7469 6174 6520      EVE.to.initiate.
0x0060  7472 616e 7366 6572 2e0d 0a                  transfer...
06:27:54.607029 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 75:83(8) ack 357 win
8404 (DF)
0x0000  4500 0030 5d65 4000 7106 68c9 ca88 bd33      E..0]e@.q.h....3
0x0010  d151 ea8b 0dc3 0015 3743 0915 a92c bc75      .Q......7C...,.u
0x0020  5018 20d4 c4b0 0000 5245 5354 2030 0d0a      P.......REST.0..
06:27:54.607340 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 357:424(67) ack 83 win
5840 (DF)
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0000  4500 006b 0cea 4000 4006 ea09 d151 ea8b      E..k..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bc75 3743 091d      ...3.....,.u7C..
0x0020  5018 16d0 c69a 0000 3335 3020 5265 7374      P.......350.Rest
0x0030  6172 7469 6e67 2061 7420 302e 2053 656e      arting.at.0..Sen
0x0040  6420 5354 4f52 4520 6f72 2052 4554 5249      d.STORE.or.RETRI
0x0050  4556 4520 746f 2069 6e69 7469 6174 6520      EVE.to.initiate.
0x0060  7472 616e 7366 6572 2e0d 0a                  transfer...
06:27:54.935819 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 83:89(6) ack 424 win
8337 (DF)
0x0000  4500 002e 6665 4000 7106 5fcb ca88 bd33      E...fe@.q._....3
0x0010  d151 ea8b 0dc3 0015 3743 091d a92c bcb8      .Q......7C...,..
0x0020  5018 2091 e3c6 0000 5359 5354 0d0a           P.......SYST..
06:27:54.936030 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 424:443(19) ack 89 win
5840 (DF)
0x0000  4500 003b 0ceb 4000 4006 ea38 d151 ea8b      E..;..@.@..8.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bcb8 3743 0923      ...3.....,..7C.#
0x0020  5018 16d0 39dc 0000 3231 3520 554e 4958      P...9...215.UNIX
0x0030  2054 7970 653a 204c 380d 0a                  .Type:.L8..
06:27:55.231727 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 89:95(6) ack 443 win
8318 (DF)
0x0000  4500 002e 6f65 4000 7106 56cb ca88 bd33      E...oe@.q.V....3
0x0010  d151 ea8b 0dc3 0015 3743 0923 a92c bccb      .Q......7C.#.,..
0x0020  5018 207e e6d6 0000 5041 5356 0d0a           P..~....PASV..
06:27:55.235507 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 443:494(51) ack 95 win
5840 (DF)
0x0000  4500 005b 0cec 4000 4006 ea17 d151 ea8b      E..[..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bccb 3743 0929      ...3.....,..7C.)
0x0020  5018 16d0 ee64 0000 3232 3720 456e 7465      P....d..227.Ente
0x0030  7269 6e67 2050 6173 7369 7665 204d 6f64      ring.Passive.Mod
0x0040  6520 2832 3039 2c38 312c 3233 342c 3133      e.(209,81,234,13
0x0050  392c 3536 2c31 3330 290d 0a                  9,56,130)..
06:27:55.692769 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: . ack 494 win 8267 (DF)
0x0000  4500 0028 7d65 4000 7106 48d1 ca88 bd33      E..(}e@.q.H....3
0x0010  d151 ea8b 0dc3 0015 3743 0929 a92c bcfe      .Q......7C.).,..
0x0020  5010 204b 9780 0000 0204 05b4 0d0a           P..K..........
06:27:55.884143 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 95:103(8) ack 494 win
8267 (DF)
0x0000  4500 0030 8565 4000 7106 40c9 ca88 bd33      E..0.e@.q.@....3
0x0010  d151 ea8b 0dc3 0015 3743 0929 a92c bcfe      .Q......7C.).,..
0x0020  5018 204b c586 0000 5459 5045 2041 0d0a      P..K....TYPE.A..
06:27:55.884390 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 494:514(20) ack 103 win
5840 (DF)
0x0000  4500 003c 0ced 4000 4006 ea35 d151 ea8b      E..<..@.@..5.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bcfe 3743 0931      ...3.....,..7C.1
0x0020  5018 16d0 15f4 0000 3230 3020 5479 7065      P.......200.Type
0x0030  2073 6574 2074 6f20 412e 0d0a                .set.to.A...
06:27:56.104516 IP 202.136.189.51.3494 > xxx.yyy.zzz.143.21: S
1728831932:1728831932(0) win 8192 <mss 1460> (DF)
0x0000  4500 002c 8b65 4000 7106 3ac9 ca88 bd33      E..,.e@.q.:....3
0x0010  d151 ea8f 0da6 0015 670b e1bc 0000 0000      .Q......g.......
0x0020  6002 2000 de05 0000 0204 05b4 2041           `............A
06:27:56.192167 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 103:111(8) ack 514 win
8247 (DF)
0x0000  4500 0030 9165 4000 7106 34c9 ca88 bd33      E..0.e@.q.4....3
0x0010  d151 ea8b 0dc3 0015 3743 0931 a92c bd12      .Q......7C.1.,..
0x0020  5018 2037 ca91 0000 4c49 5354 202f 0d0a      P..7....LIST./..
06:27:56.193021 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 514:577(63) ack 111 win
5840 (DF)
0x0000  4500 0067 0cee 4000 4006 ea09 d151 ea8b      E..g..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bd12 3743 0939      ...3.....,..7C.9
0x0020  5018 16d0 1171 0000 3135 3020 4f70 656e      P....q..150.Open
0x0030  696e 6720 4153 4349 4920 6d6f 6465 2064      ing.ASCII.mode.d
0x0040  6174 6120 636f 6e6e 6563 7469 6f6e 2066      ata.connection.f
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0050  6f72 2064 6972 6563 746f 7279 206c 6973      or.directory.lis
0x0060  7469 6e67 2e0d 0a                            ting...
06:27:56.701028 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: . ack 577 win 8184 (DF)
0x0000  4500 0028 a465 4000 7106 21d1 ca88 bd33      E..(.e@.q.!....3
0x0010  d151 ea8b 0dc3 0015 3743 0939 a92c bd51      .Q......7C.9.,.Q
0x0020  5010 1ff8 9770 0000 0204 05b4 202f           P....p......./
06:27:56.701118 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 577:601(24) ack 111 win
5840 (DF)
0x0000  4500 0040 0cef 4000 4006 ea2f d151 ea8b      E..@..@.@../.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bd51 3743 0939      ...3.....,.Q7C.9
0x0020  5018 16d0 d182 0000 3232 3620 5472 616e      P.......226.Tran
0x0030  7366 6572 2063 6f6d 706c 6574 652e 0d0a      sfer.complete...
06:27:57.025287 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 111:121(10) ack 601 win
8160 (DF)
0x0000  4500 0032 af65 4000 7106 16c7 ca88 bd33      E..2.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0939 a92c bd69      .Q......7C.9.,.i
0x0020  5018 1fe0 6a0c 0000 4357 4420 2f62 696e      P...j...CWD./bin
0x0030  0d0a                                         ..
06:27:57.025924 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 601:630(29) ack 121 win
5840 (DF)
0x0000  4500 0045 0cf0 4000 4006 ea29 d151 ea8b      E..E..@.@..).Q..
0x0010  ca88 bd33 0015 0dc3 a92c bd69 3743 0943      ...3.....,.i7C.C
0x0020  5018 16d0 c2ec 0000 3235 3020 4357 4420      P.......250.CWD.
0x0030  636f 6d6d 616e 6420 7375 6363 6573 7366      command.successf
0x0040  756c 2e0d 0a                                 ul...
06:27:57.338221 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 121:127(6) ack 630 win
8131 (DF)
0x0000  4500 002e b965 4000 7106 0ccb ca88 bd33      E....e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0943 a92c bd86      .Q......7C.C.,..
0x0020  5018 1fc3 e6b6 0000 5041 5356 0d0a           P.......PASV..
06:27:57.341398 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 630:682(52) ack 127 win
5840 (DF)
0x0000  4500 005c 0cf1 4000 4006 ea11 d151 ea8b      E..\..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bd86 3743 0949      ...3.....,..7C.I
0x0020  5018 16d0 db64 0000 3232 3720 456e 7465      P....d..227.Ente
0x0030  7269 6e67 2050 6173 7369 7665 204d 6f64      ring.Passive.Mod
0x0040  6520 2832 3039 2c38 312c 3233 342c 3133      e.(209,81,234,13
0x0050  392c 3230 312c 3139 3829 0d0a                9,201,198)..
06:27:57.815719 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: . ack 682 win 8079 (DF)
0x0000  4500 0028 c365 4000 7106 02d1 ca88 bd33      E..(.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0949 a92c bdba      .Q......7C.I.,..
0x0020  5010 1f8f 9760 0000 0204 05b4 0d0a           P....`........
06:27:58.048129 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 127:135(8) ack 682 win
8079 (DF)
0x0000  4500 0030 cb65 4000 7106 fac8 ca88 bd33      E..0.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0949 a92c bdba      .Q......7C.I.,..
0x0020  5018 1f8f c55e 0000 5459 5045 2049 0d0a      P....^..TYPE.I..
06:27:58.048346 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 682:702(20) ack 135 win
5840 (DF)
0x0000  4500 003c 0cf2 4000 4006 ea30 d151 ea8b      E..<..@.@..0.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bdba 3743 0951      ...3.....,..7C.Q
0x0020  5018 16d0 0d18 0000 3230 3020 5479 7065      P.......200.Type
0x0030  2073 6574 2074 6f20 492e 0d0a                .set.to.I...
06:27:58.359394 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 135:148(13) ack 702 win
8059 (DF)
0x0000  4500 0035 d365 4000 7106 f2c3 ca88 bd33      E..5.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0951 a92c bdce      .Q......7C.Q.,..
0x0020  5018 1f7b 4a00 0000 414c 4c4f 2031 3034      P..{J...ALLO.104
0x0030  3135 340d 0a                                 154..
06:27:58.359584 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 702:729(27) ack 148 win
5840 (DF)
0x0000  4500 0043 0cf3 4000 4006 ea28 d151 ea8b      E..C..@.@..(.Q..
0x0010  ca88 bd33 0015 0dc3 a92c bdce 3743 095e      ...3.....,..7C.^
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0020  5018 16d0 ad95 0000 3230 3220 414c 4c4f       P.......202.ALLO
0x0030  2063 6f6d 6d61 6e64 2069 676e 6f72 6564       .command.ignored
0x0040  2e0d 0a                                       ...
06:27:58.682417 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 148:156(8) ack 729 win
8032 (DF)
0x0000  4500 0030 dd65 4000 7106 e8c8 ca88 bd33       E..0.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 095e a92c bde9       .Q......7C.^.,..
0x0020  5018 1f60 c467 0000 5245 5354 2030 0d0a       P..`.g..REST.0..
06:27:58.682614 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 729:796(67) ack 156 win
5840 (DF)
0x0000  4500 006b 0cf4 4000 4006 e9ff d151 ea8b       E..k..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c bde9 3743 0966       ...3.....,..7C.f
0x0020  5018 16d0 c4dd 0000 3335 3020 5265 7374       P.......350.Rest
0x0030  6172 7469 6e67 2061 7420 302e 2053 656e       arting.at.0..Sen
0x0040  6420 5354 4f52 4520 6f72 2052 4554 5249       d.STORE.or.RETRI
0x0050  4556 4520 746f 2069 6e69 7469 6174 6520       EVE.to.initiate.
0x0060  7472 616e 7366 6572 2e0d 0a                   transfer...
06:27:59.012639 IP 202.136.189.51.3523 > xxx.yyy.zzz.139.21: P 156:170(14) ack 796 win
7965 (DF)
0x0000  4500 0036 e965 4000 7106 dcc2 ca88 bd33       E..6.e@.q......3
0x0010  d151 ea8b 0dc3 0015 3743 0966 a92c be2c       .Q......7C.f.,.,
0x0020  5018 1f1d 30b1 0000 5354 4f52 2031 3031       P...0...STOR.101
0x0030  2e35 3834 0d0a                                .584..
06:27:59.013631 IP xxx.yyy.zzz.139.21 > 202.136.189.51.3523: P 796:848(52) ack 170 win
5840 (DF)
0x0000  4500 005c 0cf5 4000 4006 ea0d d151 ea8b       E..\..@.@....Q..
0x0010  ca88 bd33 0015 0dc3 a92c be2c 3743 0974       ...3.....,.,7C.t
0x0020  5018 16d0 7369 0000 3535 3320 3130 312e       P...si..553.101.
0x0030  3538 343a 2050 6572 6d69 7373 696f 6e20       584:.Permission.
0x0040  6465 6e69 6564 206f 6e20 7365 7276 6572       denied.on.server
0x0050  2e20 2855 706c 6f61 6429 0d0a                 ..(Upload)..
```

That's some pretty scary traffic to see directed at you FTP server! The tool was likely trying to upload some sort of attack tool to the various subdirectory of my Linux server, including /bin!! Luckily, the server's permissions are set to deny uploads via FTP, or things could have turned out very much for the worse.

Correlations -

On February 4th (less than 2 months ago, as I write this), an individual named "Hoof Hearted" capbligh2001@hotmail.com reported observing the following traffic directed at his or her FTP logs in the discussion forum at:
http://cert.uni-stuttgart.de/archive/incidents/2003/02/msg00027.html:

[1] Tue 04Feb03 10:16:03 - Starting FTP Server... (Version 2.5f (32-bit))
[5] Tue 04Feb03 10:21:20 - (000001) Connected to 203.198.145.93 (Local address 192.168.1.9)
[6] Tue 04Feb03 10:21:20 - (000001) 220 Serv-U FTP-Server v2.5f for WinSock ready...
[5] Tue 04Feb03 10:21:20 - (000001) IP-Name: MAIL.HYPRINT.COM
[2] Tue 04Feb03 10:21:21 - (000001) USER **anonymous**
[6] Tue 04Feb03 10:21:21 - (000001) 331 User name okay, please send complete E-mail address as password.
[2] Tue 04Feb03 10:21:21 - (000001) PASS **ano@ano.com**
[5] Tue 04Feb03 10:21:21 - (000001) ANONYMOUS logged in, password: ANO@ANO.COM
[6] Tue 04Feb03 10:21:21 - (000001) 230 User logged in, proceed.
[2] Tue 04Feb03 10:21:22 - (000001) **TYPE I**
[6] Tue 04Feb03 10:21:22 - (000001) 200 Type set to I.
[2] Tue 04Feb03 10:21:22 - (000001) **STRU F**
[6] Tue 04Feb03 10:21:22 - (000001) 200 STRU F ok.
[2] Tue 04Feb03 10:21:22 - (000001) **MODE S**

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[6] Tue 04Feb03 10:21:22 - (000001) 200 MODE S ok.
[2] Tue 04Feb03 10:21:23 - (000001) **REST 0**
[6] Tue 04Feb03 10:21:23 - (000001) 350 Restarting at 0 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:23 - (000001) **REST 1**
[6] Tue 04Feb03 10:21:23 - (000001) 350 Restarting at 1 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:24 - (000001) **REST 0**
[6] Tue 04Feb03 10:21:24 - (000001) 350 Restarting at 0 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:24 - (000001) **SYST**
[6] Tue 04Feb03 10:21:24 - (000001) 215 UNIX Type: L8
[2] Tue 04Feb03 10:21:25 - (000001) **PASV**
[6] Tue 04Feb03 10:21:25 - (000001) 227 Entering Passive Mode (192,168,1,9,4,14)
[5] Tue 04Feb03 10:22:06 - (000001) Closing connection for user ANONYMOUS (00:00:46 connected)

Note that commands and the order in which they are executed are **identical** to those recorded by my tcdump capture file. I believe that this FTP log was created by the same attack tool that produced the trace routes on my network.

Also, note that both of the attacking hosts (mine and the one "Hoof Hearted" observed) are registered IP addresses of mail servers located in southeast Asia (Singapore in my case, Hong Kong in Hoof Hearted's).

Hoof-hearted did receive one reply - (located at http://www.fiberstarr.com/pipermail/incidents_fiberstarr.com/2003-February/000381.html) to his query about this traffic, stating that it was likely just normal authorized FTP access. In light of the activities I have documented here, I find this assertion very difficult to believe. The chances of these exact commands being repeated in exactly the same sequence are neglibible. Also, note the timestamps in these logs; these commands are executed with **just a few tenths of a second** separating them. This is decidedly an automated tool, and **not** a human being manually typing these commands. In addition, we have seen ample evidence of this automated tool's true motives from the above analysis of the myriad attempted web exploits it generates.

Evidence of Active Targeting -

There is absolutely no evidence of active targeting here. If anything, there is overwhelming evidence that the attacker merely enters a range of IP addresses that he would like to investigate and/or compromise, and the tool just blindly does his or her bidding. Every IP address in my network was probed, regardless of whether there was a live host there or not, and regardless of operating system, function, or publicly available information.

Severity -

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

Criticality: importance of the targeted system. These servers on my DMZ subnet provide email, file storage, and limited web services to me and a community of hobbyists. While no highly sensitive data is stored on any of them, it would be a significant inconvenience if they were to go down . I will assign a rating of **3** here.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Lethality: how severe is the damage if the attack succeeds? Had this automated attack tool been successful, it could have resulted in remote compromise of several servers on my DMZ. Also, these servers would likely then be utilized as attack hosts to launch malicious attacks against other networks, the damage from which I could conceivably be held liable for in a court of law. Therefore, I will assign a worst-case rating of **5** here.

System Countermeasures: Patches and hot-fixes are in very good shape, and all but one unnecessary service was turned off. Unfortunately, it was *that one service* (FTP, with anonymous access allowed) than very nearly enabled the attack tool to anonymously upload malware to my Linux server. I will assign a **2** here.

Network Countermeasures: Port 80 is wide open at the firewall by necessity (these are publicly-accessible web servers, after all). All IP addresses appear to be allowed access, regardless of geographic location. An IDS is obviously in place, or we would not be analyzing this detect in the first place. I will assign a rating of **2** here.

Severity = (3 + 5) – (2 + 2) = 4

Defensive Recommendations -

With regards to the anonymous FTP server, *mea culpa*!! I do not generally run FTP anywhere on my network at all, and had "temporarily" enabled it just a few hours prior to this attack, to facilitate the transfer of the large packet sniffer capture files between systems. Regardless, the anonymous feature should have been disabled, and I should have set the FTP parameters to allow only one simultaneous logon, and then stopped the server the instant I was done transferring the files. This is yet another example of how easily and quickly an automated tool or worm can potentially compromise a vulnerable Internet-facing system! Luckily in this case, other system countermeasures prevented the attack from succeeding, but this was definitely a close call.

On the web-servers, system countermeasures were adequate to thwart this attack, but this certainly reinforces the absolute necessity for keeping up on all the latest service packs and patches!

On the network side, as a direct result of this attack, I have decided to disallow all incoming ICMP echo requests, even those directed to my DMZ subnet. Had my DMZ hosts not responded to the initial ping requests, the automated tool would have totally skipped my IP address entirely. In that case, my hosts, packet sniffer and Snort IDS would not have even noticed anything amiss. Of course, it could well be argued that it is probably a good idea to know when someone is attacking you, whether they have any chance of success or not. If I want to know about these sorts of attacks in the future, I will need to deploy some IDS technology outside the DMZ's external firewall.

I am also considering implementing a block list on my border router that will drop all traffic from well-documented hostile IP addresses and subnets.

Multiple Choice Question –

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

What is the most plausible explanation for this log file?

```
[6] Tue 04Feb03 10:21:20 - (000001) 220 Serv-U FTP-Server v2.5f for WinSock ready...
[5] Tue 04Feb03 10:21:20 - (000001) IP-Name: MAIL.HYPRINT.COM
[2] Tue 04Feb03 10:21:21 - (000001) USER anonymous
[6] Tue 04Feb03 10:21:21 - (000001) 331 User name okay, please send complete E-mail address as password.
[2] Tue 04Feb03 10:21:21 - (000001) PASS ano@ano.com
[5] Tue 04Feb03 10:21:21 - (000001) ANONYMOUS logged in, password: ANO@ANO.COM
[6] Tue 04Feb03 10:21:21 - (000001) 230 User logged in, proceed.
[2] Tue 04Feb03 10:21:22 - (000001) TYPE I
[6] Tue 04Feb03 10:21:22 - (000001) 200 Type set to I.
[2] Tue 04Feb03 10:21:22 - (000001) STRU F
[6] Tue 04Feb03 10:21:22 - (000001) 200 STRU F ok.
[2] Tue 04Feb03 10:21:22 - (000001) MODE S
[6] Tue 04Feb03 10:21:22 - (000001) 200 MODE S ok.
[2] Tue 04Feb03 10:21:23 - (000001) REST 0
[6] Tue 04Feb03 10:21:23 - (000001) 350 Restarting at 0 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:23 - (000001) REST 1
[6] Tue 04Feb03 10:21:23 - (000001) 350 Restarting at 1 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:24 - (000001) REST 0
[6] Tue 04Feb03 10:21:24 - (000001) 350 Restarting at 0 - send STORE or RETRIEVE to initiate transfer.
[2] Tue 04Feb03 10:21:24 - (000001) SYST
[6] Tue 04Feb03 10:21:24 - (000001) 215 UNIX Type: L8
[2] Tue 04Feb03 10:21:25 - (000001) PASV
[6] Tue 04Feb03 10:21:25 - (000001) 227 Entering Passive Mode (192,168,1,9,4,14)
[5] Tue 04Feb03 10:22:06 - (000001) Closing connection for user ANONYMOUS (00:00:46 connected)
```

a) this is normal anonymous FTP usage by an authorized end-user.
b) this is an attempt to compromise an FTP server via the notorious buffer overflow in older verions of Wu-FTP.
c) this is an automated script running against an anonymous FTP server.
d) The use of the string "ANO@ANO.COM" proves this is Warezer activity, as Warezers frequently use that string as their anonymous FTP password.

Correct answer:
C – If you look at the extremely short time elapsed between the commands being sent, it should be clear that these commands could only have been generated by an automated tool of some kind.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 3:
Analyze This!

Executive Summary –

After some deliberation, I've come to the conclusion that the University is confronted with three major issues with regard to its Intrusion Detection efforts:

1) There is far too much "noise" being generated by the IDS system. The majority of the alerts being generated appear to due to benign traffic, mis-configured hosts or IDS rules, and some customized alerts that do not appear to serve any useful function. This has the deleterious effect of swamping both the IDS sensors and the Analyst's bandwidth.

2) The use of peer-to-peer networks such as Gnutella, Morpheus, and Kazaa is obviously quite widespread at the University. Rampant uncontrolled use of P2P networks is becoming much more controversial and potentially costly, as the Recording Industry Association of America has recently begun mounting major legal challenged to educational institutions which turn a blind eye to the resulting inevitable theft of copyrighted material. This uncontrolled file-sharing also constitutes a serious abuse of the University's Internet capacity, which is quite likely to be interfering with much more legitimate bandwidth demands.

3) There are indications that several University systems may have been compromised by worms and/or external attackers. These should be examined immediately for any signs of potential compromise by the University's InfoSec personnel.

Recommendation:
I recommend that the University embark upon the following lock-down strategy, post-haste:

1) Fine tune the IDS to ignore traffic that is generally benign, e.g. internal SMB/Netbios Wildcards, Unicode traffic directed at well known and legitimate webservers in Southeast Asia, etc.
2) Block all outbound **unsolicited** HTTP traffic on the standard web server ports (tcp 80, 433, 8080, etc). This will stop the University from infecting any external systems, and thereby hopefully limit any potential legal liabilities. This will **not** prevent the University's legitimate webservers from doing their job, as any legitimate traffic from them will be a response to already established incoming requests.
3) Clarify the University's policy forbidding the trafficking in copyrighted materials via P2P protocols on the University's data networks. Set a start date for the policy, this will be the date that the main P2P protocols are blocked at the border routers and/or firewalls.
4) Seek out all internally compromised systems and rebuild them (see section entitled "Possibly Compromised Hosts).

The immediate execution of these 4 steps will greatly enhance the security of the University's data networks. Also, a great deal of legal liability can potentially be avoided, especially in light of the RIAA's recent aggressive legal posture regarding P2P file-sharing of copyrighted material.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Scope of the Investigation –

The University provided me with the following data files:

Snort Alert files from 3/27/03 through 3/31/03, in "fast alert" format and gzipped:

```
alert.030327.gz
alert.030328.gz
alert.030329.gz
alert.030330.gz
alert.030331.gz
```

Snort Scan files from the same time period:

```
scans.030327.gz
scans.030328.gz
scans.030329.gz
scans.030330.gz
scans.030331.gz
```

Snort "OOS" Out Of Spec Reports from the same time period:

```
OOS_Report_2003_03_27_23034
OOS_Report_2003_03_28_5271
OOS_Report_2003_03_29_20502
OOS_Report_2003_03_30_15595
OOS_Report_2003_03_31_15057
```

Unfortunately, no other data was available, so I did not have the opportunity to corroborate my finding with full packet capture files, application or firewall logs, etc. The University should endeavor to corroborate these findings with the relevant system log files at the earliest opportunity.

"Top Talkers" -

In this section, I focus on the hosts (both internal and external) that generated the largest number of Snort alerts. These are the so called "Top Talkers" of this particular data set. By this, I mean they are the most frequently occurring source IP addresses in the population of Snort alerts.

Top 10 internal and external source IP addresses:

	Internal Source IP Address	# of Alerts	External Source IP Address	# of Alerts	DNS Name
1	MY.NET.105.204	6561	68.49.35.0	16151	bgp01534079bgs.gambrl01.md.comcast.net
2	MY.NET.222.194	6100	61.56.247.174	8924	adsl-61-56-247-174.KHON.sparqnet.net
3	MY.NET.201.58	4408	212.179.48.177	5808	fw.cloverleafcomm.com
4	MY.NET.240.78	3425	63.148.150.226	5589	fomp.com
5	MY.NET.222.174	2298	194.87.6.230	5405	230.6.87.194.dynamic.dol.ru
6	MY.NET.242.250	2085	66.95.149.154	4510	66-95-149-154.generic.nas-inter.net
7	MY.NET.152.157	1629	128.8.10.18	3610	grapevine.wam.umd.edu
8	MY.NET.75.144	1038	212.179.43.225	3333	bzq-179-43-225.cust.bezeqint.net

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

9	MY.NET.223.114	850	212.179.14.14	3204	cablep-179-14-14.cablep.bezeqint.net
10	MY.NET.220.214	506	66.42.68.210	3191	66-42-68-210.stkn.mdsg-pacwest.com

The vast majority of the traffic generated by the "top talkers" can be classified into just a few distinct categories. By far the most common of these is Peer to Peer (P2P) file sharing activity, using such programs as Kazaa, Morpheus, eDonkey, etc. While not overtly malicious, this traffic should be of significant concern to The University. The RIAA has recently stepped up legal pursuits institutions that allow unauthorized exchange of copyrighted materials via P2P networks. These P2P software programs are also well-known vehicles for the dissemination of viruses and trojan horse programs.

Another major category of traffic observed from the "top talkers" is the frequent use of streaming media programs such as MS Media Player, Real Player, QuickTime, etc. While much of this traffic may be legitimate University traffic (video learning, online teleconferencing, etc), there is a strong probability that students are using such programs to stream on-line radio and video across the Internet. This is primarily a bandwidth utilization issue, and it is up to The University to clearly define its Acceptable Use Policy regarding such activities.

A third major category of traffic frequently seen passing between the "top talkers" is Internet Relay Chat traffic on tcp ports 6666-6667. Again, while this is not necessarily malicious in and of itself, there is significant evidence that several hosts inside The University are being used as "XDCC Bots" (see section on Compromised Hosts below), and may well be illegally serving up copyrighted materials, and making their presence known via IRC communications channels.

Most Commonly Occurring Alerts -

The following are the most frequently occurring alerts generated by the University's IDS system. I have listed only the top 25 most common here. It should not be inferred that the most common alerts are the ones that deserve the most attention; that is decidedly not the case. I present this table only to give a general sense of the overall status and operation of the University's IDS.

Table 1 –
Most Common Alerts Reported by the University's IDS
(3/27/03 – 3/31/03)

Frequency	Snort Alert Description
406011	SMB Name Wildcard
65882	TCP SRC and DST outside network
45660	CS WEBSERVER - external web traffic
30109	Watchlist 000220 IL-ISDNNET-990517
22221	High port 65535 udp - possible Red Worm - traffic
20342	MY.NET.30.3 activity
15861	spp_http_decode: IIS Unicode attack detected
14801	External RPC call
11978	Russia Dynamo - SANS Flash 28-jul-00
8128	SUNRPC highport access!
6057	MY.NET.30.4 activity

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
5495      TFTP - Internal TCP connection to external tftp server
4939      Watchlist 000222 NET-NCFC
4829      High port 65535 tcp - possible Red Worm - traffic
4384      Tiny Fragments - Possible Hostile Activity
3944      Queso fingerprint
3413      spp_http_decode: CGI Null Byte attack detected
1367      CS WEBSERVER - external ftp traffic
1303      IDS552/web-iis_IIS ISAPI Overflow ida nosize
```

"SMB Name Wildcard" -
The SMB Name Wildcard alert is caused by the normal behavior of Windows networking clients and server doing their routine WINS name resolutions that they do so frequently. Numerous GCIA analysts (most recently and notably Todd Beardsley & Les Gordon) have noted that these alerts are generally benign if caused by internal traffic, which the vast majority of these are.

Provided that all port 135-139 traffic is adequately blocked at all perimeter devices (both tcp and udp!), this alert should be deactivated to save wear and tear on the IDS and its analysts. Alternatively, in the very unusual event that some Netbios traffic is allowed to cross the network perimeter, this rule can be modified to fire **only** upon Netbios Wildcard traffic that crosses the network perimeter boundary.

Customized Watch Lists -
Several of these are alert signatures have been pre-defined in the IDS to watch for traffic to or from certain hosts. These are:

```
CS WEBSERVER - external web traffic
CS WEBSERVER - external ftp traffic
Watchlist 000220 IL-ISDNNET-990517
Watchlist 000222 NET-NCFC
MY.NET.30.3 activity
MY.NET.30.4 activity
Russia Dynamo - SANS Flash 28-jul-00
```

These hosts are generating a tremendous number of alerts (by definition, *any* traffic directed to or from these watchlists will generate an alert". Also, the majortiy of the Much of the traffic being generated by these hosts is Peer to Peer file sharing and streaming media traffic. It appears that these hosts are generating very large quantities of IDS alerts, with very little real malicious activity behind them.

I would recommend dispensing with the watchlists, and focus on identifying attacks via the effective use of an up-to-date Snort database. If there are certain subnets or regions the University does not need to exchange traffic with, a more effective strategy may be to block all traffic to our from those subnets altogether at the firewall or border router.

Possibly Compromised Hosts –
Even from the limited data available in files provided, there is significant evidence that several hosts on the University's internal network have been compromised by worms and/or external

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

attackers. We see a significant number of attack attempts originating on the internal network and directed at hosts on the Internet. Also, there are significant indications that some of these same systems are being utilized as attack hosts to perform scanning against other external networks.

I will now examine the hosts showing the most significant evidence of prior compromise:

"XDCC Bots" –
130.85.151.107
130.85.237.6
130.85.80.209
130.85.253.42
130.85.195.5
130.85.150.179
130.85.203.234
130.85.87.87
130.85.234.54
130.85.227.202
130.85.122.106
130.85.86.33
All of these hosts were responsible for the generation of at least one "IRC evil - running XDCC" alert. An XDCC "bot" is an automated process running on a compromised system that is generally used to make pirated movies, MP3s and other copyrighted material available for download via Internet Relay Chat (IRC channels). Recently, American universities have become a prime target for these "bots," because they tend to have extremely fast Internet connections, coupled with relatively lenient network perimeter defenses. This has prompted the Recording Industry Association of America to go on a major legal offensive against some of the leading offenders. This could potentially become an area of significant legal liability for the University.

These alerts are very unlikely to be false positives, as the alert is keyed of a very specific text string in the payload of the packet. Also, manual verification of the destination IP addresses has confirmed them to be IRC servers well-known for the hosting of XDCC bot activity (see "Significant External Hosts" section for details).

Possible Adore "Red Worm" & use as a scanning/attack host -
130.85.240.78
```
High port 65535 tcp - possible Red Worm - traffic
TFTP - External TCP connection to internal tftp server
```

This host has been the source of an extremely large number of Snort "Tiny Fragment" alerts. These types of alerts are frequently caused maliciously crafted tcp fragments fabricated for the express purpose of evading firewalls and IDS systems. This host should be examined for signs of possible compromise, it is possible that it has been taken over and is being used as an "attack host".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Significant External Hosts:

Several external hosts warrant more detailed scrutiny. These include the master controllers of compromised systems on the University Network, the IRC servers that control the XDCC "bots," and a few other external hosts which consume a relatively large fraction of the University's network bandwidth.

Evil IRC Server #1 at 65.57.64.224 –

This IRC server is responsible for a great deal of abuse. It is the control center for several of the XDCC bot parasites that are infesting the University's network. Why Dshield has not yet seen fit to send a "fightback" notice to Level3 Communications is beyond me! Here is the detailed result of a query on this IP address at www.Dshield.org. Note there are over 72,000 prior attacks logged against 21 unique targets!

```
IP Address: 65.57.64.224
HostName: irc-4.aniverse.com
DShield Profile: Country:
Contact E-mail:
Total Records against IP:  72707
Number of targets:  21
Date Range: 2003-01-11 to 2003-03-29
Ports Attacked:
Port  Attacks     Start       End
23    3598        2003-03-05  2003-03-31
1080  3544        2003-03-05  2003-03-31
6588  3519        2003-03-05  2003-03-31
8080  3513        2003-03-05  2003-03-31
81    3489        2003-03-05  2003-03-30
8000  3488        2003-03-05  2003-03-30
8001  3483        2003-03-05  2003-03-30
8081  3459        2003-03-05  2003-03-30
3128  1774        2003-03-05  2003-03-31
8520  1758        2003-03-05  2003-03-30
OrgName:    Level 3 Communications, Inc.
OrgID:      LVLT
Address:    1025 Eldorado Blvd.
City:       Broomfield
StateProv:  CO
PostalCode: 80021
Country:    US
NetRange:   65.56.0.0 - 65.59.255.255
CIDR:       65.56.0.0/14
NetName:    LC-ORG-ARIN-BLK2
NetHandle:  NET-65-56-0-0-1
Parent:     NET-65-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.LEVEL3.NET
NameServer: NS2.LEVEL3.NET
RegDate:    2001-09-21
Updated:    2002-08-08
TechPhone:  +1-877-453-8353
TechEmail:  ipaddressing@level3.com
OrgAbuseHandle: APL8-ARIN
OrgAbuseName:   Abuse POC LVLT
OrgAbusePhone:  +1-877-453-8353
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
OrgAbuseEmail:  abuse@level3.com
```

Evil IRC Server #2 at 205.188.149.12 –

This IRC Server at AOL.com is also controlling some of the XDCC bot activity at the University:

```
IP Address: 205.188.149.12
HostName: undernet.irc.aol.com
DShield Profile: Country: US
Contact E-mail: TOSUsenet@aol.com
Total Records against IP:  1197
Number of targets:  319
Date Range: 2003-01-12 to 2003-03-27
Ports Attacked (up to 10):
Port        Attacks     Start       End
2793        388         2003-03-21  2003-03-28
3476        116         2003-03-20  2003-03-22
113         83          2003-03-07  2003-04-02
1693        75          2003-03-24  2003-03-31
4266        61          2003-03-18  2003-03-19
1352        27          2003-03-19  2003-03-19
1722        27          2003-03-30  2003-03-31
2433        22          2003-03-09  2003-03-09
1281        18          2003-03-28  2003-03-29
2839        16          2003-03-17  2003-03-18
Fightback:  not sent
OrgName:    America Online, Inc
OrgID:      AMERIC-59
Address:    22080 Pacific Blvd
City:       Sterling
StateProv:  VA
PostalCode: 20166
Country:    US
NetRange:   205.188.0.0 - 205.188.255.255
CIDR:       205.188.0.0/16
NetName:    AOL-DTC
NetHandle:  NET-205-188-0-0-1
Parent:     NET-205-0-0-0-0
NetType:    Direct Assignment
NameServer: DNS-01.NS.AOL.COM
NameServer: DNS-02.NS.AOL.COM
RegDate:    1998-04-18
Updated:    1998-04-27
TechHandle: AOL-NOC-ARIN
TechName:   America Online, Inc.
TechPhone:  +1-703-265-4670
TechEmail:  domains@aol.net
```

Evil IRC Server #3 at 193.163.220.3 –

Yet another known “evil” IRC server controlling some of the XDCC bot traffic, this one is in Denmark:

```
IP Address: 193.163.220.3
HostName: irc.inet.tele.dk
DShield Profile: Country:
Contact E-mail:
Total Records against IP:  21
Number of targets:  5
```

© SANS Institute 2003, Author retains full rights.

```
Date Range: 2003-01-16 to 2003-02-26
Ports Attacked (up to 10):
Port   Attacks      Start        End
113    40           2003-03-11   2003-03-31
1433   7            2003-03-17   2003-03-21
Fightback:  not sent
inetnum:      193.163.220.0 - 193.163.220.7
netname:      JAN-CHRILLESEN-NET
descr:        IRC services
country:      DK
admin-c:      JC301-RIPE
tech-c:       JC301-RIPE
status:       ASSIGNED PI
mnt-by:       TDINET-MNT
remarks:      -------------------------------------
remarks:      For abuse and security issues contact
remarks:      abuse@eris.dk
remarks:      -------------------------------------
changed:      jan@chrillesen.dk 20030204
source:       RIPE
route:        193.163.220.0/24
descr:        Jan Chrillesen
origin:       AS3292
mnt-by:       AS3292-MNT
changed:      auto-ripe@ip.tele.dk 20000629
changed:      auto-ripe@ip.tele.dk 20010311
changed:      auto-ripe@ip.tele.dk 20020730
address:      Hougaardsvej 48, 2.th
address:      DK-8220 Brabrand
address:      Denmark
phone:        +45 87 47 00 01
fax-no:       +45 87 47 00 02
nic-hdl:      JC301-RIPE
changed:      hostmaster@DK.net 19970212
```

FastSearch Web Bot Server at 66.77.73.144 -

This is the exact same Web Bot activity that I analyzed in Assignment 2, section 2 of this document. Here, it is doing a content update of the University's Internet-facing web server at IP address 130.85.100.165.

```
IP Address: 66.77.73.144
HostName: cr005r01.sac2.fastsearch.net
DShield Profile: Country: US
Contact E-mail: ip-admin@qis.qwest.net
Total Records against IP:  23
Number of targets:  3
Date Range: 2003-01-14 to 2003-02-03
Ports Attacked (up to 10):
Port  Attacks     Start       End
80    35          2003-03-10  2003-03-26
 CustName:   Fast Search, Inc.
Address:    93 Worcester Street, 4th Floor
City:       Wellesley
StateProv:  MA
PostalCode: 02481
Country:    US
RegDate:    2002-01-10
Updated:    2002-01-10
NetRange:   66.77.73.0 - 66.77.73.255
CIDR:       66.77.73.0/24
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
NetName:    QWEST-MCC-FASTSRCH3
NetHandle:  NET-66-77-73-0-1
Parent:     NET-66-77-0-0-1
NetType:    Reassigned
RegDate:    2002-01-10
Updated:    2002-01-10
```

Notable False Positives:

130.85.106.92
130.85.106.108
130.85.104.117
130.85.152.45

I've grouped these four hosts together because they all show a very similar set of symptoms. All of them are sending out large amounts of "IIS Unicode attack" traffic. Virtually all of this traffic is directed at one specific host (*210.219.197.11*) in South Korea. Here is the IP registration information for this hosts network. There are no prior complaints against this address in Dshield:

```
IP Address          : 210.219.197.0-210.219.197.127
Connect ISP Name    : ELIMNET
Connect Date        : 19990510
Registration Date   : 20001004
Network Name        : DONGA-LACADEMY
[ Admin Contact Information]
Name                : HONGSOON CHOI
State               : SEOUL
Address             : #601 SEOJIN PLAZA, 403-1 SANG1 DONG, WONMI GU, PUCHEN SI
Zip Code            : 420-031
Phone               : +82-32-666-3301
E-Mail              : domain@elim.net
```

The "IIS Unicode" attack is frequently associated with the Nimda worm, which relies heavily on the Unicode decoding flaw in the IIS web-server (as well as several other IIS vulnerabilities) to do its dirty work. However, after some investigation, I do NOT believe this host to be infected with the Nimda worm. With Nimda, we would expect to see other signatures being triggered, such as the "Remote CMD" execution and the "Double-Decode" alerts. While it is possible that these alerts have been suppressed in the IDS system, another factor that leads me to conclude that this is not a Nimda-infected host has to do with the target selection. Nimda will typically target several different hosts in a somewhat random manner (somewhat, in that it prefers to target subnets that are relatively "close" to the infected host in IP space). This host is not doing this at all. Rather, it appears to be limiting its attacks to a very small number of target hosts, which it is very rigorously probing repeatedly with Unicode attacks.

Numerous GCIA candidates have speculated upon the underlying cause of these Unicode alerts. Carlin Carpenter also noticed the preponderance of traffic involved sites in SE Asia, and speculated that it might have something to do with the international hacking incidents (prompted by the US Spyplane incident) which was occurring at the time. However, we now see that this Unicode traffic appears to be a permanent fixture in the University's portfolio of IDS alerts.

A more fitting explanation is presented by Les Gordon in his December 31st, 2002 practical, where he notes that these alerts are triggered whenever Snort encounters a Unicode encoded form of the period, comma, or forward/backslash characters. Unfortunately, these encodings are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

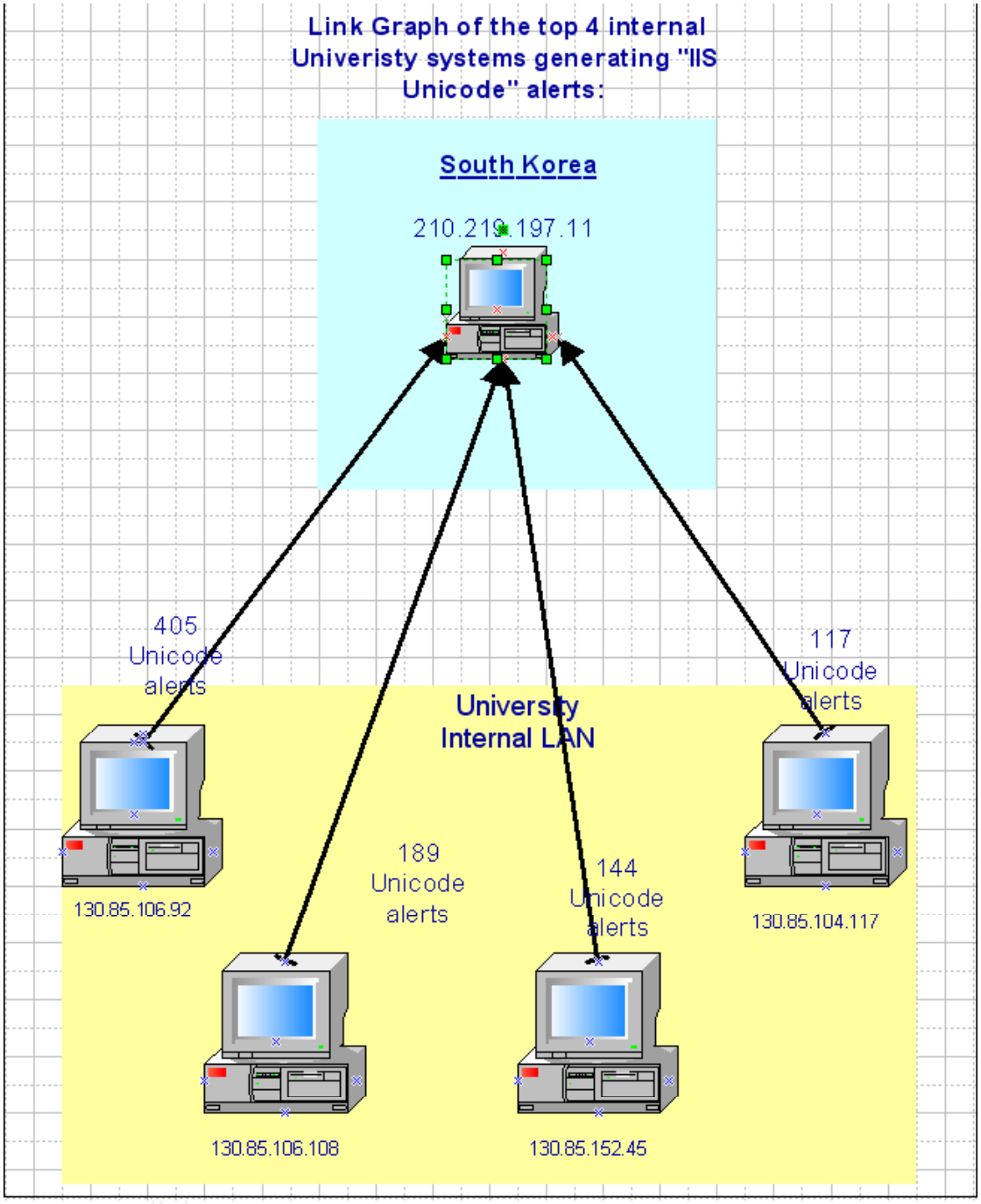
rather common in legitimate ssl-encrypted traffic, as well in normal http communications with any web-sites that use extended character sets (including Korean).

Indeed, I had already independently reached the exact same conclusion prior to reading Mr Gordon's excellent and very recently released practical. As I indicated in the first submission of this paper, I believe, quite simply, that the vast majority of these Unicode alerts are being caused by Korean-speaking students and/or faculty legitimately surfing Korean-language web-servers. Snort's unicode attack signature may well be misinterpreting the Unicode encoding of the Korean language characters as Unicode attacks. This would certainly explain why so many of these alerts are consistently directed at a very small handful of web servers in South Korea. Indeed, of the nearly "4,00 IIS-Unicode Attack" alerts generated by Snort in the 3-31-03 alerts file, 855 were generated by four client systems communicating with exactly ONE web server owned by ELIMNET in South Korea (210.219.197.11). No other alerts were detected by any of these systems, and the web-server comes up clean on Dshield.Org. The lack of any other suspicious traffic from any of these systems corroborates the theory that these this is valid web-surfing traffic setting off false-positive Unicode alerts due to the prevalence of unicode encoding in the extended character sets used to represent Korean language characters.

A link graph depicting the alert frequency of the Unicode alerts for these top four hosts should help make the argument more convincing:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



If it does indeed turn out these alerts are being generated by legitimate web surfing, the University should attempt to tighten up the firing syntax for the "Unicode Attack" Snort rule. Perhaps unicode traffic directed toward well-known bona fide Korean language webservers could be excluded from scrutiny. Alternatively, the unicode detect could be dispensed with altogether, as there is ample correlation indicating its propensity to false positives. Most unicode-based attacks possess other distinguishing signatures we can "netgrep" for, as long as these rules are in place, maybe the Unicode rule is simply not worth its false positive baggage! A rule that constantly fires on legitimate (and frequent!) traffic is worse than no rule at all, as it

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

invariably has the perverse effect of instilling complacency on the part of the University's InfoSec staff who monitor the IDS.

Scanning Activity Overview:

Nearly 3.2 million scans were detected by the University's IDS during the 5 day period from 3/27/03 through 3/31/03. The following table shows the daily breakdown of the scans that were detected. Note the overwhelming tendency for the scans to occur during the weekend hours (3/29/03 was a Saturday).

Daily Distribution of Scans Reported by the University's IDS (3/27/03 – 3/31/03)

	Number of Scans Detected	Type of Scan
1	1128025	3/29/03
2	1252924	3/30/03
3	5991	3/27/03
4	1606	3/28/03
5	896	3/31/03

The vast majority of these scans were TCP SYN and UDP scans. In general, the bulk of these scans are likely to be generated by automated port-scanning tools such as nmap.

Scan Types Reported by the University's IDS (3/27/03 – 3/31/03)

	Number of Scans Detected	Type of Scan
1	2014622	SYN scan
2	1252924	UDP scan
3	5991	FIN scan
4	1606	NULL scan
5	896	NOACK scan
6	586	VECNA scan
7	328	INVALIDACK scan
8	217	UNKNOWN scan
9	45	XMAS scan
10	29	FULLXMAS scan

The following table lists the ten most active "scanning" source IP addresses, much as our "Top Talkers" listed the hosts that generated the most Snort alerts. Note that eight of the top ten scanning source addresses are local to the University's internal network. While port-scanning is not inherently illegal, it is frequently a leading indicator that the host's owner may be enumerating potential targets for future nefarious activities. Therefore, these hosts should be scrutinized on an ongoing basis for signs of compromise and/or malicious hacking by the users who control them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Top Ten "Scanners"
(3/27/03 – 3/31/03)

	Number of Scans Detected	IP Address of Scanning Host
1	226065	130.85.97.43
2	118942	130.85.1.3
3	116768	130.85.195.155
4	59656	130.85.217.150
5	59488	130.85.235.250
6	47786	130.85.97.53
7	42993	211.58.53.253
8	36080	217.215.65.6
9	33889	130.85.228.30
10	32734	130.85.217.50

Summary –

The University is confronted with three major issues with regard to its Intrusion Detection efforts:

1) There is far too much "noise" being generated by the IDS system. The majority of the alerts being generated appear to due to benign traffic, mis-configured hosts or IDS rules, as well as some customized alerts that do not appear to serve any useful function. This has the deleterious effect of swamping both the IDS sensors and the Analyst's bandwidth.

2) The use of peer-to-peer networks such as Gnutella, Morpheus, and Kazaa is obviously quite widespread at the University. Rampant uncontrolled use of P2P networks is becoming much more controversial and potentially costly, as the Recording Industry Association of America has recently begun mounting major legal challenged to educational institutions which turn a blind eye to the resulting inevitable theft of copyrighted material. This uncontrolled file-sharing also constitutes a serious abuse of the University's Internet capacity, which is quite likely to be interfering with much more legitimate bandwidth demands.

3) There are indications that several University systems may have been compromised by worms and/or external attackers. These should be examined immediately for any signs of potential compromise by the University's InfoSec personnel.

Defensive Recommendations:
I recommend that the University embark upon the following lock-down strategy, post-haste:

5) Fine tune the IDS to ignore traffic that is generally benign, e.g. internal SMB/Netbios Wildcards, Unicode traffic directed at well known and legitimate webservers in Southeast Asia, etc.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

6) Block all outbound **unsolicited** HTTP traffic on the standard web server ports (tcp 80, 433, 8080, etc). This will stop the University from infecting any external systems, and thereby hopefully limit any potential legal liabilities. This will **not** prevent the University's legitimate webservers from doing their job, as any legitimate traffic from them will be a response to already established incoming requests.
7) Clarify the University's policy forbidding the trafficking in copyrighted materials via P2P protocols on the University's data networks. Set a start date for the policy, this will be the date that the main P2P protocols are blocked at the border routers and/or firewalls.
8) Seek out all internally compromised systems and rebuild them (see section entitled "Possibly Compromised Hosts).

The immediate execution of these 4 steps will greatly enhance the security of the University's data networks. Also, a great deal of legal liability can potentially be avoided, especially in light of the RIAA's recent aggressive legal posture regarding P2P file-sharing of copyrighted material.

Methodology used for Analyze This!

At first I attempted to run the SnortSnarf Perl on the entire dataset. Unfortunately, as was the case with several worthy analysts before me, I encountered difficulties with the use of non-numeric data to designate the home network Class B address "MY.NET", as well as a general lack of sufficient RAM and CPU resources to get the job down in a timely fashion. . A tip for those who follow: having massive amounts of RAM is evidently the key, otherwise your system is like end up thrashing for days.

I was, however, successful in processing a couple of individual days worth of the Alerts data with SnortSnarf, and found the tool to be incredibly useful in terms of the holistic view it provided into the relationships amongst the various hosts. I used these smaller SnortSnarf datasets to extensively to track down specific relationships between various source and destination hosts, as well as to give a general "reality check" to the results I obtained via other means (see below) .

As a fallback, I borrowed some tricks and scripts from the excellent previous practicals by Thomas Beardsley and Lorraine Weaver. Lorraine clued me in to a very simple and efficient way to concatenate all the data files together:

```
cat alert.1 > alerts
cat alert.2 >> alerts
cat alert.3 >> alerts
cat alert.4 >> alerts
cat alert.5 >> alerts
```

Which I translated into command-line Windows as:

```
Copy alert.1+alert.2+alert.3+alert.4+alert.5 alerts.all
```

This process was repeated with the Scan and the OOS files.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Once all files are concatenated (a surprisingly quick and painless process, using this method), I was able to use Thomas Beardsley excellent Perl scripts: csv.pl and summarize.pl to process and summarize the data files.

In general, my approach from this point on was identify the Top Talkers in terms of alerts and scans, then look them up in the individual day's SnortSnarf data I had processed. Once you have the alert or host of interest identified, SnortSnarf provides extremely convenient hyperlinks to relevant port information, source and destination IP addresses, Dshield lookups, etc.

References for Sections 2 & 3:

Anonymous. "WEB-IIS _vti_inf access." Mar 13, 2002. Snort Signatures Database. URL: http://www.snort.org/snort-db/sid.html?id=990

Anonymous. "WEB-FRONTPAGE _vti_rpc access." Mar 13, 2002. Snort Signatures Database. URL: http://www.snort.org/snort-db/sid.html?id=937

Beardsley, Thomas. "GCIA Practical Assignment." GIAC Certified Intrusion Analysts (GCIA). URL: http://www.giac.org/practical/Tod_Beardsley_GCIA.doc

Carpenter, Carlin, "GCIA Practical Assignment." GIAC Certified Intrusion Analysts (GCIA). URL: http://www.giac.org/practical/Carlin_Carpenter_GCIA.doc

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

Coochey, Giles. "WEB-IIS cmd.exe access." Snort Signatures Database. URL: http://www.snort.org/snort-db/sid.html?id=1002

Edward, Perry. "Many, many, many security holes in the Microsoft Frontpage extensions." Exploit World!. Apr 23, 1998. URL: http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html

FAST Seach, Inc. Description of Automated Web Indexing Bot. URL: http://www.fastsearch.net/products/websearch/index.asp

Gordon, Les, "GCIA Practical Assignment." GIAC Certified Intrusion Analysts (GCIA). URL: http://www.giac.org/practical/Les_Gordon_GCIA.doc

Internet Assigned Numbers Authority [IANA]. "Port Numbers." URL: http://www.iana.org/assignments/port-numbers

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Melvin, Capt. John, "LOGS: GIAC GCIA Version 3.2 Practical Detect", posting to Incidents.Org mailing list, Sept. 15th, 2002. URL: http://cert.uni-stuttgart.de/archive/intrusions/2002/09/msg00265.html

MITRE Corporation. CAN-2001-0906. Common Vulnerabilities and Exposures. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0906

Patrick, Andrew, "GCIA Version 3.3 Practical Detect...", posting to Incidents.Org mailing list, March 28th, 2003. URL: http://cert.uni-stuttgart.de/archive/intrusions/2003/03/msg00378.html

Roesch and Green. "Snort User's Manual Chapter 2: Writing Snort Rules." Snort User's Manual. URL: http://www.snort.org/docs/writing_rules

Jones, Andrew Rucker, "Re: GCIA Version 3.3 Practical Detect...", posting to Incidents.Org mailing list, March 29, 2003. http://cert.uni-stuttgart.de/archive/intrusions/2003/03/msg00385.html

Silicon Defense, Inc. "SnortSnarf" Perl Scripts. URL:

Sourcefire, Inc. "Snort Ports Database." URL: http://www.snort.org/ports.html

Weaver, Lorraine. "GCIA Practical Assignment." GIAC Certified Intrusion Analysts (GCIA). URL: http://www.giac.org/practical/Lorraine_Weaver_GCIA-Part3.doc

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 24th, 2017

Upcoming Training

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