# With Speed The Hacker Cometh…

Craig Valli

*School of Computer and Information Science*
*Edith Cowan University, Australia*
*Email: c.valli@ecu.edu.au*

## ABSTRACT

*This paper is an examination of six months of IDS reports and firewall logs for a small enterprise that has a new broadband ADSL connection. The paper examines the information contained in the logfiles and the implications of detected activities by would be attackers. An examination of the issues that the deployment of broadband has for home and small business users is also undertaken.*

*Keywords: broadband, intrusion detection, firewalls, home users, ADSL*

## INTRODUCTION

This paper is an examination of six months of Intrusion Detection System (IDS) reports and firewall log entries for a small enterprise that has a new broadband 1.5Mbit ADSL connection. Over 60,000 log file entries from machines within the enterprise were examined for this case study. The author used simple statistical measures to examine the information contained in the log files.

The paper examines what patterns of scanning or attacks were targeted at the machines in the enterprise. Timing of attacks on various ports or services will be checked against releases of known vulnerabilities from security vulnerability databases such as CERT and CVE. The paper then discusses the implications of the findings of the case study and looks specifically at issues for the deployment of broadband connections for the home and small business user.

## THE NETWORK LAYOUT

The IDS and firewall on the two servers in the DMZ detected and logged over 60,000 suspicious events from May 2001 to November 2001. The enterprise upgraded from an existing 128K ISDN connection to a new 1.5MB ADSL connection for the primary reason of increased bandwidth in May 2001. The other main benefit was that of cost savings in physical provision of a connection to the Internet for the enterprise down from $4400 per annum to just $700 per annum.The 2 servers were both hardened RedHat 6.2 Linux boxes that existed within a DMZ configuration. see figure 1 below

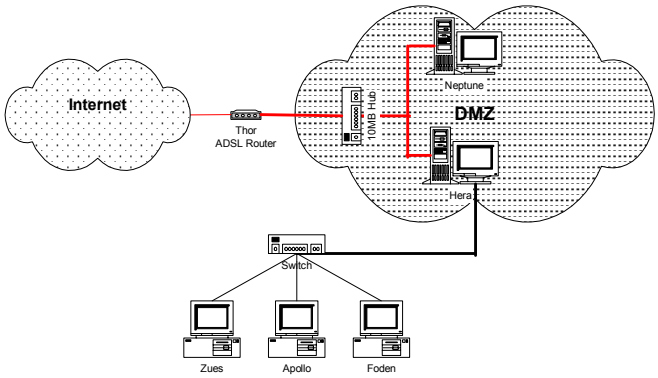


**Figure 1** – network layout

Hera is a dual homed bastion host that acts as the secondary router in the DMZ design. Both Hera and Neptune run a basic firewalling rule set that performs mandatory blocks of access from bogus or undelegated IP address ranges. In addition it denies access to all server ports other than what is meant to be open and available for access these ports are outlined in Table 1.

| **Hera** | Port 22 SSH<br>Port 25 SMTP<br>Port 53 DNS<br>Port 80 HTTP<br>Port 443 HTTPS<br>Port 995 POP3S | **Neptune** | Port 22 SSH<br>Port 53 DNS<br>Port 80 HTTP<br>Port 443 HTTPS |
|---|---|---|---|

**Table 1** – Open Ports on Servers

The primary DNS for the organization is located on Hera with Neptune providing secondary backup services. The intrusion detection system (IDS) used was Portsentry (Psionic, 2001) set with a high trigger level to lower false positives in the detection of suspicious network activity. Upon detecting suspicious activity the IDS triggered a firewall rule that then blocked all traffic from the attacking IP. Full logging via syslogd was done on both these machines and logs were secured via a script that extracted relevant information from the logfiles daily and forwarded them via e-mail to a machine (Apollo) located beyond the DMZ.

The script extracted two main forms of data that was all Portsentry IDS alerts and messages plus the entire kernel based firewall alerts and messages. These messages showed the initiation of dynamic blocking of sites that triggered the IDS. A typical firewall denial entry looks like this

> Nov 30 15:04:36 neptune kernel: Packet log: input DENY eth0 PROTO=17 ATTACK_IP:32800 NEPTUNE:53 L=60 S=0x00 I=18941 F=0x0000 T=8 (#64)

The logfiles yielded 64073 unique lines of firewall-based information, Hera generated 61565 of these and the remaining 2489 were generated by Neptune. This was obtained by concatenating the logfiles together in raw format initially. Then using a customized Perl script to extract information from these logfiles in the DSHIELD format (Consulting, 2002). This is a tab-delimited file that contains for each line

1. Date
2. Host (UserID)
3. Count (number, used to summarize identical records, default=1)
4. Source IP address (in 1.2.3.4 format)
5. Source port
6. Target IP address
7. Target port
8. Protocol
9. TCP flags – SYN, ACK, FIN, URG, RES

These extracted log entries were then imported into an Access Database and SPSS for basic statistical analysis and examination of any trends or patterns in the data set.

## ANALYSIS OF LOG FILE ENTRIES

There were 1201 unique attacking IP numbers recorded by the log files and identified by the analysis process. Of these attacking IP numbers the top 15 displayed in Table 2 below were responsible for 46095 (71.9%)of all logged attack entries to the machines in the DMZ. The top 15 attackers activities can really only be considered as brute forced automated attacks upon the systems. Upon further

analysis of the log files most of the top 15 attackers did so in the period 12th –15th August 2001 where 49320 (80.1%) of all logged attack lines were recorded. During this period Code Red (CERT/CC, 2001b) was emergent and some of these log entries for this period showed Code Red signatures. The problem was that the attack that caused this traffic was not in fact a Code Red attack but was an attempted distributed denial of service attack upon the DNS services on port 53 directed at Hera which is the primary DNS server for the network.

| | Frequency | Percent | Cumulative Percent |
|---|---|---|---|
| 01_attacker | 13376 | 20.9 | 20.9 |
| 02_attacker | 7370 | 11.5 | 32.4 |
| 03_attacker | 3855 | 6.0 | 38.4 |
| 04_attacker | 3832 | 6.0 | 44.4 |
| 05_attacker | 2562 | 4.0 | 48.4 |
| 06_attacker | 2281 | 3.6 | 51.9 |
| 07_attacker | 1771 | 2.8 | 54.7 |
| 08_attacker | 1548 | 2.4 | 57.1 |
| 09_attacker | 1545 | 2.4 | 59.5 |
| 10_attacker | 1544 | 2.4 | 61.9 |
| 11_attacker | 1476 | 2.3 | 64.2 |
| 12_attacker | 1380 | 2.2 | 66.4 |
| 13_attacker | 1199 | 1.9 | 68.3 |
| 14_attacker | 1181 | 1.8 | 70.1 |
| 15_attacker | 1171 | 1.8 | 71.9 |
| All_Others | 17978 | 28.1 | 100.0 |
| Total | 64069 | 100 | 100 |

**Table 2** – Number of Scans per top attacker

The logfiles on Hera 10th August showed attacker01 attempting what appears to have been an operating system fingerprinting scan. Then on 11th August a selective scan on ports 21, 22, 25, 53, 80, 111, 443, 520, 995, 3128, 3130, 8080 would have indicated that the attacker at least knew they were dealing with a UNIX based system. The evidence for this was that they went after port 111 (AUTH), 3128 and 3130 that are Squid Proxy default ports that are only found on UNIX/POSIX variants. To add further weight to the argument there was no scan done of the SMB and NetBIOS ports 137, 138 and 139, which an inexperienced hacker or hacker targeting Windows based machines would have attempted.

The Portsentry IDS placed blocking routes for the IP address of the attacker during the scan on port 53 effectively dropping all of their traffic to this service. Then on the 12th August an attack was directed at the Domain Name Services (DNS) daemon on Hera, which resulted in the 43116 log entries relating to attacks on the DNS services over a 74 hour period, or an average of just less than 600 probes an hour.

The controller in this case attacker01 appeared to control or compromise the systems in groups of three whether this was limitation of bandwidth or the tool that was used is unsure and cannot be determined from the evidence. The majority of the attack patterns were cycled consistently e.g. controller, host1, host2, host3, controller, host1, host2, host3, controller, ….. which further indicates an automated or script based attack in nature.

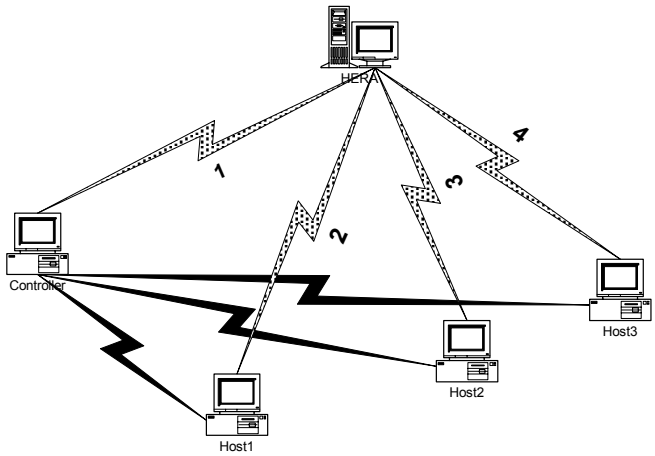


**Figure 2** – Attack trace

The time to live (TTL) between each host also varied across compromised host groupings with one group capable of a less than 1 second delay to almost 5-10second TTL delay between hosts in another group. The compromised hosts used static ports from which to commission the attacks. But the selection of port number used to attack was not consistent across the compromised attack devices. The other interesting point was that the length of packet sent also varied in each of the attack packets from a Length of 44 bytes to 324 bytes. The packet patterns indicated fragmented attacks and attempted buffer overflows by the attacker. Which due to the speed and the complexity of launching these packets manually would further indicate automation of the attacks.

The effect of the attack was that the primary domain server performance was severely compromised during this attack. The owners of the system emailed the administrator of the domain for attacker01. The administrator immediately responded and shutdown the compromised server which halted the distributed denial of service.

| Port | Protocol | Frequency | Percent | Cumulative Percent |
|---|---|---|---|---|
| **53** | DNS | 47997 | 74.91 | 74.91 |
| **80** | HTTP | 8459 | 13.20 | 88.11 |
| **25** | SMTP | 2743 | 4.28 | 92.39 |
| **520** | EFS | 1548 | 2.42 | 94.81 |
| **111** | SUNRPC | 731 | 1.14 | 95.95 |
| **21** | FTP | 334 | 0.52 | 96.47 |
| **137** | NETBIOS-NS | 74 | 0.12 | 96.59 |
| **17300** | KUANG2THEVIRUS | 33 | 0.05 | 96.64 |
| **4417** | ???? | 27 | 0.04 | 96.68 |
| **3053** | DSOM-SERVER | 20 | 0.03 | 96.71 |
| **22** | SSH | 19 | 0.03 | 96.74 |
| **443** | HTTPS | 17 | 0.03 | 96.77 |

**Table 3** - Port Scan Frequency

The high percentage of domain name service based attacks concurs with new vulnerabilities (CERT/CC, 2001a, CERT/CC, 2001d) that were found in the BIND daemon which is used to run DNS services in 2001. Many machines if unpatched were susceptible to these attacks some of which allowed for root/administrator compromise of the system as well as buffer overflow based denials of service. Some of the logged entries attempted to send large packets of over 900 bytes to the BIND servers that would have caused buffer overflow based attacks if the servers were in fact vulnerable to that particular attack.

Over 60% of all of the malicious traffic to port 80 were SYN packets sent by a wide range of attacking IP numbers. The packets were either SYN scans or maliciously formed denial of service packets. Of the remaining log file entries in the http daemons log for the corresponding timestamps the probes were against known CGI vulnerabilities and known buffer overflow exploits. The speed at which these probes took place would indicate the use of automated vulnerability scanners or they were pre-programmed by the attackers. There was a high proportion of NIMDA (CERT/CC, 2001c) based attacks in this traffic as would be expected for the latter section of the log file entries relating to the http services.

SMTP (Simple Mail Transport Protocol) was the next most highly probed service. SMTP is one of the most vulnerable services that is run on servers due to it complexity of configuration and overall size. Many of the corresponding entries again indicated activity of automated tools for the majority of traffic simply brute probing for known vulnerabilities. SUNRPC is also a highly vulnerable port on a Linux based PC.

FTP services were scanned 334 times which is interesting considering there was no services or inetd configuration for this service. The ftp binaries had in fact been removed from the system. This would indicate that many of the attackers were naïve or careless in their probing of the systems. FTP is also one of the most vulnerable services that is deployed on systems and hence automated vulnerability scanners will probe for FTP many vulnerabilities.

## IMPLICATIONS OF THE LOG FILE ANALYSIS

These are logfiles that are gathered from systems where the administrator is a competent network security professional. The problem is that many home and small business users are now adopting ADSL and other broadband technologies as replacements for conventional modems and are largely unaware of the increased security implications and are typically not computer or network security literate (Glass, 2001, Goldberg, 2000, Hoffman, 2000). Modems are typically restricted and hampered in their ability to sustain a high intensity scan due to bandwidth and technological barriers. ADSL on the other hand does not have such impediments and can see home users with a 1.5 Megabit per second connection to the Internet awaiting an attack by those with malicious intent.

This faster connection leaves the broadband user with a decreased attack detection window in which to detect and respond to probes by the attacker. Conversely, it allows the attacker to spend a smaller amount of time in a position where they may be detected scanning or probing a host. With a high bandwidth connection they are also able to scan a wider range of ports due to this increased speed. Based on the assumption that ADSL is 30-50 times faster than a conventional 56K modem this means an attack that took 5 minutes to commission previously could now take place in as little as 6-10 seconds with ADSL.

The logfiles showed patterns of attack that are consistent with the widespread use of automated attack tools and vulnerability scanners. This is consistent with data from other authors where there is an increase in scanning activity on the Internet brought about by script kiddies activity (Conry-Murray, 2001a, Conry-Murray, 2001b, Harrison, 1999). Much of this activity is often done without knowledge of the tools used or their true destructive capabilities.

Many of the attacks that were recorded in the logfiles were also perpetrated as a result of vulnerabilities becoming “known” to the wider public through release of these details on legitimate sites such as CERT or CVE. These activities would indicate again bulk scanning and probing for the new vulnerabilities by attackers with little understanding or knowledge of the attack as many vulnerability scanners will quickly incorporate any new vulnerabilities into their scanning database for use by legitimate users.

## CONCLUSION

The introduction of broadband technology has many benefits all of which can work against the user from a security perspective. This case has demonstrated that users are potentially susceptible to a wide range of attacks due to the increase in available bandwidth to their home desktops through the adoption of broadband. There are several questions that arise for instance does the ISP have an obligation to provide more secure services to broadband customers? Are the risks of successful attack raised by the installation of broadband services, which in turn provides reduced attack and detect windows? To what extent does the home user or small business have the ability to recognize or even defend against an attempted automated attack?

Many of the users of new mass marketed broadband services it could be argued would lack basic network security skills. To further exacerbate the problem experiences of cases like (Love, 2001) would indicate that software vendors are not aiding novice users in the effective deployment of personal and home use firewalls. Further research is needed in this area to identify the risk that broadband potentially raises as it becomes more ubiquitous in deployment leaving an increasingly larger collection of viable victim systems for hackers to compromise.

## REFERENCES


CERT/CC (2001a) CERT® Advisory CA-2001-02 Multiple Vulnerabilities in BIND, *http://www.cert.org/advisories/CA-2001-02.html*, August 07, 2001

CERT/CC (2001b) CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL", CERT/CC.

CERT/CC (2001c) CERT® Advisory CA-2001-26 Nimda Worm, *http://www.cert.org/advisories/CA-2001-26.html*, September 25, 2001

CERT/CC (2001d) CERT® Incident Note IN-2001-03 - Exploitation of BIND Vulnerabilities, *http://www.cert.org/advisories/CA-2001-02.html*,

Conry-Murray, A. (2001a) Network security's not-so-secret ingredients, Network Magazine, **16** (8)**,** pp 68.

Conry-Murray, A. (2001b) Swatting persistent security pests, Network Magazine, **16** (12)**,** pp 36.

Consulting, E. (2002) Guidelines for Developing DShield Client Software, *http://www.dshield.org/specs.html#dshield_format*, 27/Feb/2002 23:24

Glass, B. (2001) Got Broadband? You're Under Attack, *http://www.extremetech.com/print_article/0,3428,a=1620,00.asp*, June 12, 2001

Goldberg, A. (2000) DSL is unsafe unnecessarily, Upside, **12** (2)**,** pp 30.

Harrison, A. (1999) When good scanners go bad, Computerworld, **33**(12)**,** pp 66.

Hoffman, N. (2000) One-in-Four Broadband PCs at Hack Risk, ZDNet News.

Love, T. (2001) Designing Information Security for Small Businesses: Lessons from a Case Study, In 2nd Australian Information Warfare & Security Conference(Eds, Hutchinson, W., Burn, J. and Warren, M.) We-bCentre, Perth, Western Australia.

Psionic (2001) Portsentry, Psionic Technologies, Austin, Texas.