GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC Certified Incident Handler
Practical Assignment v3

VPN Aggressive Mode Pre-shared Key Brute Force Attack

Steve Pitts
Submitted January 29, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Statement of Purpose: 1
The Exploit Tools: 1
IkeProbe: 1
IKE-scan: 2
Cain: 2
IKEcrack: 3
The Vulnerability: 3
Advisories and references: 4
Operating Systems Affected: 4
Vendor Status Date Updated 5
Targeted protocols, Services and Applications: 6
Phase 1 7
Phase 1 Main Mode messages: 7
Aggressive Mode: 9
Phase 2 11
MD5 and SHA Hashing algorithms: 11
Variants: 11
IKE username sniffing: 11
IKE username guessing: 11
Description: 12
MAIN MODE vs Aggressive Mode: 12
Peer Authentication method: 13
Attack process: 13
Exploit Story/The setting: 14
Description of the campus network: 15
Reconnaissance: 17
Scanning: 19
Gaining access: 21
Keeping Access: 35
Covering his tracks: 36
Incident handling process: 37
Preparation: 37
Identification 39
Containment: 42
Eradication: 44
Recovery: 46
Lessons learned: 47
Conclusion: 48

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

List of Figures

Figure 1: IKEprobe Results 20
Figure 2: Safenet Client configuration 21
Figure 3: Safenet Client configuration 22
Figure 4: Phase 1 Information Derived by Cain Sniffer 23
Figure 5: Cain Sniffer Capture Including the Responder's Hash Payload 23
Figure 6: Cain Cracker Utility 24
Figure 7: Cain Cracker Utility Details 25
Figure 8: Cracked Pre-shared Key 26
Figure 9: Real and Virtual Adapter IP Addresses 27
Figure 10: Safenet Client Remote Party Identity Configuration 28
Figure 11: Safenet Connection Monitor 29
Figure 12: Superscan Results 29
Figure 13: Results of TigerTools Site Scan 30
Figure 14: Shares Discovered by Enum 31
Figure 15: List of Users Discovered by Enum 31
Figure 16: Password Policy Discovered by Enum 32
Figure 17: Successful Dictionary Attack on the Administrator Account 33
Figure 18: Mapping the Remote Drive 33
Figure 19: Explorer View of Remotely Mapped Drive 34
Figure 20: Running PWdump Remotely 35
Figure 21: PWdump Output Containing Password Hashes 36

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Statement of Purpose:

This paper will describe the VPN Aggressive mode pre-shared key brute force attack. The vulnerability was described in Michael Thurman's paper: "PSK cracking using Aggressive Mode". Vulnerabilities related to this attack were revealed in products of several leading vendors of RFC 2409 compliant VPN devices including Cisco and Checkpoint. The vulnerability, which is based on a weakness of the IKE protocol, will be discussed as well as some tools used to facilitate the attack. I will discuss the IKE protocol, the attack tools, how the attack can be used to gain access to a VPN network, and several methods for protecting against this attack. A hypothetical example of an incident based on this attack will also be discussed.

The Exploit Tools:

There are several tools available that may be used to exploit Aggressive Mode VPN networks. IKEprobe and IKE-scan are scanning tools that can be used to identify the presence of and gain information about VPN gateways, which may be targeted. Cain and IKEcrack are tools designed to carry out the aggressive mode brute force attack. Cain and IKEcrack basically do the same thing to carry out the exploit. However, I found Cain to be the easiest to use and chose to examine its use in the attack incident. Cain also has an advantage in that it cracks pre-shared keys hashed with MD5 and SHA. IKEcrack just supports MD5.

IkeProbe:

IkeProbe is a vulnerability scanner used to locate VPN devices, which are susceptible to the Aggressive Mode PSK brute force attack. The tool was created by Anton Rager and made publicly available in Nov 2003. An executable and the Perl source code for the tool can be downloaded from www.ernw.de/download/ikeprobe.zip. The command syntax for using IKEprobe is " IKEprobe <target ip>". IKE probe sends an IKE phase 1 aggressive mode packet to the target IP address containing an ISAKMP header, an SA payload containing a single transform set, a key exchange payload, a nonce payload, an ID payload and a vendor ID payload. IKEProbe then listens for the response from the target device. A vulnerable device will respond with a similar aggressive mode packet in an attempt to continue the negotiation. IKEprobe examines the response packet to determine if the transform set submitted by IKEprobe was acceptable to the target VPN gateway. The target device will respond with a NOTIFY message indicating NO_PROPOSAL_CHOSEN if the proposal submitted by IKEprobe doesn't match the phase 1 configuration of the target. If IKEprobe receives NO_PROPOSAL_CHOSEN from the target, it will sequentially cycle through combinations of phase 1 parameters, checking the response each time. If the target accepts the proposal, IKEprobe then indicates a success and identifies the phase 1 parameters of the target device including the Hash algorithm, the encryption method and the Diffie-Hellman group. The target is identified as being vulnerable to the Aggressive Mode pre-shared key attack. Algorithms supported by IKEprobe include DES, 3DES, AES-128 and CAST encryption, Diffie-Hellman groups 1, 2, and 5 and hash algorithms MD5 and SHA. To use IKEprobe, the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

target Gateway must either be configured to accept VPN connections from any IP, or the machine running the tool must use an IP address acceptable to the gateway. (1)

IKE-scan:

IKE-scan is a tool designed to fingerprint VPN devices using the IKE protocol. The tool is not linked specifically to aggressive mode, but can be used for reconnaissance purposes. IKE Scan is classified as a security-auditing program and employs the principal of UDP re-transmission back-off to fingerprint IPSEC VPN devices. For discovery, IKE-scan takes advantage of the fact that many VPN gateways will respond to an initiator sending phase 1 main mode requests thereby revealing their presence. In order to fingerprint VPN devices, IKE-scan examines the UDP re-transmission behavior of the target device. The tool runs on UNIX, Linux and various Windows platforms including Win-9x/ME, NT, 2000 and XP. The Windows version requires the Cygwin DLL. The source code, description and executables are available from: http://www.nta-monitor.com/ike-scan/. A white paper authored by Roy Hills, (2) developer of the tool, provides an overview of the tool and an example of its use. Being able to identify a VPN gateway in a network is a necessary starting point for an attack on a VPN.

IKE-scan can be employed during the scanning process to locate target devices such as VPN appliances, gateways, access concentrators and routers configured to support IPSec Virtual Private Networking. IKE-scan identifies the presence of VPN devices by sending a phase 1 Main Mode session initiation packet to the target device. IKE-scan takes advantage of the fact that many VPN devices will, by default, respond to a session initiation packet from any source. The session initiation packet contains an ISAKMP header and an SA. The target device will send a response packet to IKE-scan with an ISAKMP header and SA. The information obtained through this process is used to confirm the presence of a device running the UDP port 500 ISAKMP service.

IKE-scan does not respond to the gateway at this point, but listens as the gateway retransmits in an effort to complete the negotiation. The IKE protocol requires gateways to re-transmit lost packets. However, the timing of the retransmission attempts by the target gateway are not specified by the IKE standard, (3) so the retransmission behavior will vary from vendor to vendor. The retransmission behavior is recorded by IKE-scan and compared to a lookup table, which is installed with the tool containing results recorded from previous scans against known devices. Knowing specific information about the target VPN device, such as vendor or model information may allow an attacker to correlate known device vulnerabilities or weaknesses in the attack.

Cain:

Cain is described as a general-purpose WINNT password recovery tool providing the capability to sniff network traffic and retrieve password information from the traffic. (4) Cain has the built in capability to analyze information from multiple protocols including FTP, Telnet, HTTP, IMAP, ICQ and RADIUS. Cain also has the ability to perform

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

cryptanalysis on secure protocols such as HTTPS and SSH. Recently the capability to capture and analyze IKE Aggressive Mode phase1 traffic has been added. Using this feature, it is possible to sniff phase 1 traffic, send the captured data to the cracking application and derive the pre-shared key using a dictionary attack or brute force method. Combined with these features, the easy to use GUI and seamless operation make Cain an ideal tool to perform the aggressive mode attack, which is the subject of this paper. The machine running the sniffer must be able to capture the traffic somewhere along its path from source to destination. Other useful information can be obtained, such as the public Diffie-Hellman values, user-id, initiator and responder SA payload, IP addresses of the peers participating the IKE exchange, and initiator and responder cookies. Cain is available from http://www.oxid.it/cain.html

IKEcrack:

IKEcrack is an open-source cracking tool designed to derive IKE Aggressive Mode pre-shared keys. It is available from http://sourceforge.net/projects/ikecrack. An overview and some example performance data is available from http://ikecrack.sourceforge.net/. The function of IKEcrack is similar to Cain in that IKEcrack takes input from a sniffer capture of the IKE phase 1 messages and extracts the information from the target gateway's response, and runs a cracker against it. (5)

The Vulnerability:

The Aggressive Mode pre-shared key attack takes advantage of an inherent weakness in phase 1 Aggressive Mode negotiation based on the RFC 2409 standard (http://www.ietf.org/rfc/rfc2409.txt). The primary vulnerability is that the pre-shared key and other pieces of information are transmitted in an unencrypted hash and can be intercepted by eavesdropping. If this network traffic can be captured, the hash can be cracked off-line using a technique similar to password cracking. This authentication hash contains the pre-shared key used to authenticate the peers in the VPN session. Once the pre-shared key is derived from the hash, it can be used to connect to the target VPN gateway. Some additional factors related to specific vendor implementation contribute to the problem and can be used by attackers. When using Aggressive Mode, the user ID information is exchanged between peers unencrypted. This means that if someone is able to capture the phase 1 messages, the identification information of the peers can be gathered. Also, the IP addresses of the participants can be matched to the ID information. Some VPN implementations have a design flaw in which it was possible to force the gateway to use Aggressive Mode at the request of the VPN client (6). Cisco IOS may use Aggressive Mode even if configured not to do so. (7) When a gateway is using Aggressive Mode, the gateway will usually respond to an un-authenticated phase 1 initiator. This means that the attacker can do this with no knowledge of pre-shared keys or acceptable user IDs. Also, many VPN gateways have no mechanism to lock out repeated unsuccessful connection attempts. (8) This weakness facilitates use of scanning tools such as IKEprobe and IKEscan and similar attacks involving a brute force or dictionary attack against the user ID such as the one described in http://www.nta-monitor.com/news/checkpoint/checkpoint-tech.htm. Note that sending user ID information in the clear also yields useful reconnaissance information to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

attackers for other avenues of exploits. (9)

Advisories and references:

SecurityFocus Bugtraq ID:
http://www.securityfocus.com/bid/7423/exploit/

Cert advisory:
http://www.kb.cert.org/vuls/id/886601

NTA monitor discovers Checkpoint flaw:
http://www.nta-monitor.com/news/checkpoint.htm

Roy Hill's description of the vulnerability
http://seclists.org/lists/fulldisclosure/2002/Sep/0023.html

Statement from Cisco:
http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html

Statement from Checkpoint:
http://www.checkpoint.com/techsupport/alerts/ike.html

Description of the IKEcrack tool
http://ikecrack.sourceforge.net/

Michael Thurman's paper describing the vulnerability and how to exploit it:
http://www.ernw.de/download/pskattack.pdf

John Pliam's white paper on the vulnerability:
http://www.ima.umn.edu/%7Epliam/xauth/

Operating Systems Affected:

Vulnerable IETF RFC 2409: The Internet Key Exchange (IKE)
+ Check Point Software Firewall-1 [VPN + DES + STRONG] 4.1 Build 41439
+ Check Point Software Firewall-1 [VPN + DES + STRONG] 4.1 SP2 Build 41716
+ Check Point Software Firewall-1 [VPN + DES] 4.1
+ Check Point Software VPN-1 4.1
+ Check Point Software VPN-1 4.1 SP1
+ Check Point Software VPN-1 4.1 SP2
+ Check Point Software VPN-1 4.1 SP3
+ Check Point Software VPN-1 4.1 SP4
+ Cisco VPN 3000 Concentrator 2.0
+ Cisco VPN 3000 Concentrator 2.5.2 (A)
+ Cisco VPN 3000 Concentrator 2.5.2 (B)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

+ Cisco VPN 3000 Concentrator 2.5.2 (C)
+ Cisco VPN 3000 Concentrator 2.5.2 (D)
+ Cisco VPN 3000 Concentrator 2.5.2 (F)
+ Cisco VPN 3000 Concentrator 3.0
+ Cisco VPN 3000 Concentrator 3.0
+ Cisco VPN 3000 Concentrator 3.0.3 (A)
+ Cisco VPN 3000 Concentrator 3.0.3 (B)
+ Cisco VPN 3000 Concentrator 3.0.4
+ Cisco VPN 3000 Concentrator 3.1
+ Cisco VPN 3000 Concentrator 3.1 (Rel)
+ Cisco VPN 3000 Concentrator 3.1.1
+ Cisco VPN 3000 Concentrator 3.1.2
+ Cisco VPN 3000 Concentrator 3.1.4
+ Cisco VPN 3000 Concentrator 3.5 (Rel)
+ Cisco VPN 3000 Concentrator 3.5.1
+ Cisco VPN 3000 Concentrator 3.5.2
+ Cisco VPN 3000 Concentrator 3.5.3
+ Cisco VPN 3000 Concentrator 3.5.4
+ Cisco VPN 3000 Concentrator 3.5.5
+ Cisco VPN 3000 Concentrator 3.6
+ Cisco VPN 3000 Concentrator 3.6.1
+ Cisco VPN 3002 Hardware Client

Vendor Status Date Updated

3Com Unknown 18-Sep-2002
Alcatel Unknown 18-Sep-2002
Apple Computer Inc. Vulnerable 20-Sep-2002
AT&T Unknown 18-Sep-2002
BSDI Unknown 18-Sep-2002
Check Point Vulnerable 8-Oct-2002
Cisco Systems Inc. Unknown 18-Sep-2002
Compaq Computer Corporation Unknown 8-Oct-2002
Computer Associates Unknown 18-Sep-2002
Conectiva Unknown 18-Sep-2002
Cray Inc. Unknown 18-Sep-2002
Data General Unknown 18-Sep-2002
Debian Unknown 18-Sep-2002
F5 Networks Not Vulnerable 8-Oct-2002
FreeBSD Not Vulnerable 17-Oct-2002
Fujitsu Not Vulnerable 18-Sep-2002
Guardian Digital Inc. Not Vulnerable 2-Oct-2002
Hewlett-Packard Company Unknown 8-Oct-2002
IBM Unknown 18-Sep-2002
Intel Unknown 18-Sep-2002
Juniper Networks Unknown 18-Sep-2002

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

KAME Project Vulnerable 15-Oct-2002
Lachman Unknown 18-Sep-2002
Lotus Software Unknown 18-Sep-2002
Lucent Technologies Unknown 18-Sep-2002
MandrakeSoft Unknown 18-Sep-2002
Microsoft Corporation Not Vulnerable 30-Sep-2002
MontaVista Software Not Vulnerable 20-Sep-2002
Multinet Unknown 18-Sep-2002
NEC Corporation Unknown 8-Oct-2002
NetBSD Vulnerable 17-Oct-2002
Network Appliance Not Vulnerable 20-Sep-2002
Nortel Networks Unknown 18-Sep-2002
OpenBSD Unknown 18-Sep-2002
Openwall GNU/*/Linux Unknown 18-Sep-2002
Oracle Corporation Unknown 18-Sep-2002
Red Hat Inc. Unknown 18-Sep-2002
Sequent Unknown 18-Sep-2002
SGI Unknown 18-Sep-2002
Sony Corporation Unknown 18-Sep-2002
Sun Microsystems Inc. Not Vulnerable 20-Sep-2002
SuSE Inc. Not Vulnerable 20-Sep-2002
The SCO Group (SCO Linux) Unknown 18-Sep-2002
The SCO Group (SCO UnixWare) Unknown 18-Sep-2002
Unisphere Networks Unknown 18-Sep-2002
Unisys Unknown 18-Sep-2002
Wind River Systems Inc. Unknown 18-Sep-2002
Xerox Corporation Not Vulnerable 4-Apr-2003

Targeted protocols, Services and Applications:

This exploit targets the Internet Key Exchange protocol, specifically IKE using Aggressive Mode. This protocol is described in RFC2409 and is one of several protocols used by IPSEC to establish a VPN. The IKE protocol is used to facilitate an authenticated key exchange between two participants in a VPN network. IKE performs automatic key negotiation using the Diffie-Hellman algorithm. The IKE process consists of two distinct phases. Phase 1 is used to create a secure management tunnel to protect IPSEC negotiations. During phase 2, the IPSEC tunnel is established, which once completed, is used to carry protected user traffic. Security Associations are built during phase 1 and phase 2 which define the VPN tunnel parameters, including key lifetimes, encryption and authentication types, and other details used by the end systems to manage traffic carried in the VPN. To create an IPSEC VPN, a suite of protocols is employed. These include AH (Authentication Header), ESP (Encapsulating Security Protocol), and IKE (Internet Key Exchange). ESP and AH are used to protect user traffic carried in the VPN. IKE is used to establish and manage automatic key exchange used in the VPN session. IKE uses Internet Security Association and Key Management Protocol (ISAKMP) to perform authenticated key exchange for IKE and manage Security Associations. IPSEC VPNs employ encryption algorithms to encrypt data, hash algorithms to authenticate data, authentication methods to validate participating peers and the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Diffie-Hellman algorithm to securely exchange keying material used for encryption and hashing. A brief discussion of the messages exchanged between peers during tunnel establishment will help the reader to understand the attack mechanism and the vulnerability upon which it is based. While the attack, which is the focus of this paper is based on aggressive mode, the following discussion will also include details covering main mode. It is worth noting the differences between Aggressive Mode and Main Mode, and we will see why Main Mode is not vulnerable to the attack and should be used instead of Aggressive Mode.

Phase 1

Phase 1 of IKE is used to build an ISAKMP tunnel, which can be thought of as a management tunnel. This management tunnel does not carry user traffic, but instead is used to carry out secure, authenticated negotiation of the IPSEC tunnel established during phase 2. Establishment of a VPN begins with phase 1. During Phase 1, the VPN endpoints or IKE peers, negotiate the encryption and authentication methods used to protect further traffic required to establish the VPN. The devices also exchange keying material used by the encryption and authentication processes and validate the identity of the partner. There are two modes used to carry out the phase 1 process: Main Mode and Aggressive Mode. Main Mode is most commonly used and is typically employed to create site-to-site VPNs. Main mode uses three 2-way message exchanges between peers to accomplish phase 1. Aggressive Mode is a streamlined version of Main Mode involving a 2-way message exchange to carry out the phase 1 negotiations. Configuration parameters of the phase 1 tunnel include peer authentication method, Diffie-Hellman group, data encryption algorithm, data hash algorithm and key lifetime. These attributes are applied to the creation of the management tunnel and are independent of the parameters used to protect user traffic in phase 2.

Phase 1 Main Mode messages:

The first set of messages exchanged during phase 1 are used to negotiate the phase 1 encryption algorithm, hash algorithm, authentication method and key lifetime. The initiating peer sends a proposal containing a set of parameters it can use. The responding peer selects an acceptable subset of parameters contained in the proposal and notifies the initiator of its choice. (10)

First message of Main Mode:

Message #1 / Initiators message:
ISAKMP header
SA header containing: proposal payload, transform set payload ---------->
Initiator's cookie

Message #2 /responder's message:
ISAKMP header
<----------SA header containing: accepted proposal
Responder's cookie

This 2-way message exchange allows the peers to negotiate encryption and authentication

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

methods used to protect the establishment of the phase 1 session. The cookies are used to help reduce the peers' susceptibility to ISAKMP denial-of-service attack. After this exchange has taken place, and, assuming that an acceptable proposal has been agreed upon by the responder, both peers generate public and private Diffie-Hellman values which will be used for secure key exchange. This key exchange mechanism is used by the participants to establish the SKEYID, which is the root key upon which the ancillary keys are derived.

Second message of Main Mode:

The second set of messages are used by the peers to exchange Public Diffie-Hellman values and Nonces:

Message #3 / Initiators message:
ISAKMP header
Key exchange payload ---------->

Message #4 /responder's message:
ISAKMP header
<---------- Key exchange payload
Initiator's Nonce

After the second 2-way exchange, both peers will use the public Diffie-Hellman values to compute the root key SKEYID and the ancillary keys. Exactly how the root key is computed is dependent upon the peer authentication method. When using pre-shared keys, SKEYID is computed as:

SKEYID =prf (preshared key, Nonce_I, Nonce_R)

The key used for phase 1 data encryption and authentication is then computed, as well as the SKEYID_d, used to create keys for phase 2. At this point, further Main Mode exchanges are protected using the encryption and hashing algorithms negotiated by the peers during the first message exchange.

The third set of messages is used by the peers to authenticate the key exchange. The peers now exchange ID information contained in a hash formed from the ID payload and other pieces of information exchanged in the previous phase messages. In Main Mode, the phase 1 encryption protects the identity information contained in the hash. This process is used to link the key exchange to the identity information of the peers.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Third messages of Main Mode:

Message #5 / Initiator's message:
ISAKMP header
ID payload---------->
Hash payload

Message #6 /responder's message:
ISAKMP header
<----------ID payload
Hash payload

The encrypted ID payload contains identification information about the peer such as IP address, FQDN or User FQDN. The Hash payload contains a hash of several elements from the previous messages and is computed using the chosen phase 1 hash algorithm, usually MD5 or SHA:

prf (SkeyID, Ya | Yb| cookie_i | cookie_r | SA offer | ID_i)

The hash is encrypted by the SKEYID_E key, which has been derived from the root key, SKEYID. After the completion of the phase 1 message exchange, the phase 2 negotiations can begin. (11)

Aggressive Mode:

The goal for Aggressive Mode is the same as Main Mode, to negotiate acceptable transforms and authenticate the peers. Aggressive Mode is a streamlined version of Main Mode and is faster. However, limited ability to negotiate some options and the lack of protection for the ID payload and hash containing the pre-shared key is the cost. The identity information exchanged in the last 2 messages of Main Mode is encrypted, which hides the identity information from sniffing off the wire. Aggressive Mode identity information is not encrypted and can be captured using a sniffer during the phase 1 negotiation.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Phase 1 messages exchanged using Aggressive Mode:

When using Aggressive Mode, the negotiations begin with a message from the initiator sent to the gateway constructed as follows:
(CKYi, SAi, g^I, Ni, Idi) Where:

CKY is the Initiator's randomly generated cookie

SAi is the initiator's transform set. This information could be set according to the values found using IKEprobe

g^I is the initiator's public Diffie-Hellman value

Ni is the initiator's Nonce, also a random value

IDi is the initiator's Identification payload. When using preshared keys, the contents of this field are arbitrary, I.E., the gateway will not drop the session according to the validity of the user id information.

The VPN Gateway will respond with: (CKYr, SAr, g^r, Nr, Idr, Hr) Where:

CKY is the responder's randomly generated cookie

SAr is the transform set chosen by the responder

g^r is the responder's public Diffie-Hellman value

Nr is the responder's Nonce, also a random value

Idr is the responder's Identification payload

Hr is the authentication hash used to authenticate the phase 1 exchange. The authentication hash is formed using similar components from Main Mode:
Hr = F (s, (g^r g^,i CKYr CKYi SAr Idr))

The component "s" in the responders hash is formed by:

s= f(pw, Ni, Nr)) where pw is the pre-shared key, and f is a pseudo-random function.

The initiator sends the last message of Aggressive Mode, which contains

Hi = F (s, (g^i, g^,r, CKYi, CKYr, SAi, IDi)

The initiator and responder will generate their own hash of the components presented during the negotiations and compare this hash to the hash sent by the peer. Similar to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Main Mode, a match will validate the exchange, whereas a mismatch will invalidate the exchange and cause the peers to drop the session. At this point, a final session key is generated by the peers completing phase 1. (12)

Phase 2

During phase 2, IPSEC SAs are created which define encryption, authentication and key lifetime parameters used to protect user data passed through the VPN. The phase 2 tunnel carries encrypted and authenticated user data. Phase 1 must successfully complete before phase 2 can start. Duration of the tunnel is primarily determined by key lifetime parameters based on time or quantity of data.

MD5 and SHA Hashing algorithms:

MD5 and SHA-1 are common hashing algorithms used in VPNs. Hashing algorithms are used to authenticate data in IPSEC. Hashing algorithms are also employed during phase 1 negotiations to authenticate the Diffie-Hellman exchange used to establish root keys. Hashing is performed by inputting a message into a mathematical process that creates a value called a message digest. This message digest is ideally a totally unique value, which cannot be arrived at by any other possible input message. (13)

Variants:

IKE username sniffing:

When using Aggressive Mode during IKE phase 1, the initiator sends ID information in the clear to the VPN gateway. The initiator's packets can be sniffed allowing retrieval of the user-id. (14)

IKE username guessing:

Previous versions of the Checkpoint FW-1 Firewall/VPN gateway have been reported to be vulnerable to user name guessing. When attempting Aggressive Mode phase 1 to the gateway with an invalid user-id, the gateway will respond with an IKE notification message indicating that the user is not valid for IKE or other information indicating why the user is not accepted. Distinctions in the behavior of the Checkpoint firewall when responding to various user ID conditions can be used to determine the version of the firewall, which could be useful in helping the attacker determine an attack approach. (15)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Description:

VPNs have become a prominent solution for securing remote network access. VPNs allow corporations to use existing dial-up or broadband connectivity to create secure channels for telecommuters and mobile users. By using remote access VPNs, a corporate IT staff can extend the corporate network out to the remote user over a dynamically established, encrypted link and experience benefits over other methods which may be less secure or more expensive. A typical configuration for allowing remote access for mobile users employs an access concentrator, such as the Cisco VPN3000 series to serve as the VPN gateway at a corporate site, and the use of a VPN client running on the remote users PC. Used in conjunction with the access concentrator, a VPN client is a software product used to enable a remote user's PC to act as an IKE peer and terminate a VPN tunnel. Mode Config may also be used to allow the gateway to assign a virtual IP address to the client from a pre-configured pool similar to a DHCP pool. The virtual address assigned to the client places the client in the corporate private network. Once the tunnel is established, the user can send traffic securely from the PC through the tunnel to the VPN gateway, which un-encrypts the traffic and delivers it to the network similar to a site-to-site VPN. The remote access scenario that lends itself to the attack described in this paper is based on remote access provided to a VPN client using a dynamically assigned IP address, common for remote users. In this scenario, the central site VPN gateway may be configured to accept connection attempts from any IP address. (16) For example, Cisco employs the concept of a dynamic crypto map to accomplish this.

MAIN MODE vs Aggressive Mode:

Remote access VPNs using pre-shared key authentication are the primary application for Aggressive Mode. Aggressive Mode negotiations are faster than Main Mode negotiations since there are fewer messages exchanged during Phase 1. In some remote access schemes, the encryption and authentication parameters are fixed, so there is no need to send additional messages to negotiate them. Also, since the identity information is sent in the clear in the first message by the initiator, the responder may be able to use the ID information to link the initiator to a valid list of users. (17) The fact that identity information is sent in the clear and is easily picked up by eavesdroppers is a notable disadvantage. Since fewer messages are sent, the set of parameters that can be negotiated by VPN devices using Aggressive Mode is limited. Main mode takes longer to complete phase 1 but protects the identity information by sending it over the phase 1 encrypted channel. The additional delay incurred by Main Mode, however is small and will usually not be noticed by remote users. Main Mode allows negotiation of encryption, authentication parameters, Diffie-Hellman group and key length.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Peer Authentication method:

Common peer authentication methods used for VPNs are pre-shared keys and digital certificates. These methods can be used to validate the identity of the endpoints participating in the VPN. Note that these methods do not provide verification of the identity of the users, but instead authenticate the devices participating in the VPN. Additional authentication mechanisms may be employed to validate users, such as Xauth with RADIUS or RSA Secure ID token. The strongest means to authenticate a Remote Access VPN tunnel involves a combination of digital certificates and Xauth with Secure token. However, the complexity of this method makes it difficult for system administrators to implement and hard for users to understand, and is one reason why many choose to use simpler means such as pre-shared keys. Pre-shared keys are easy to set-up, but when combined with dynamic IP addresses require the use of Aggressive Mode. This configuration is subject to the pre-shared key brute force attack.

Attack process:

The first piece of information needed to perform the attack is the IP address of the target VPN gateway. Frequently, this can be determined in a variety of ways. IP addresses or resolvable domain names for the VPN gateways may be published on a website with remote access information. A network scan looking for listeners on UDP port 500 can also be used to identify VPN devices. With the target VPN gateway's IP address, a scanner such as IKEscan or IKEprobe can be used to gain additional information and determine if the gateway is using Aggressive Mode. If the target gateway is using Aggressive Mode, IKE probe can also get the Phase 1 information an attacker would need to configure the VPN client with matching parameters. IKE-scan may also be used to fingerprint the VPN gateway and identify the vendor of the device. We also must have network access to the gateway, and be able to sniff ISAKMP traffic somewhere along the way from the client device to the gateway. The next step in the process involves capturing a phase1 response from the target gateway during a connection attempt. In order to perform the attack, the phase 1 Aggressive Mode response from the gateway must be captured. The session can be initiated by a legitimate VPN user, or the attacker. If the attacker attempts to initiate phase 1, he may need to do so from a machine using an IP address the Gateway will accept. However, in many remote access scenarios, the target VPN gateway will accept connection attempts from any device. (18) It is not necessary to complete the tunnel to obtain the information used in the attack since the exchange is un-authenticated. This means that the attacker doesn't need to know a user-id or anything about the pre-shared key. All the attacker needs to do is send a phase 1 initiation packet to the target gateway and capture the gateway's response as follows:

Initiator's (attacker's) message to the gateway :

(CKYi, SAi, g^I, Ni, Idi)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The sniffer will capture the VPN gateway's response:

(CKYr, SAr, g^r, Nr, Idr, Hr)

Hr is the Hash payload containing the digest of session information, which the cracker will use to derive the pre-shared key. Note that in a normal exchange, the initiator would, at this point answer the gateway with a Hash_i message. When cracking the pre-shared key, the reponse from the gateway is un-answered. As mentioned earlier in the discussion of IKEscan, the gateway will assume that the response was lost and resend the response multiple times until timing out. The responder's hash payload is a message digest created by hashing the following components:

Hr = F (s, (g^i, g^,r, CKYi, CKYr, SAi, IDi)

" The attacker conducts an off-line dictionary attack, enumerating all candidates pw* and for each computing s*= f(pw*, Ni, Nr)) and
Hi* = f(s*, g^i, g^r, CHYi, CKYr, SAi, IDi)). If Hi = Hi*, then with high probability, pw = pw". (19) Cain and IKEcrack both perform this cracking operation to derive Aggressive Mode pre-shared keys. Once the pre-share key is obtained, the attacker enters this value into their VPN device configuration and retries the connection. Using the derived key and other configuration parameters retrieved using IKEprobe will allow the connection to complete.

Exploit Story/The setting:

Miskatonic is a small university in south central Tennessee consisting of a single campus containing a dozen buildings. They have a small IT staff that spends most of their time maintaining services, upgrading servers and tending to network problems. The university also uses the help of volunteer faculty and students to manage departmental network equipment, but this practice is being discouraged by new management. Internet service is provided by a local ISP. Much of the equipment was donated by a local telecommunications company, Adtran, a producer of routers, switches, and VPN appliances. They also purchased equipment from a variety of vendors including Cisco, Linksys and Netgear. No one had been trained in incident handling other than the on-the-job training that came with the territory. The security program was outdated, and for the most part consisted of anti-virus protection, occasional server patching, and blocking unsolicited inbound traffic destined to the internal campus network. There is no password policy, and little attention to system hardening. Physical security is also very lax. Other than common e-mail viruses, the university had suffered no significant internal or external network attacks, hence, there was no sense of urgency among higher management. As is typical in academic environments, the main priority was on maintaining open and free access to resources and less on security. A few newer security upgrades had been incorporated into the network a few years ago during a revamping sponsored by one of the engineering department faculty enlisting the help of several students and the donation by Adtran of some networking equipment.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Description of the campus network:

The campus consists of a dozen or so buildings. Each building was placed on its own subnet and its own VLAN. Wiring for each building was based on a star configuration. Office workstations and lab computers were cabled to a network closet and terminated onto Catalyst switches. The Catalyst switches had been used to replaced hubs and were part of the recent security upgrade to provide protection against sniffing. The switches contained in each building were connected to routers which all accessed a backbone network. The backbone connects to a 3640 Cisco router. Additional interfaces on the router are used to create subnets for various networks including the campus DMZ, the Admin systems subnet, the campus server subnet and other miscellaneous subnets. Access to the Administrative systems subnet and the campus server's subnet is considered restricted and was controlled with access lists. The servers in this administration building contains critical databases, which holds student records, grades, status, transcripts, and billing information. The 3640 has a single frame-relay T1 connected to a local ISP for Internet access. There are two mechanisms in place to allow Off-campus access to the university network. The old system was a modem dial-in pool. Registration with the IT department was required to obtain a remote access account. In an attempt to modernize, a new VPN access solution had been recently set up. To provide VPN access, the university employed the Adtran 3305 router with the VPN/firewall feature set at the central site and issued the Safenet VPN client to remote users. Using either method allowed a remote user to operate a remote workstation as though it physically resided on the campus network. The purpose of the remote access network was to provide students with access to campus servers and to allow faculty access to administrative systems for student records and related information. The security for the dial-in access and the remote access VPN was considered equivalent.

Marty is a full time employee of the university's IT staff and a graduate of the university's computer science program. His main responsibilities includes everything from patching servers and configuring switches to running patch cables in the network closets. Having a high degree of motivation and a special interest in network security, Marty had worked his way into becoming the de-facto campus network security expert and was involved in setting up the remote access VPN. The computer science curriculum and open access to the Internet from several campus computer labs tended to foster innocent, and occasionally, malicious tampering with the school network by the more technically inclined students. Dr. Krycheck, was a teacher in the computer science department who had a penchant for trying new ideas. When a student was caught using a sniffer to capture traffic on the building's subnet, he suggested the idea of using an internal VPN network that would allow faculty to transmit confidential information across the internal network and protect the traffic from eavesdropping. Marty had done well in Dr. Krycheck's classes and the two had worked together on several campus networking projects. Setting up the internal VPN network became Marty's project. While not as common an application, internal VPNs can be used to secure network communication in a hostile environment. An internal VPN may also be used in conjunction with an external VPN in high security environments. The internal VPN configuration allows a software VPN client on a laptop or desktop machine anywhere on the campus to create a VPN tunnel across the university's private

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

network to reach restricted access networks protected by the Firewall. This utility allowed a teacher to send confidential traffic across the relatively un-secure campus backbone with the same protection offered by the remote access VPN.

The campus internal network was not truly a hostile environment, but the idea of the internal VPN became a pet project for Dr. Krycheck. Since the university already had the hardware and Safenet VPN client, the only additional cost was the time required for Marty to set it up. Use of the internal VPN was not mandated by the University's security policy, but many of the faculty and staff in the engineering and computer science building began using it. The internal VPN capability was not intended to be used by students, since unlike the remote access network, it provided a direct connection to the Admin network, but eventually its use became common knowledge among students. Being somewhat eccentric and boastful, Dr. Krycheck had mentioned in a computer networking class " Don't bother trying to catch a glimpse of next weeks quiz by sniffing the network, I use a VPN off campus and on campus to transmit test files. It won't do any good unless you can crack 3DES. If you can figure out how to do that, you get an automatic A for the semester". One student that took special notice to this comment was Mark. Mark was a computer science major, a semester away from graduating and in dire straits. As is typical for some students, at some point during the academic career, you meet an instructor that you just don't get along with. For Mark, it was Dr. Krycheck and as far as Mark was concerned it was mutual. The worst of it was that somehow even though Mark felt like he had worked hard and done well, he had earned poor grades in the class and saw himself as treated unfairly.

As finals rolled around, Mark became very concerned about his grade in the class. His grade-point average had fallen slightly over the last few semesters and he was concerned that another low grade would jeopardize his chances of getting a good job at the company he had co-oped at for the last 4 years, Adtran. Adtran's engineering managers seemed extremely picky about grades and Mark worried that if his GPA dropped below 3.5, he might not get hired. Wednesday, December 5th, after taking Dr. Krycheck's final exam, he knew he was sunk for the semester. Mark deeply resented what seemed like unfair treatment he had received from Dr. Krycheck, enough so that he no longer had any moral qualms about cheating if that's what it took to get through the semester and be done with it. During his co-op terms at Adtran, Mark had developed some networking skills as well as an interest in hacking tools. He also spent one co-op term testing one of their VPN/firewall devices. So, when Dr. Krycheck mentioned using his VPN client to transmit test files, it caught Mark's attention. He began to wonder if there might be an opportunity to do some academic espionage. That weekend, Mark began to do some research. He found information about VPN man-in-the-middle attacks. This was complicated stuff and was beyond his skill level. Eventually, more refined searches on Google revealed some vulnerabilities that related to remote access VPNs, specifically the Aggressive Mode brute force attack. This attack was not designed to try to crack VPN encryption, but instead was focused on capturing packets exchanged during the tunnel setup and using a password cracker to crack the pre-shared key contained in the captured packets. As he studied more, this approach began to appear doable, and more intriguing. There were readily available

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

tools on the Internet but several questions remained about exactly how to pull this thing off, and not get caught. Mark began to study the tools, collect them on his laptop, and construct with a plan.

Reconnaissance:

Mark reasoned that with no password policy, a lazy network administrator would probably use pre-shared keys to authenticate the tunnels, and that with so many remote users they might also set up the VPN gateway to accept connections from any IP address, which meant use of Aggressive Mode. He needed the addresses of the VPN gateway interfaces, so he could scan them and determine if they would accept Aggressive Mode connections. He found some documentation about the VPN network lying around in one of the labs but he couldn't find an IP address or any other specific information about the Public or Internal VPN server. Mark began to do some Internet searches on the campus web site. Here, on a help page set up by the IT department providing information for setting up a remote access VPN, he found information about the university's VPN gateway, which VPN clients they supported and the gateway's IP address. Then he came up with another idea. He knew the external VPN was used by students and faculty, but that the internal VPN was only used by faculty. There must be additional authentication mechanisms placed on the external VPN that might not be applied to the internal VPN. He knew that at least some of the faculty in the computer science building had recently used the VPN to log into the admin network to post grades, and others were probably still in the process of doing so. If he could get access to the internal network, capture some phase 1 VPN traffic and run the cracker, he might be able to get a teacher's pre-shared key. Then he could use the VPN exploit to gain access to the admin systems. In order to do this, he had to have physical access to the building's network. He decided to look around the engineering building to see if there were avenues for physically gaining access to the building's network. Usually, there was no one around on the weekends and the building and labs were typically unlocked.

Saturday afternoon, he headed over to the engineering building and casually looked around. His first goal was to find an unoccupied office with a live network jack. He knew from experience that the university had a habit of leaving network jacks live, even when the office was unoccupied for a whole semester. He also knew where there were offices used by teaching assistants and graduate students. He found several offices that were vacant, making special note of one with cubical partitions. He also made note of the data jack number, 347B. He also made note of the office numbers of several teacher's offices in the Engineering Department. Next, he went over to the main computer lab. Having worked in the computer labs quite a bit over the years at the university, Mark knew that the computer labs had an adjacent network room where physical connections were made to the campus network. The Cisco catalyst switches forming the building's VLAN were located there. With easy access to this area, he might be able to sniff traffic from the building's VLAN. This would require configuring a spanning port on the switch, which was a simple procedure. There were a few students using computers in the lab, but having been in and around the lab frequently over the last couple of years, Mark didn't feel his entering the network room would raise any suspicion. He could see

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

though a glass window into the network room as he walked through the computer lab. He could see a rack containing various network equipment, RJ-45 patch panels and a couple desks with workstations. There was no one in the network room at that time. He could see several catalyst switches rack-mounted in the equipment rack.

Late Sunday, as he considered the consequences of getting caught, his enthusiasm faded slightly. In order to leave town early, Dr. Krycheck had given the final exam several days ahead of the normal semester schedule. By Monday he had already posted grades and left to go out of town for a technology conference. Mark went by Dr. Krychecks office at 3:00 and found his final grade. “A d!.That does it. I am going to do something about this!” he thought. One thing Mark was concerned about was the timing of his intervention. The grade had to be changed before it made it into the master records. He decided to employ a little social engineering to try to get some information. He called the student record office. “ I had my final already, but I don’t see my grades on the website. How soon will my grade be posted? “. The reply “ Its still kind of early. A lot of the teachers have sent in their grades, but we haven’t had time to enter them all yet. We probably wont be done until next week”. Based on this information, he surmised that it was possible that the grade file had been transmitted, but no one in student records had done anything with it. His goal would be to alter the information in the grade file before student records entered the data. His plan was to just slightly alter the data. From D to B would be adequate to preserve his GPA.

That night, Mark went back to the engineering building with his laptop, an RS232 cable and a couple of ethernet cables. A quick glance revealed that there was no one in the network room. He powered up his laptop and opened a Hyperterminal session. Using information contained in a diagram on the wall, he traced several connections from the Engineering department’s teacher’s offices to a particular switch. He connected the serial port of his laptop to a console port using the blue Cisco cable still attached to the switch console. He logged into the switch using the default login: admin admin. The output from “show config” indicated that most switch ports were on VLAN 192. Mark configured an unused port to be a spanning port, allowing this port to “see” all traffic passing through the switch using the following command:

```
topswitch(config)#interface fastEthernet 0/17
topswitch(config-if)#switchport mode access
topswitch(config-if)#switchport access vlan 192
topswitch(config-if)#port monitor
```

This would provide the capability to sniff traffic on the building’s VLAN. Next, he took the ethernet cable and connected one end to the spanning port and ran the other end to a patch panel mounted on the wall. He found jack 347 B on the patch panel and connected the ethernet cable to the jack. He guessed that no one would notice another random cable in the rat’s nest of wiring in the network room.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Scanning:

Next Mark went back to the office with the cubicle partition and connected his other ethernet cable from data jack 347 B to the NIC card on his laptop PC. He booted his laptop into Linux. He also started Tcpdump to capture all traffic on the NIC card using promiscuous mode. The capture was saved to a file on the hard drive.

TCPdump –I eth0> project.txt

Right away he could see miscellaneous activity on the network including a few ARP requests and HTTP gets. This confirmed he was capturing traffic on the building's network. He left the TCPdump running and slightly closed the laptop. He then put the laptop under the desk and pushed a box in front of it to conceal it. He decided to let the capture run overnight. The next morning, Mark went back to the campus to check on his laptop. It was still there and still connected. Later, that evening he went by the cubicle again and after making sure no one was around, he got out the laptop and stopped the TCPdump capture. He opened up the file using VI:

pico project.txt

He scanned through the results file, which was quite large. Eventually he found what he was looking for. A capture of an Aggressive Mode negotiation:

```
11:52:38.213807 arp who-has 192.168.1.2 tell 192.168.1.3
11:52:38.213807 arp reply 192.168.1.2 is-at 0:a0:c8:b:f6:37
11:52:39.533807 192.168.1.3.isakmp > 192.168.1.2.isakmp: isakmp: phase 1 I
agg: [|sa]
11:52:39.603807 192.168.1.2.isakmp > 192.168.1.3.isakmp: isakmp: phase 1 R
agg: [|sa]
11:52:40.483807 192.168.1.3.isakmp > 192.168.1.2.isakmp: isakmp: phase 1 I
agg[E]: [|hash]
11:52:40.803807 192.168.1.3.isakmp > 192.168.1.2.isakmp: isakmp: phase
2/others I oakley-quick[E]: [|hash]
11:52:40.823807 192.168.1.2.isakmp > 192.168.1.3.isakmp: isakmp: phase
2/others R oakley-quick[E]: [|hash]
11:52:40.823807 192.168.1.3.isakmp > 192.168.1.2.isakmp: isakmp: phase
2/others I oakley-quick[E]: [|hash]
11:52:45.603807 192.168.1.3 > 192.168.1.2: ESP(spi=0xe4e99bf6,seq=0x1)
11:52:47.033807 192.168.1.3 > 192.168.1.2: ESP(spi=0xe4e99bf6,seq=0x2)
11:52:48.533807 192.168.1.3 > 192.168.1.2: ESP(spi=0xe4e99bf6,seq=0x3)
11:52:50.033807 192.168.1.3 > 192.168.1.2: ESP(spi=0xe4e99bf6,seq=0x4)
```

From the capture, he could see that a device with IP address 192.168.1.3 had started an Aggressive Mode session with a device at 192.168.1.2. He reasoned that 192.168.1.3 must be the IP address of a VPN client. He rebooted into a Windows 2000 partition and opened a folder containing the tools chosen to carry out the attack. Next, he launched an IKEprobe scan of the supposed VPN gateway's IP address

IKEprobe 192.168.1.2 (enter)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

He watched as IKEprobe ran through various phase 1 transform set permutations. As IKEprobe ran through proposal after proposal without success, he began to sense failure. Maybe they were careful and configured their remote access policies without using Aggressive Mode. At last, a match! IKEprobe reported a successful match with the following result:

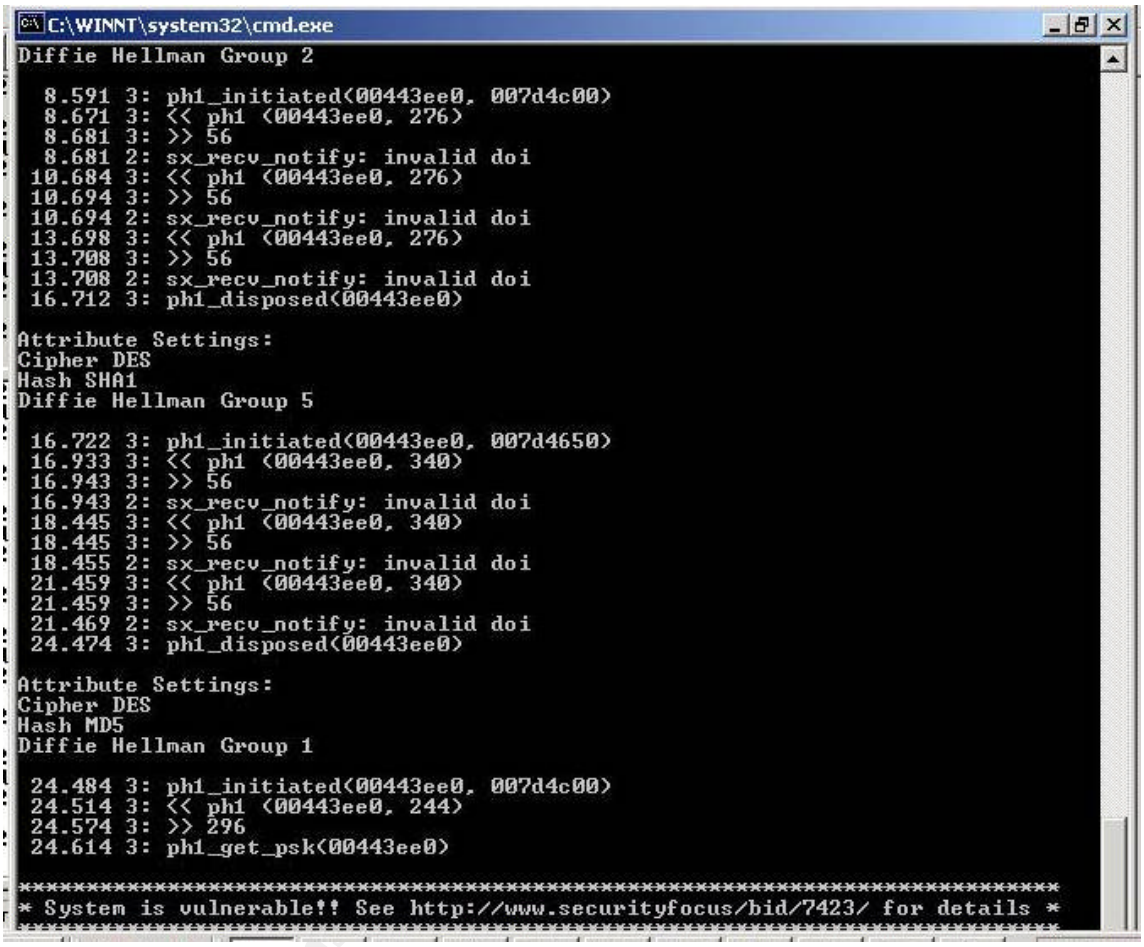


Figure 1: IKEprobe Results

Now as a result of running IKEprobe, Mark had the following information about the remote access VPN gateway:

Phase 1 parameters: Encryption DES, Authentication Hash MD5, Diffie-Hellman Group 1
The IP address of the VPN gateway public interface: 192.168.1.2
Authentication method: pre-shared keys
Phase 1 mode: Aggressive

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Gaining access:

Mark had already installed Cain. The GUI was easy to use and he was anxious to try to crack some passwords. He had also installed a stolen copy of the Safenet VPN client on his laptop. Adtran used the Safenet VPN client and during one of his recent co-op terms, he was able to get a copy of the zipped install file and store it on a USB flash drive. He configured a phase 1 proposal using the same transform set he had discovered using IKEprobe. Just guessing, he put in the same encryption and hash algorithms for phase 2. He also configured the Internal VPN gateway IP address as his IKE peer. The pre-shared key was still unknown, but that was not a problem at this point since an arbitrary key would be used. The VPN gateway should respond to his client's attempt to start a session, with an arbitrary pre-shared key and provide the Hash_r payload he needed to crack the pre-shared key. A simple guess was entered: abcdefgh. From this screen most of the remote identity information including ID-type, subnet and mask can be seen.

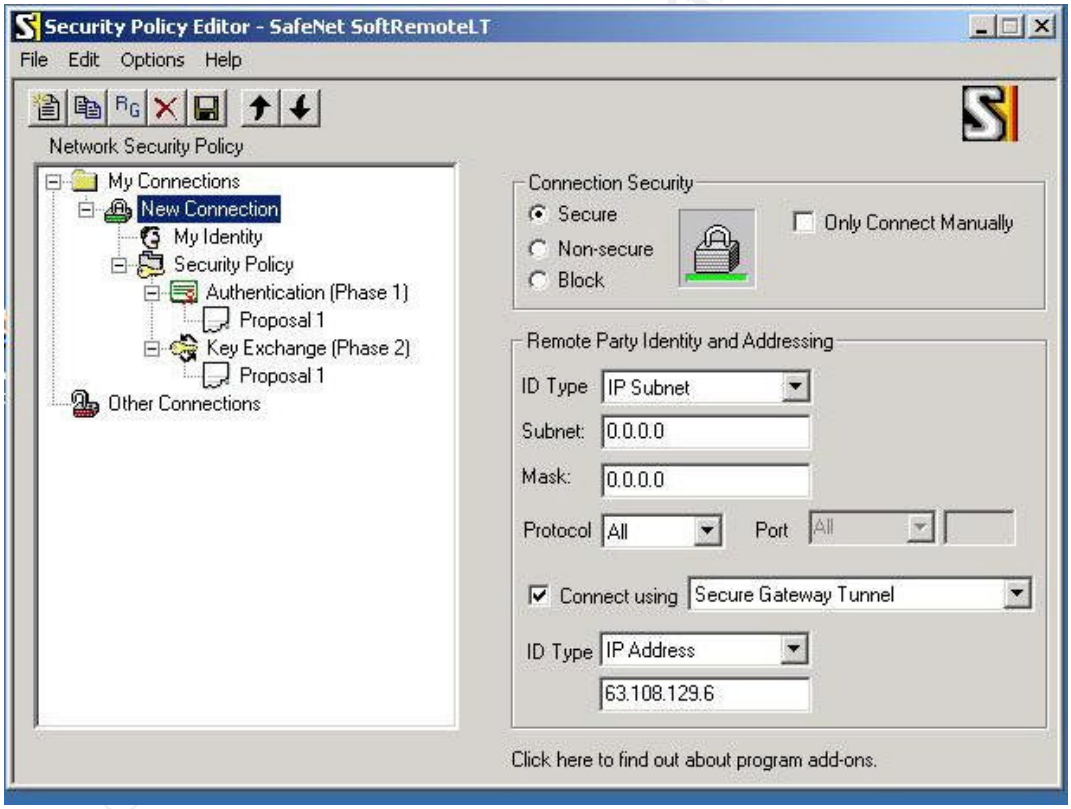


Figure 2: Safenet Client configuration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The second menu allows configuration parameters for Main or Aggressive Mode

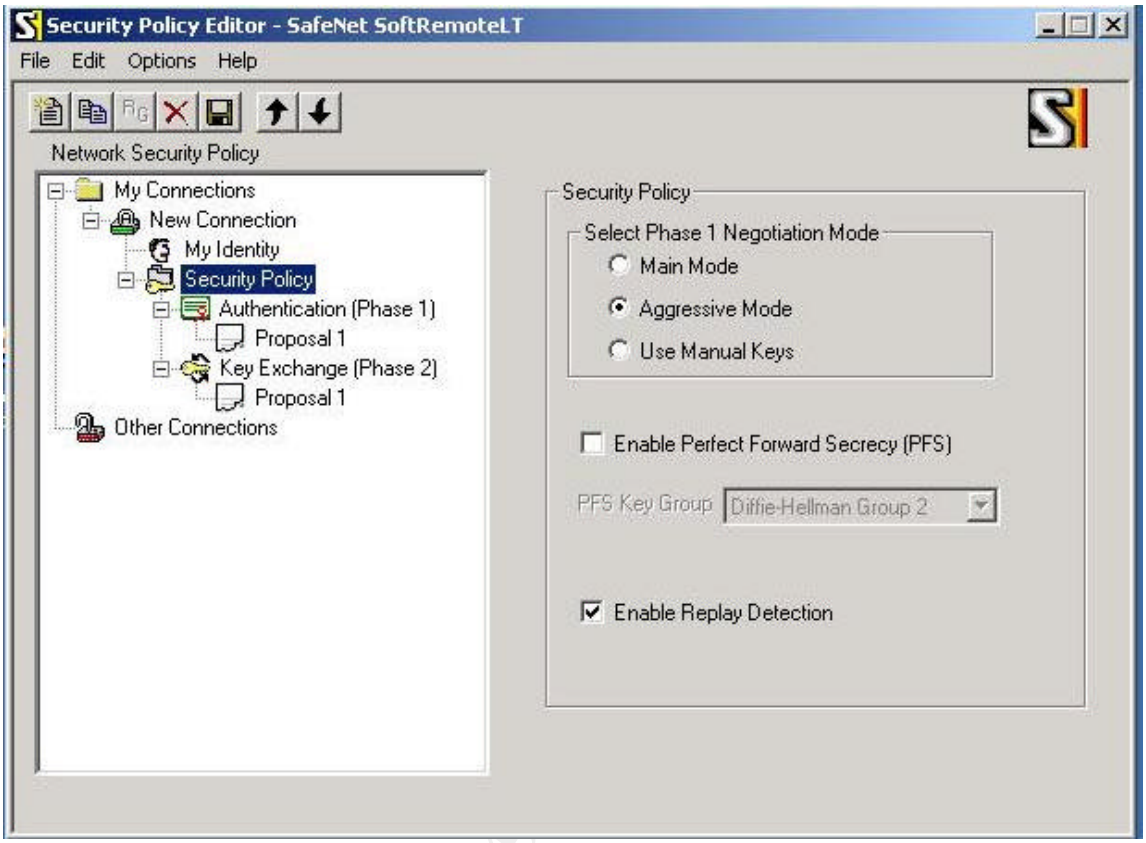


Figure 3: Safenet Client configuration

Next, he started Cain's sniffer utility. With the sniffer running, he attempted a VPN session initiation to the campus's VPN gateway. Since the pre-shared key was still unknown at this point, the VPN connection attempt was expected to fail. Cain captured the traffic created during the connection attempt.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

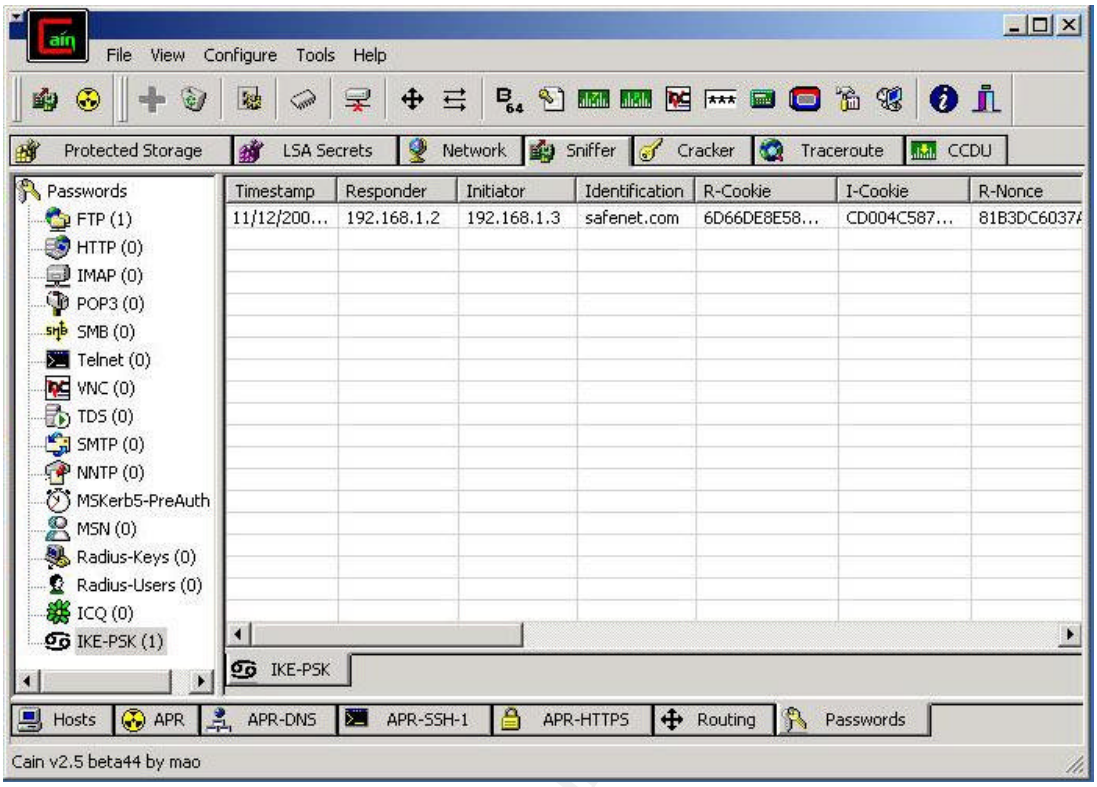


Figure 4: Phase 1 Information Derived by Cain Sniffer

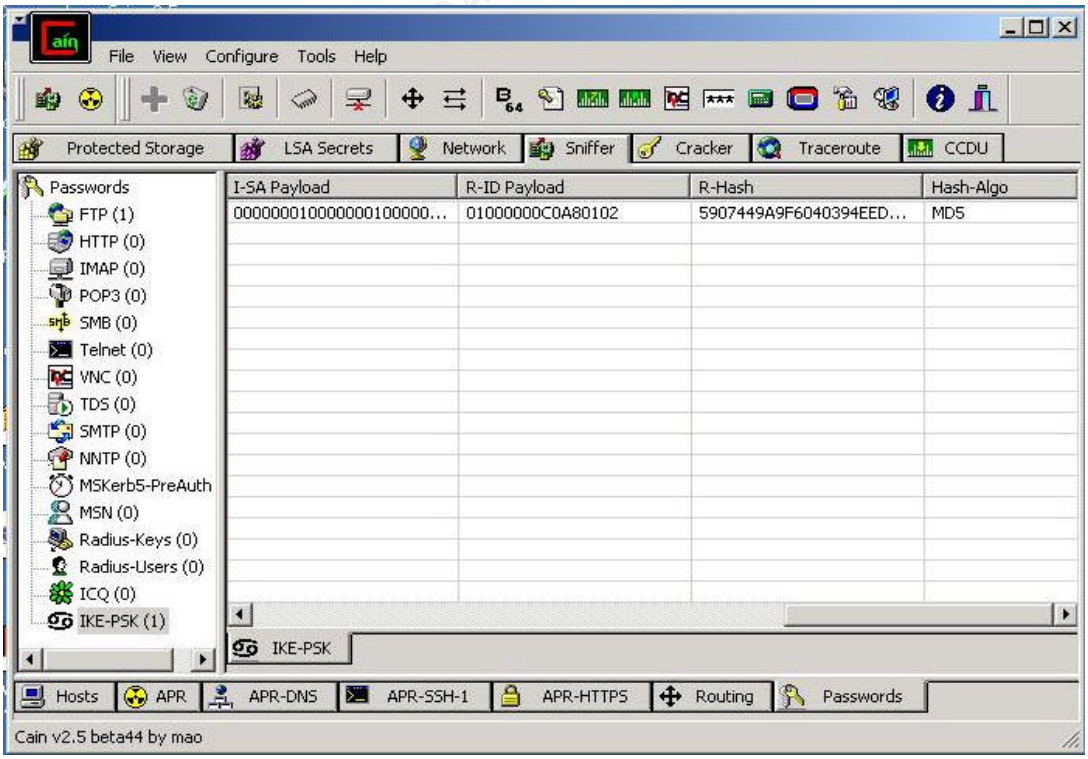


Figure 5: Cain Sniffer Capture Including the Responder's Hash Payload

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Now that the phase 1 response from the gateway has been captured by the Cain sniffer, the capture can be sent to the cracker utility.

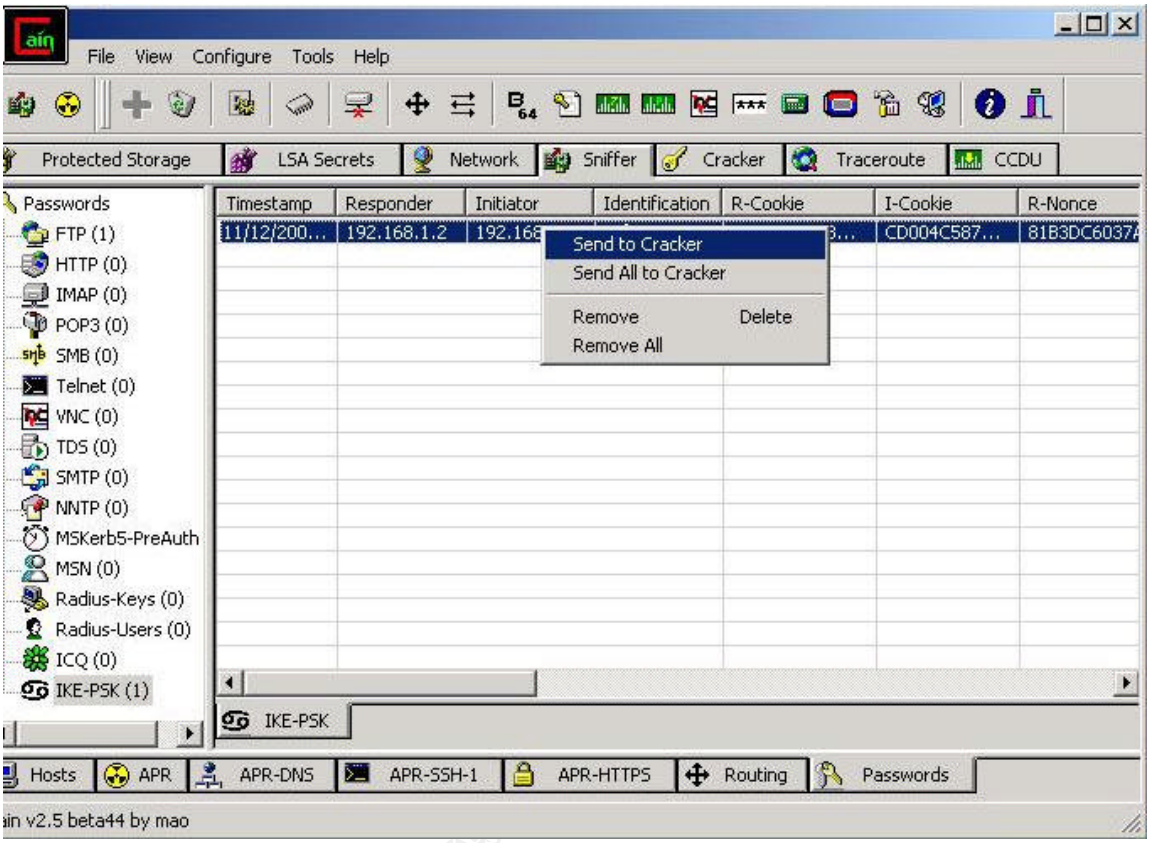


Figure 6: Cain Cracker Utility

The Dictionary attack was chosen for the first attempt at cracking the pre-shared key. Mark expected that the pre-shared key might be something easy for remote users to remember. If that didn't provide results, he would next try a brute force attack.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Dictionary attack is started using Cain from the following screen:

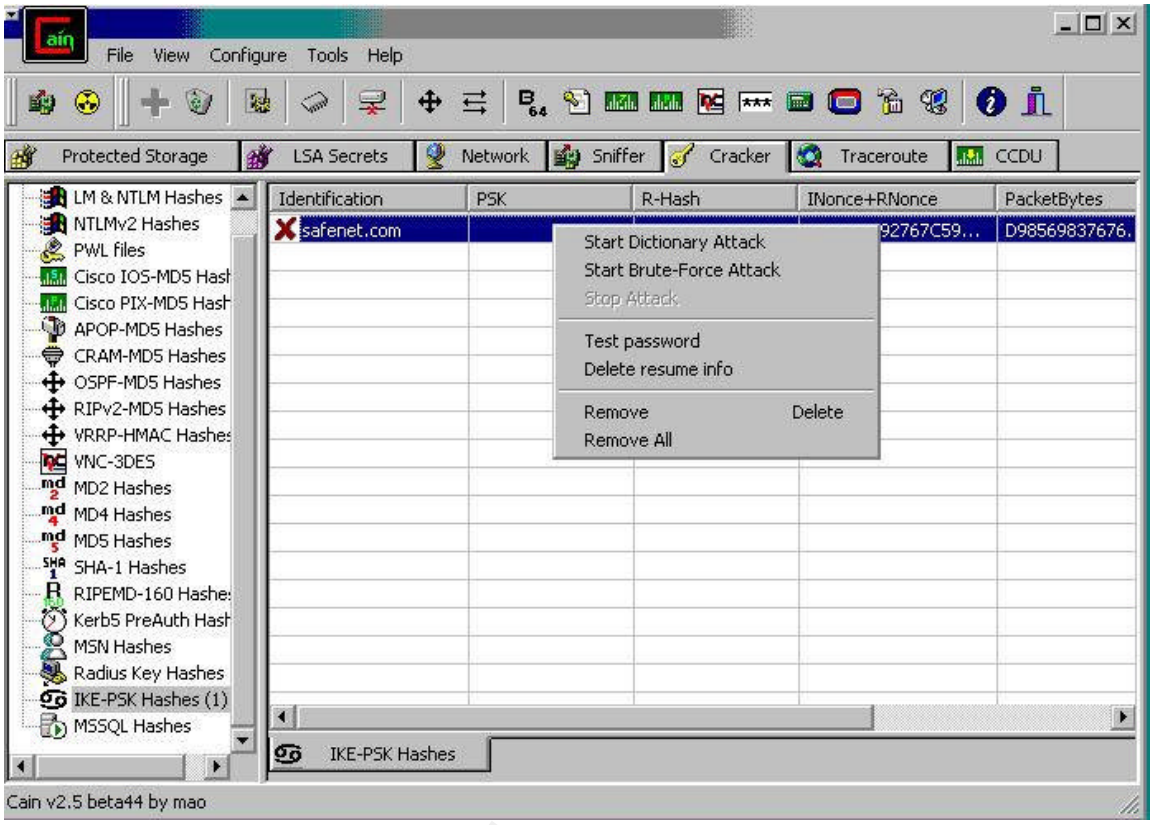


Figure 7: Cain Cracker Utility Details

At this point all there was to be done was to let the cracker run. Every couple of hours Mark checked the progress of the cracking process. He was running the cracker on a mediocre machine, so he expected it to take to time.

© SANS Institute 2004,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Eventually, Cain arrived at a result: abandon

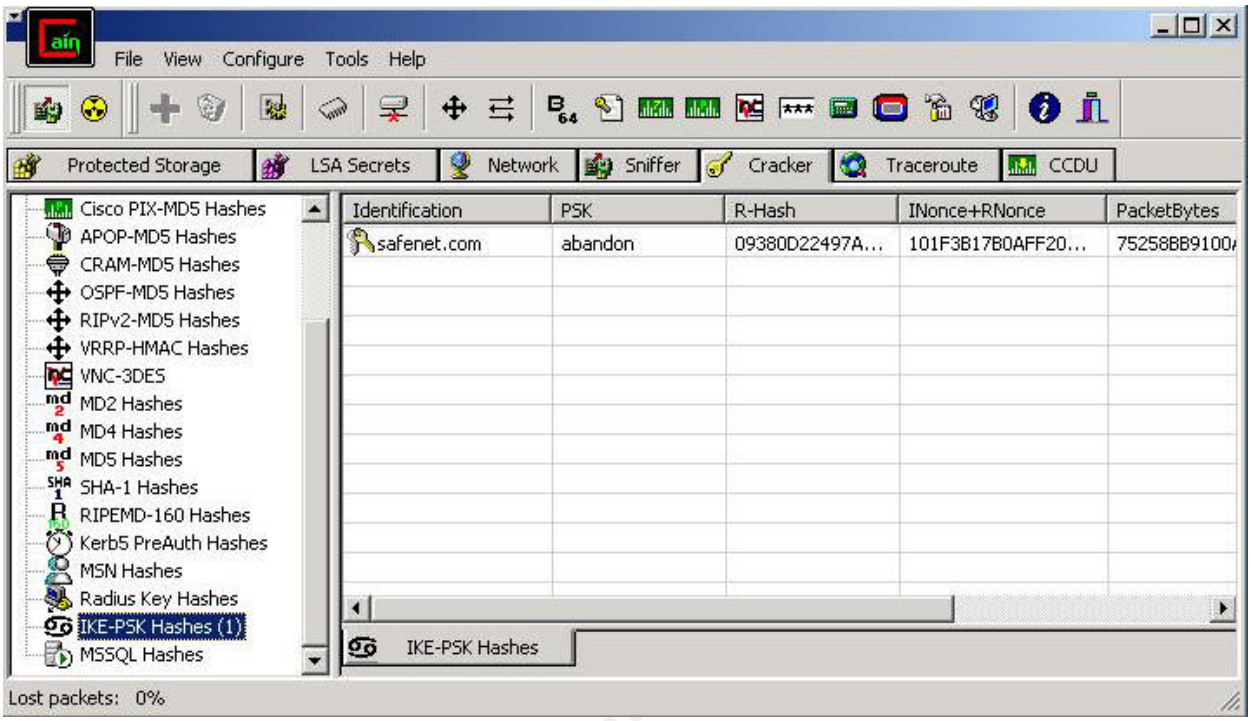


Figure 8: Cracked Pre-shared Key

Now, Mark had the all of the information he needed including the pre-shared key. Mark did not have any information about the remote network protected by the VPN containing the Admin server. He had found simple diagrams of the campus network on the University's web site, but no details about the Admin subnet. The .SPD file he had copied showed " virtual adapter preferred" under the "My Identity" submenu. This indicated that the typical remote client configuration provided to university subscribers used Mode-Config to provide the Safenet Client with a virtual IP address assigned to the client by the router from its client configuration IP pool. Mark guessed that the virtual IP address assigned to the client would belong to the admin subnet. He again attempted to initiate a tunnel by pinging a random address:

Ping 192.168.20.6

Now that the pre-shared key was entered, the ping traffic caused Phase 1 to complete. After phase 1 completed, The Safenet client's virtual adapter icon flashed indicating that VPN gateway issued a virtual IP address to Marks VPN client. Mark used the command "ipconfig/all" to obtain the virtual IP address assigned to his virtual adapter: 192.168.7.50

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

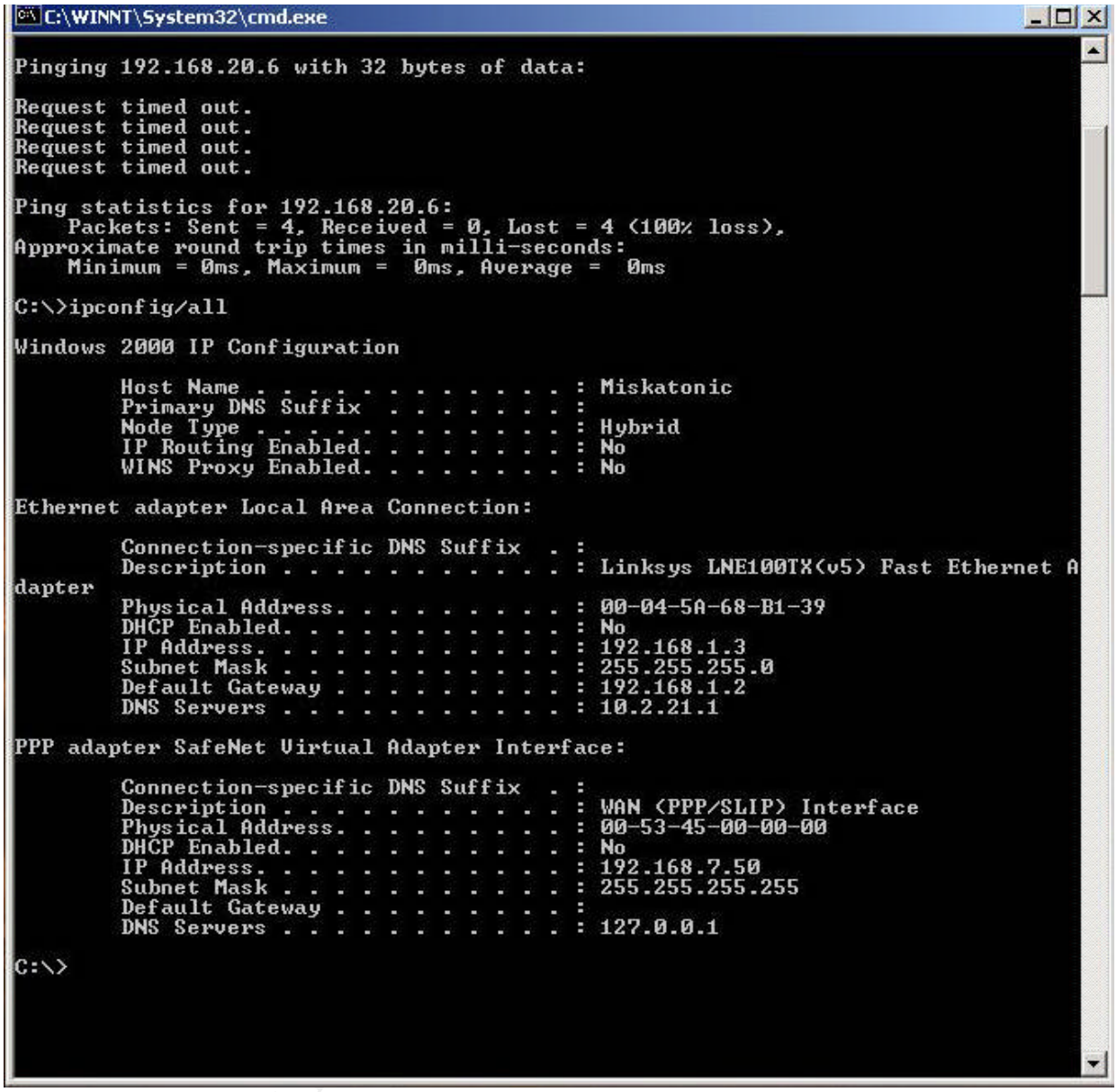


Figure 9: Real and Virtual Adapter IP Addresses

From the Virtual Adapter address, Mark made a guess that the Admin subnet could be 192.168.7.0. He had no clues as to the subnet mask. Sticking with simple guesses, he decided to try a 24-bit subnet mask.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Using this information, he adjusted the Safenet Policy as follows:

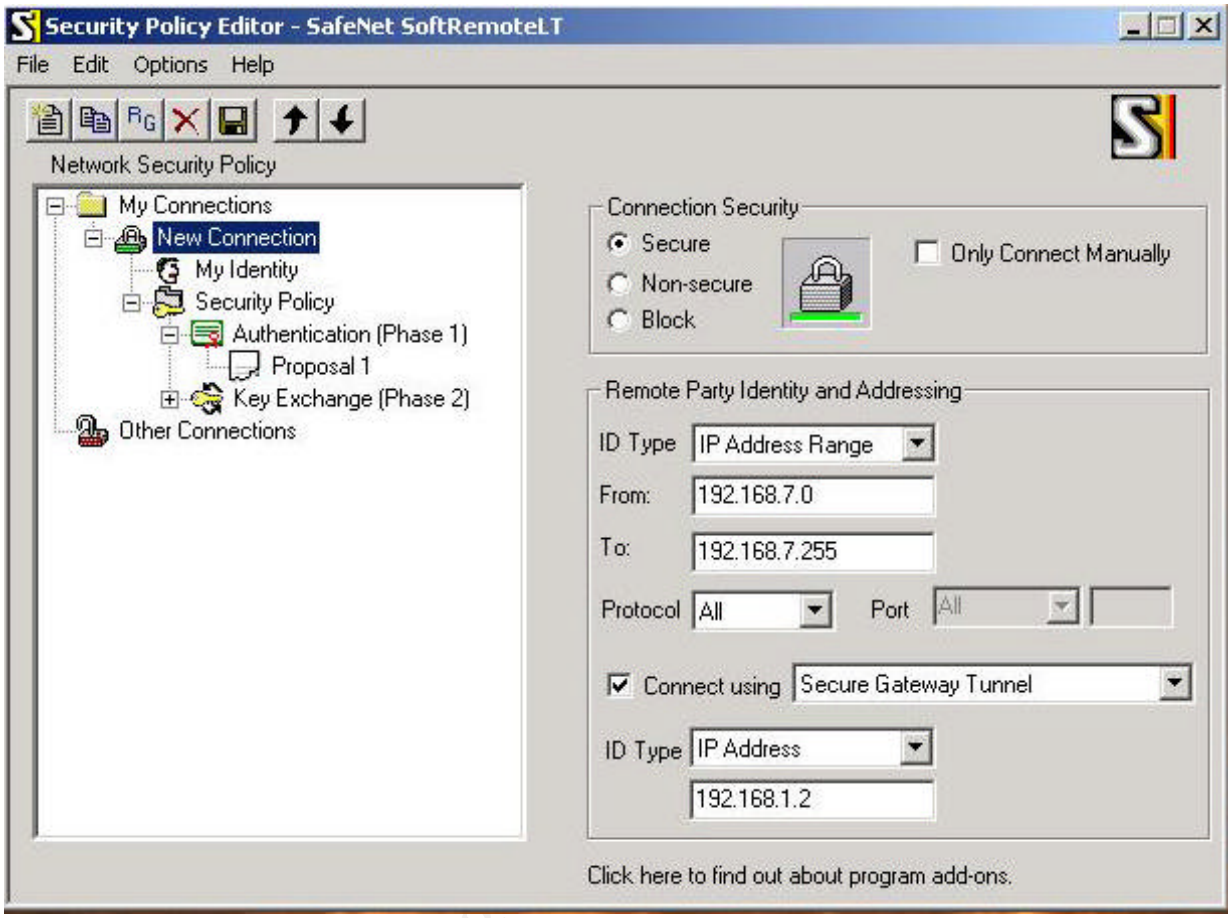


Figure 10: Safenet Client Remote Party Identity Configuration

Again, he attempted to initiate a VPN tunnel, this time using an address in the suspected range of the remote network. This time, after a series of unsuccessful pings, the Safenet Key icon flashed, indicated that phase 2 had completed.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The completion of the tunnel was confirmed by the Safenet connection monitor display:

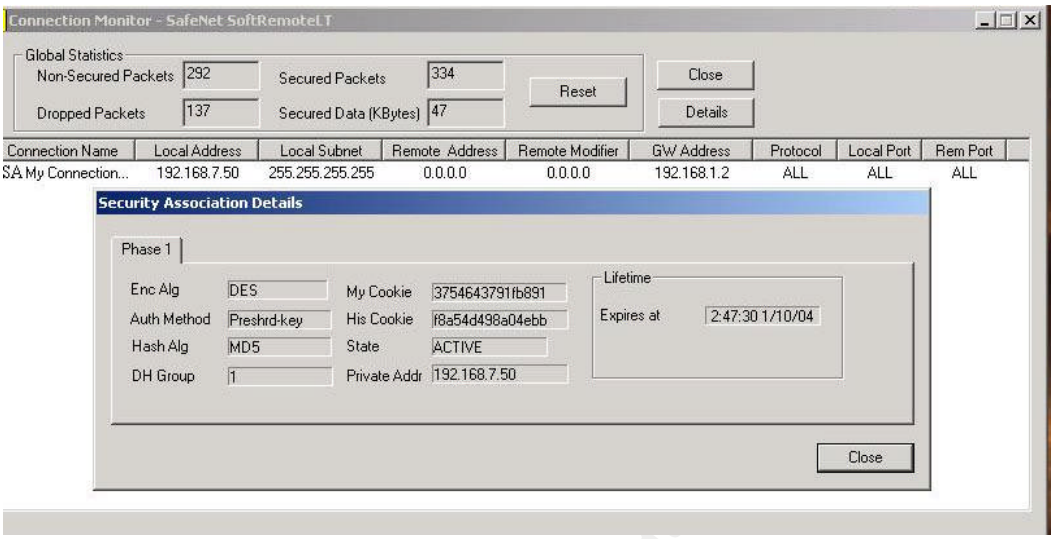


Figure 11: Safenet Connection Monitor

He was logged into the internal network. He ran Superscan to see what was there. A half dozen machines were revealed. Most were Windows XP PCs. A few appeared to be Win98 desktops. One particular machine attracted his interest. A server with IP address 192.168.7.34 appeared to be a WIN2000 server running a variety of services:

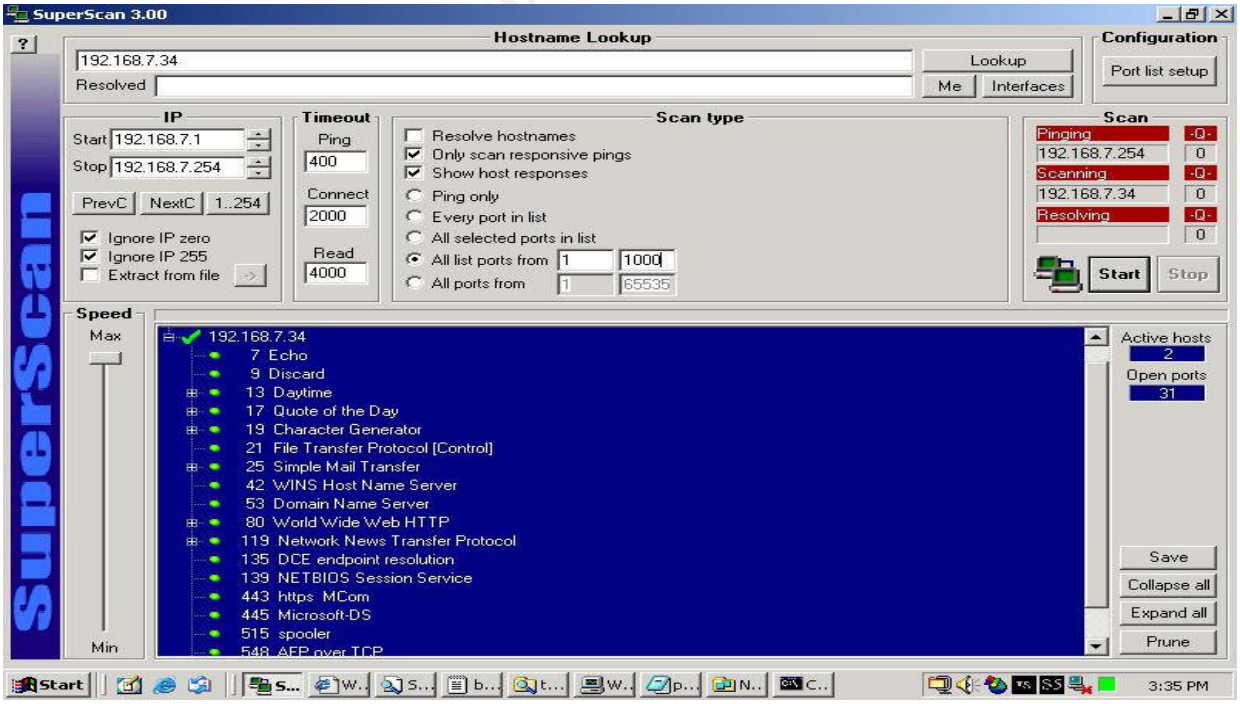


Figure 12: Superscan Results

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

He then used the Tigertool's Sitescan tool to examine the services more closely. (20)

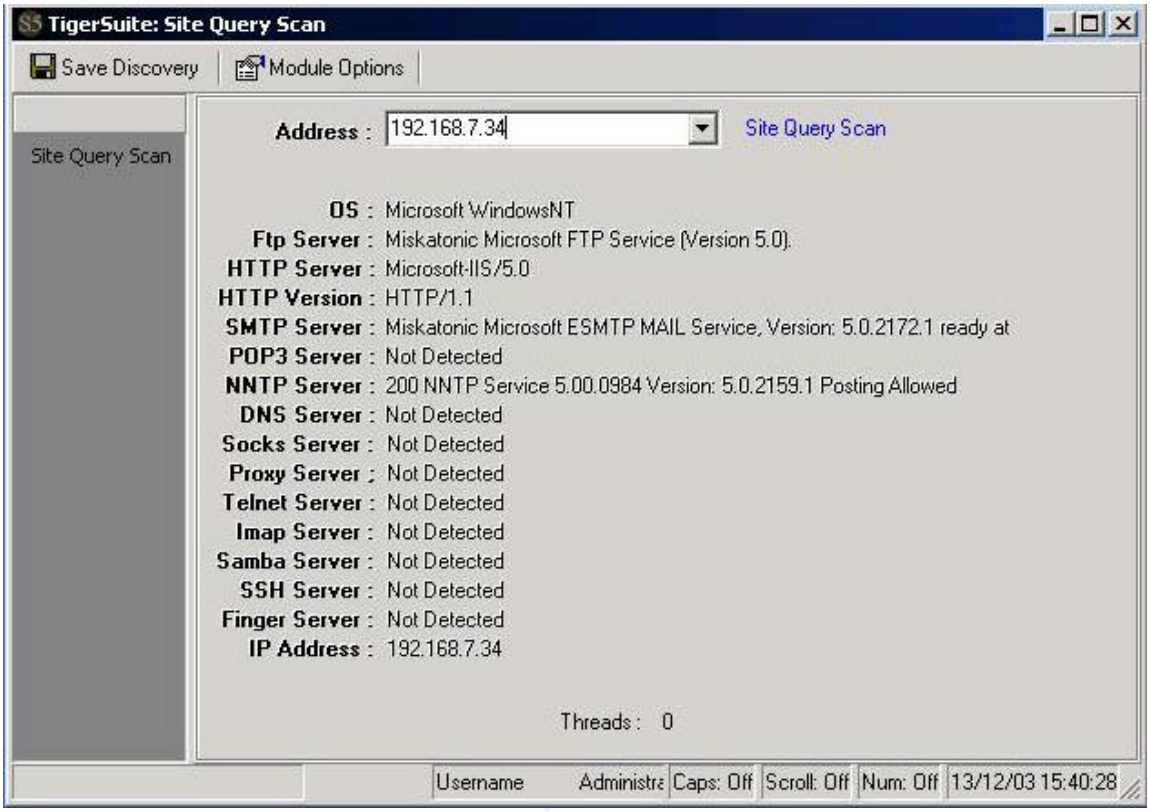


Figure 13: Results of TigerTools Site Scan

The WIN2000 server was running a multitude of services. DNS, HTTP, SMTP, and many other services were revealed by the site scan. It looked like someone had performed a default install. The machine had the WIN2000 FTP service running. Now that Mark had access to the network and identified a target machine, he decided to attempt a null user session.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Using Enum –S 192.168.7.34 he obtained a list of shares:

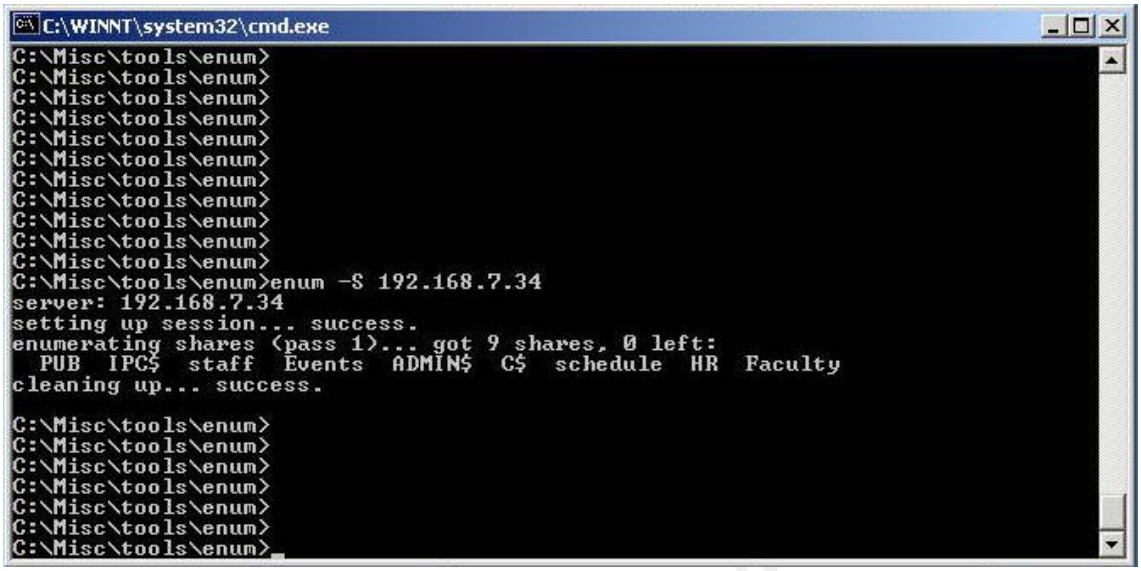


Figure 14: Shares Discovered by Enum

Using Enum –U 192.168.7.34 he obtained a list of users

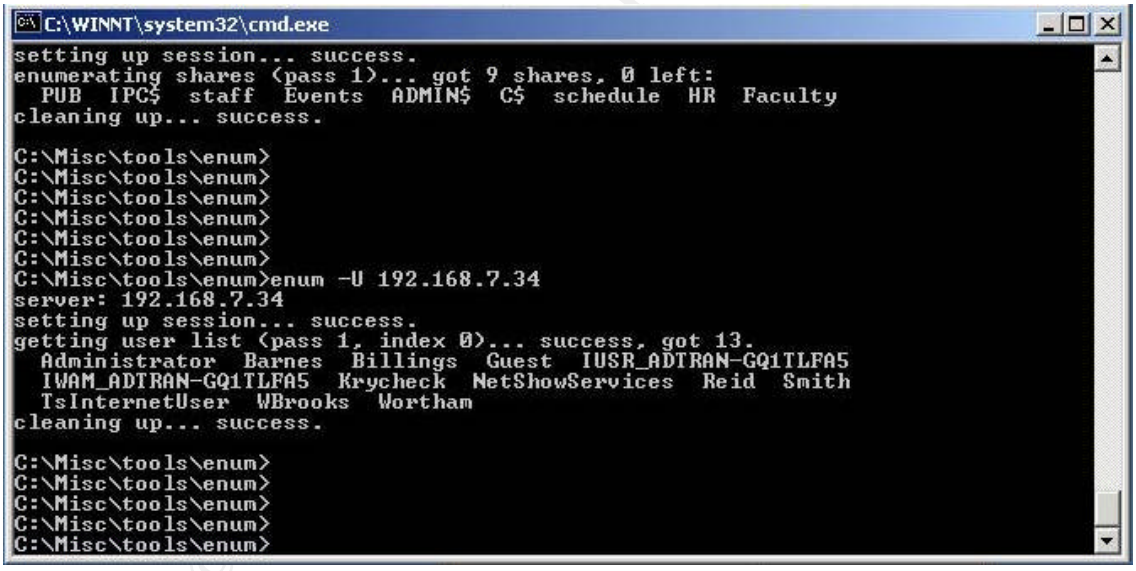


Figure 15: List of Users Discovered by Enum

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Using Enum, he queried the password policy configuration.

Enum –P 192.168.7.34

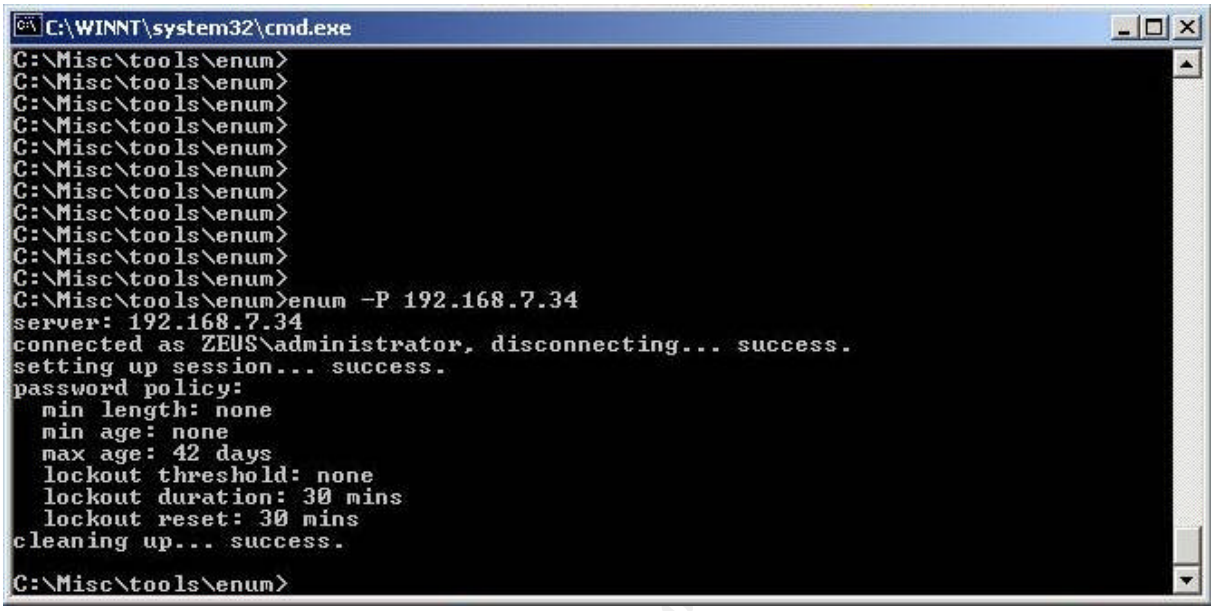


Figure 16: Password Policy Discovered by Enum

He could tell that no OS hardening had been done. There was no password lockout, and no failed login threshold, which meant system services might be vulnerable to dictionary or brute force attacks. Mark had several FTP brute force utilities including the STCtools and Tigersuite FTP brute force tools (20). He decided to try using Enum to get the Administrator password using the Tigersuite dictionary:

Enum –D –f c:\pitts\tools\enum\dicfile.txt –U Administrator

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Enum started trying the various entries in the Tigersuite dictionary. After several thousand entries, it found a match: 0charon

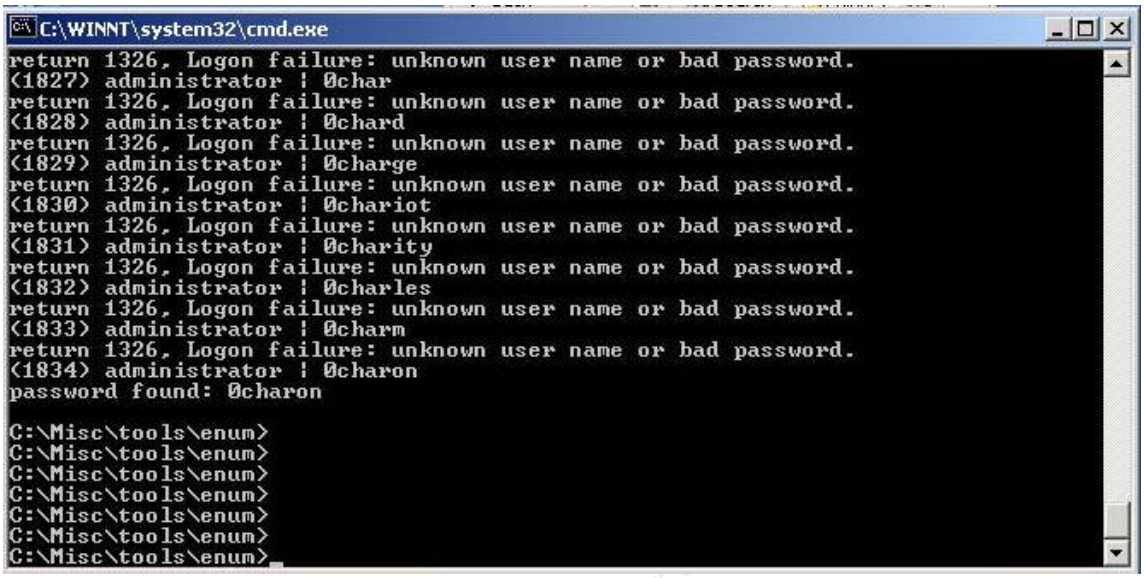


Figure 17: Successful Dictionary Attack on the Administrator Account

Next Mark mapped the remote drive:

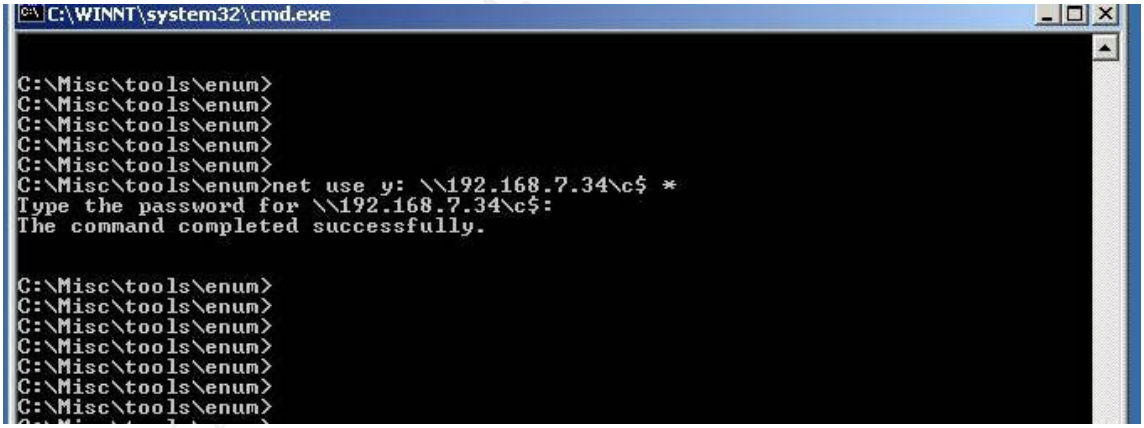


Figure 18: Mapping the Remote Drive

When prompted to enter a password, he entered “0charon”. Now Mark had access to the hard drive of the record server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

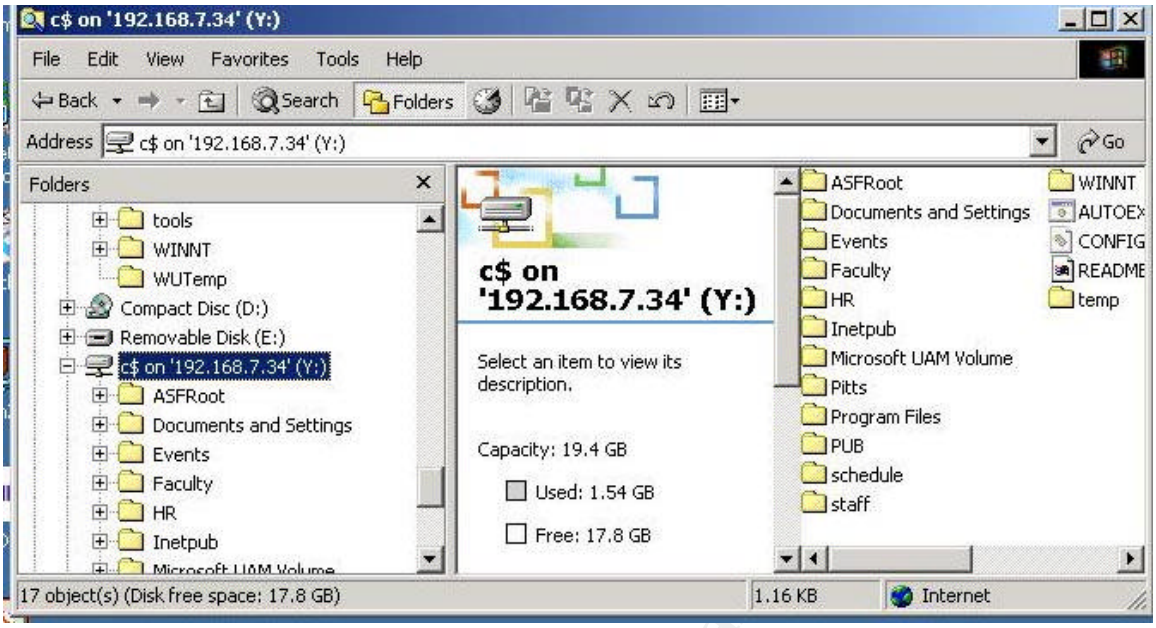


Figure 19: Explorer View of Remotely Mapped Drive

He went to the faculty folder and found folders belonging to various departments including Computer Science, Engineering, and several others.In the Computer Science folder he found Dr. Krycheck's folder and inside located:

EmbeddedSystems_Section_12.03

Inside the finals folder, indexed by his class section number, he found an Excel spreadsheet similar to printouts he had seen in Dr. Krycheck's notebook containing the grades for the class for the entire semester. He made a couple of quick calculations. He didn't want to be too obvious. He changed the final exam grade slightly and then changed the final grade. He thought, no one will notice. Dr. Krycheck is not going to review posted grades. He changed the spreadsheet and restored it to the Y: drive.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Keeping Access:

Having accomplished his goal, Mark assumed that he did not need get back into the network. However, he decided to save the information he had collected just in case. He saved the user account information he had obtained from Enum. These were copied onto a floppy. He also stored the preshared key for the internal VPN gateway as well as its interface IP. Mark also knew how to use Pwdump. He made a DOS batch file with the simple command:

Pwdump3 192.168.7.34 pwfile

He created a folder on the remote drive called temp2 and saved the batch file into this folder. He also placed the Pwdump utility in this folder. Next, he clicked on the batch file to execute it.

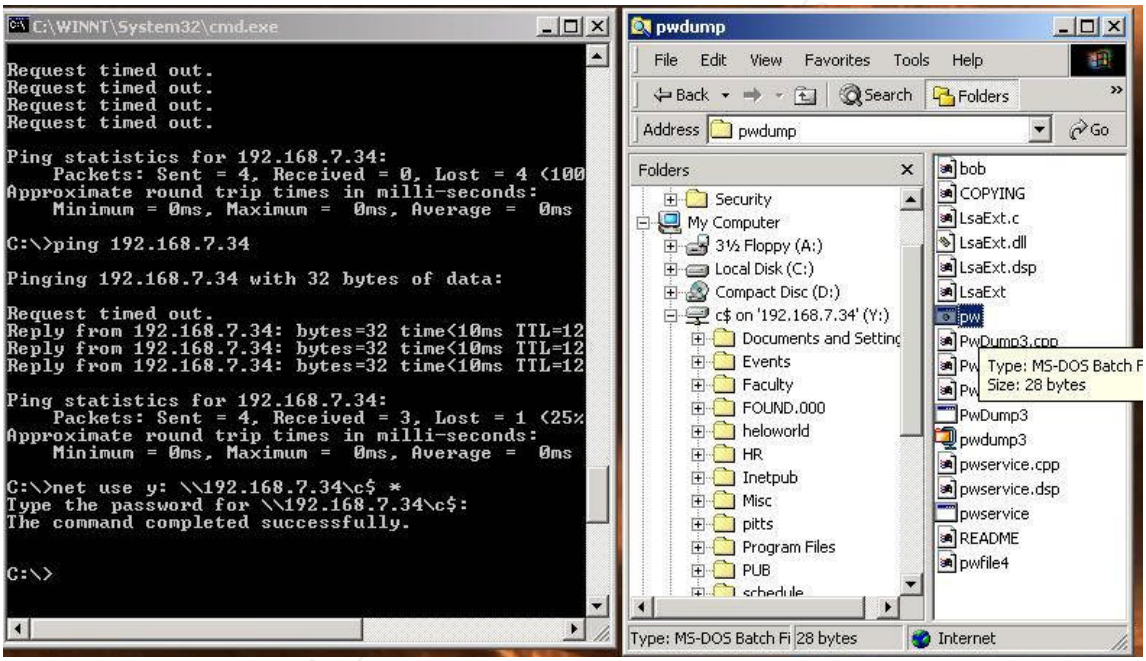


Figure 20: Running PWdump Remotely

The command in the batch file created an output file called “pwfile” containing the hashed passwords from the target machine.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

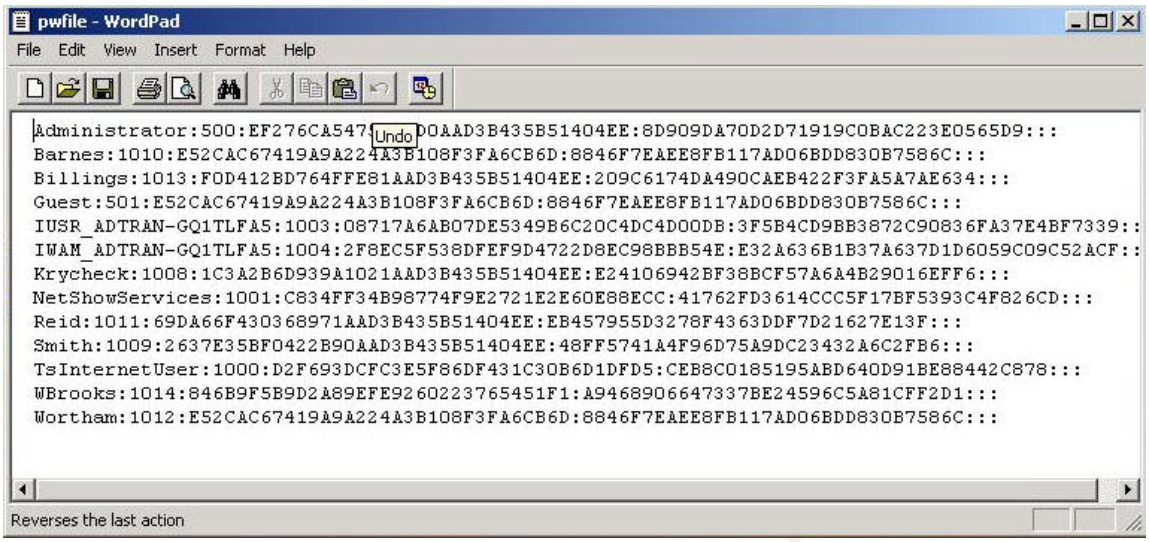


Figure 21: PWdump Output Containing Password Hashes

He had considered several other means of keeping access such as loading a simple Trojan such as Netbus, or setting up a Netcat process to shovel shell through the task scheduler. Mark's main goal was to quietly fix his grade problem and get back out of the network, minimizing any traces of his intrusion. He also had no motivation to carry out any other exploits on the University network. For these reasons, he decided not to install a backdoor or rootkit on systems he had accessed.

Covering his tracks:

His work now done, Mark set out to remove traces of his network intrusion. He deleted the Pwdump utility from the remote drive. He started removing the various tools including IKEprobe, IKE-scan, Cain, Enum, STCtools, PWdump and the Safenet VPN client software from his laptop. About that time, Mark heard the noisy chatter of some students headed into office area. This was somewhat unsettling, and a complete surprise. Suddenly, two students walked in to the cubicle. Mark asked them what they were doing there. One of the students answered " Hi. My name is Ricardo. I am starting graduate school here and this is the office that was assigned to me. Great…it looks like I already have a live Internet connection". Mark replied, "Yeah, the jack is hooked up and works fine. The office looked vacant, so I just borrowed it to get some last minute studying in. I'll get out of your way. Give me 5 minutes". They wandered off down the hallway. Somewhat rattled, Mark quickly scanned over things trying to remember where he was and quickly closed out the open application windows. He unplugged his laptop and headed over to the computer lab to remove the spanning port and the cable. The new students had congregated in the computer lab with a faculty member who seemed to be giving an impromptu tour. He felt suspicious entering the network room, and decided to come back later to remove the Ethernet cable and the spanning port config he had set up. Thursday evening, about 9:30, he went by the computer lab, and went into the network room, peeping in first to make sure no one else was around. The door was locked. He thought for a moment. Slightly perplexed, he decided there was nothing

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

left to do. It was uncertain at this point if the locked door indicated that someone had noticed evidence of tampering, but the locked door was disconcerting.

Incident handling process:

Preparation:

The university was required by law to have a security policy. (21) The policy was intended to protect the integrity of student records and keep this information confidential and to prevent the use of university computing resources from being used to attack other networks while providing high availability and relatively open access to academic resources. (22) The primary responsibility of implementing the security policy of the university was placed upon the IT staff. The IT staff recently pushed an effort to develop an Incident Handling Plan. A rough draft of a response plan was developed. The response plan standardized procedures for handling various types of security incidents, and helped build a framework for coordinating efforts during incidents. The Incident Handling plan called for the creation of an incident handling team. The team comprised members of the IT staff, system administrators, HR, legal staff, and the campus physical security office. The Security Policy was approved by the University's Board of Directors. Members from each department contributed information used in a security assessment performed by the security team. The security assessment was used to identify assets, risks, and vulnerabilities. Although it was the primary responsibility of the IT staff to manage security of the campus network, the security policy called for co-operation with systems administrators. The security team was provided with access to all of the universities network devices including routers, firewalls and, servers. The campus security office helped ensure that areas requiring restricted access were properly secured. Campus security was also called in to investigate equipment theft or tampering. A member of the incident handling team was responsible for providing information about incidents to management and the press, and coordinating efforts with law enforcement. An important component of the response plan was a communications plan. The communications plan was created to help coordinate efforts and involvement of key team members during an incident. Each department was provided with contact information for everyone in the security team. Key members of the IT staff and security team were designated as Incident Managers and were provided with cell phones and pagers. Lists were maintained containing contact information for the security team, system administrators, relevant faculty and staff. The IT staff designated an incident manager for each shift and key security team members were on call 24 hours a day. Information was provided to key faculty and staff in each campus department providing guidance in identifying suspicious activity and who to contact during such events. Basic security training was provided to relevant University staff. Management had approved funding for more specialized training for members of the security team, but this had not yet occurred.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Some relevant aspects of the Universities Security Policy are described below:

The policy provides escalation procedures dependent on levels of severity of the incident (23). It is the responsibility of the Incident handling Team to classify events as incidents and decide what actions to take.

Level one incidents:

Includes lost passwords, and virus infection are responded to with minimal urgency.

Level two incidents:

Includes stolen passwords. These events are responded to the same day.

Level three incidents:

Includes illegal system access, physical or via the network, network service outages, tampering of student records, and theft or damage of property. These incidents have highest priority. Incidents that violate the confidentiality and integrity of student records and financial information are considered criminal acts. These incidents are to be investigated by law enforcement. Prosecution involving theft and/or damage of campus computing assets is subject to the discretion of the Incident Handling team.

The security policy mandates a backup plan for mission critical servers and databases containing student record and financial information. Backups are performed during low system utilization periods (weekends) utilizing off-site backups.

Ethernet Hubs are to be replaced by switches to reduce the likelihood of sniffing,

Servers and workstations are to be upgraded and patched when new releases are available.

All Internet access passes thru a router/firewall, which serves as the primary perimeter defense. Publicly accessible servers such as web-server, and FTP server are situated in a DMZ.

Firewalls, Routers and Servers are configured to store log information using a Syslog server. Periodically, logs are reviewed by the System Administrators. Events found in the logs are to be scrutinized according to the security policy.

Time settings in network devices are to be kept up-to-date in order to maintain accuracy of log information.

Telnet is not allowed for remote management of routers and the VPN gateways. This is performed either locally using the console, or via SSH.

All areas containing networking equipment used by the campus are to be physically secured.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All remote access to student record and accounting servers is protected by a VPN. This included off-campus access, as well as on campus access from other buildings. X-Auth using RADIUS was used to authenticate external VPN access.

Identification:

Monday 3:00 PM

Wendy Sanders was trying to log into the Remote access VPN and was having problems. Marty ended up getting a call from the help desk asking for him to look into it. Marty logged into the Syslog server and skimmed through the stored 3305's Syslog output. In addition to system events, the 3305's Syslog recorded failed VPN connection attempts. Marty expected to look at the event log and find the failed connection attempts. Next, he would turn on the IKEtrace debugging utility, have Wendy re-attempt a connection and look at specific debugging information generated by the connection attempt. Managing the 3305 was exclusively Marty's responsibility, but he was very negligent about reviewing the logs. Subsequently, the log file had grown quite large. Marty scanned through the log looking for the most recent entries. As he scanned through, he noticed an unusual number of failed connection attempts that occurred in rapid succession:

```
2003.12.09 14:05:21 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
2003.12.09 14:05:21 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed
2003.12.09 14:05:22 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
2003.12.09 14:05:22 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed
2003.12.09 14:05:25 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
2003.12.09 14:05:25 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed
2003.12.09 14:05:28 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
2003.12.09 14:05:28 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed
2003.12.09 14:05:30 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
2003.12.09 14:05:30 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed
2003.12.09 14:05:33 CRYPTO_IKE.NEGOTIATION 300: IkeSelectIsakmpProposal failed
```

At first, he reasoned that someone might have forgot the correct settings for their VPN client and in a pinch they decided to try various parameters looking for a match. Still, this seemed very suspicious. All remote access users received a SPD file from the IT department when they registered for an account. The user loads the SPD file into the Safenet VPN client policy manager utility. The SPD file had all essential parameters pre-programmed in. The pattern discovered in the log file resembled a brute force attack, but Marty was not familiar with a VPN brute force attack. He had spent the majority of his time learning how to configure and maintain the systems he managed and very little time studying malicious code and exploits. This traffic occurred on the public interface of the remote access VPN, so it might not be surprising if it was some kind of scan, Marty reasoned. Marty notified the on duty network manager and sent a copy of the Syslog output via e-mail. He decides to do a little research on the web about VPN vulnerabilities.

Tuesday 3:00 PM

The help desk received a call from a lab instructor in the computer lab in the engineering building complaining about poor network performance on the engineering

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

building's VLAN. This was assessed as a level 1 priority and logged in the help desk dispatch system. An IT troubleshooter was assigned to look into the matter.

Wednesday 9:00 AM

Eric is a new employee of the campus IT staff. He is generally called in on desktop problems and basic networking issues. Eric is assigned to look into the issue called in by the lab instructor yesterday. He can't find the lab instructor to ask questions about the problem, so he decides to take a look at the VLAN and the switches that support the building's VLAN. He notices, to his chagrin, that the network room door is unlocked. The network rooms also contain some power distribution equipment and breaker panels and it seems that some facilities staff have a bad habit of leaving the network rooms unlocked. He logs into the console of each switch to examine the configuration. Being essentially configured as flat switches, the configs for each port are nearly identical so when the spanning port showed up in the list, it was an obvious exception. The spanning port may have been configured by someone else from the IT department for troubleshooting purposes, but, the fact that the port was physically routed to a jack connection located outside the network room was very suspicious.

Eric took a quick look at the patch panel and traced the spanning port connection to jack 347B. A diagram on the wall indicated the jack was in one of the temporary offices. He decides to go take a look in the office. Eric finds Ricardo and a friend in the office running some Matlab equations on their desktop computer connected to jack 347B. When questioned, Ricardo mentions that he just moved into the office late Tuesday night. The jack was already active when he moved in. Most interestingly, another student claimed to be using the office temporarily and was using a laptop computer connected to the network jack. Ricardo indicates that he had seen the student around the campus and in a few classes over the years, but he did not know his name. Ricardo genuinely appears to know nothing about the spanning port. This seems very suspicious to Eric since it is beginning to look like the student may have been up to something. He saves a copy of the switch config to a TFTP server maintained by the IT department, removes the spanning port config from the switch and leaves, locking the door behind him.

Wednesday 10:30 AM

Eric gives the information about the spanning port and the unlocked network room to the security team. The event is declared an incident and assigned a level 2 priority. This information is dispersed to the rest of the security team, which includes Marty. Marty draws a connection to the VPN scan he saw on the public VPN interface. He decides to have a look at the internal VPN gateway logs. The security team assigns several members the task of verifying physical security of the network rooms in the campus buildings. They also check for spanning port configuration in switches in other buildings on the campus.

Wednesday 11:00 AM

Marty checks the Syslog generated by the internal VPN gateway and finds similar entries indicating a rapid succession of failed connection attempts, followed by a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

successful connection. During his search on the web, Marty has found information about IKE enumeration and scanning tools. He also found the IKEscan tool, the CERT advisories for the aggressive mode brute force attack, and the paper about IKEprobe. After quickly reading through the first few pages of the document, he realizes someone has been using this attack on the university's VPN network. He contacts the on duty network manager and relays the information. He also makes copies of the log files from both VPN gateways and the switch spanning port config file.

Wednesday 12:30 PM

The event classification is quickly escalated from a level two event to a level three event. The on duty manager agreed with Marty that since the IKEprobe and resulting connection occurred on the internal network that illegal access to the school's administrative network was likely the target. A quick meeting is called for the security team during which Marty gives a brief summary of the evidence obtained so far. The systems administrator of the admin server is contacted an alerted and advised to review event logs and look for unusual activity in the student records server. Marty is assigned primary incident handler since the incident is focused on equipment with which he is most familiar.

Wednesday 2:30 PM

After scanning the event logs and examining records folders, the systems administrator finds an unusual file in the folder containing grade records for section 303 of Dr. Krycheck's class. She also notes that a record belonging to one particular student was modified several days after the others in the class and was modified at 10:00 PM, which is a somewhat unusual. She discusses this information with the security team. Marty quickly finds a time correlation connecting the Internal VPN gateway IKEprobe, the successful connection and the file modification.

Wednesday 4:30

A meeting is called for the security team and members of each campus department included in the incident handling policy. Marty presents the evidence and information about the incident using some basic network diagrams and a synopsis of the attack mechanisms. New evidence provided by the system administrator of the student records department shows that a particular student's records were altered. Comparing the records contained in the backup made 12/7 to the file altered 12/11, it is clear that one student's final exam grade and overall class grade was adjusted upwards. The initial assessment made by the team identifies several notable characteristics of the incident:

a) The attack was at least first attempted through the remote access service and was later carried out using the internal VPN network. Something will have to be done very quickly to isolate the network to prevent further intrusion.

b) The attacker seems to have some degree of skill and understanding of VPN networks and may be prepared to employ other schemes against the campus network.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

c) The purpose, so far, appears to have been to alter student records, which is a major security violation.

Marty and Eric are responsible for establishing a chain of custody. They began collecting and preserving evidence. The primary evidence was the tampered file in the student record server. The network connection of the server was disconnected from the admin network and re-connected to a hub. Two complete backups of the hard drive are made over the network to another machine connected to the hub. A second copy of last weeks backup is made to be stored with the evidence. Files containing the Syslog output for both the external and internal VPN are copied and stored. Copies of the altered switch config are also stored. Evidence collected is labeled and stored in a secure area in the operations building which contains much of the campus network facilities.

Containment:

Wednesday 5:30 PM

An emergency meeting was conducted including the incident handling staff and the campus Security team, The Dean of the engineering dept as well as a representative of the school's student records office. A discussion was held concerning the incident, the implications and what actions to take. The system administrator of the student records department again presents the evidence of tampering including the spreadsheet of grades from Dr. Krycheck's class, comparing the original contained in the backup to the altered copy made on 12/11. The unusual file discovered the folder is also presented to attendees. The Dean offers additional evidence, stating that Dr. Krycheck had left to go to a conference by 12/6 and probably did not make the alterations. It is agreed that Dr. Krycheck should be contacted and asked about this particular student.

Shutting down the VPN service was somewhat of a problem being the end of the semester, since some faculty and staff might still be trying to use it. Nevertheless, the conclusion was that something had to be done right away and the student records administrator insisted that VPN access through the private network to the admin network be closed temporarily until the problem could be solved. The public VPN was also considered vulnerable and would be temporarily shutdown as well. The network link between the admin network and the campus backbone will be shutdown temporarily until the systems on the admin network can be examined. The link is disabled by administratively shutting down an interface on the backbone router. This isolates the admin network from all external access. Due to the evidence of tampering of student record information, it was decided that an audit of the grade system should be performed which mandated the need to scan hundreds of student records at a significant cost to the university. It is also decided that a full investigation should be launched to determine the extent of the intrusion into the private network.

At this point Marty has studied the VPN aggressive mode brute force attack and understands exactly how it works and what could be done to eliminate the vulnerability. The sys-admin has also begun scanning the files containing grade records using a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

backup of the compromised server database. At the meeting, Marty offers a general description of the aggressive mode pre-shared key attack, and announces that he is working on a solution. Members of the security team are now assigned various tasks of the containment phase. As part of the development of the Incident Handling plan, a list of materials to be used in a Jump Kit is created. The following items are contained in the list:

Jump Kit Contents:

Dual boot Laptop with Winn2000 operating system and Redhat Linux
CD burner
Blank CDs
2 blank formatted 40 GB hard drives
2 portable 4-port hubs
1 6-outlet power strip
5 10ft Ethernet cables
2 Ethernet crossover cables
Digital camera
2 64 meg USB flash drives
1 128 meg flash drive with software tools:

TFTP server
FTP server
Ethereal
WinPcap
Cain
Enum
NMAP
Pstools
Various port scanning utilities
Pwdump
SAMdump
John

Contact lists
Floppy disks
Permanent markers
Command and install summaries for misc tools including Netcat, NMAP, and others.
Install CDs for Win2000, Professional, 98, NT and Linux.
Bootable floppies for several OSs

The engineering building network room is closely examined to determine if any additional backdoors, network taps or other eavesdropping mechanisms have been introduced. None are found. Earlier checks of switch configurations in switches located in several campus sites have revealed no evidence of tampering. Both the Internal and external VPN gateway configurations are examined and compared against backups.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Several router configs, including the main backbone router, are checked for new or altered passwords, accounts and access-lists. It is decided that after making two complete copies of the hard drive, the main student records server will be rebuilt with a new drive and restored from last weeks backup. The backups are sealed in poly bags labeled and given to Marty to be stored with other evidence obtained during the incident handling process. All other machines on the admin network are scrutinized for new or altered passwords, accounts and shares. The systems are also checked for evidence of backdoors and Trojans.

Wednesday: 5:45 PM

Marty went to the Admin building and to the server area, logged into the 3305 used for the internal and external VPN and administratively shuts them down. He also shuts down the interface containing the link to the admin network.

Wednesday: 6:00 PM

An e-mail was sent out to all faculty informing them that VPN access to the campus network was temporarily closed.

Thursday: 2:00PM

Teachers turning in final grades from all over the campus are hand delivering them to the Admin Building for entry into the database server. It's an inconvenient process, but it's getting done.

Thursday 2:30 PM:

Marty meets with the sys-admin to compare notes. It is observed that the successful connection to the internal VPN gateway occurs just minutes before the file in the student records server is saved. Marty also examines the unusual file found in the student record folder. It is the student records server password hash output of PWdump.

Thursday 4:30 pm:

A meeting is called with members of management from Human resources, security, the engineering department and IT to discuss the incident. Dr. Krycheck was contacted at the conference and confirmed that all of his grade were entered Friday 12/9. It was decided by the security team that the hacking incident potentially involved forgery, use of forged academic records, and criminal tampering, law enforcement will be notified as stipulated by the Security Policy.

Eradication:

The student records system administrator has reloaded the win2000 server from last weeks backup. Some recent changes to the student records files were lost and will have to be restored by hand. Marty has logged into both VPN gateways and deleted the pre-shared key assigned for the remote access accounts. Keeping restricted access areas locked has been a problem in the past due to a lack of security awareness and little or no monitoring. It is decided that keypad entry locks will be installed on network rooms and server areas. Default accounts are removed on switches, routers and other network devices and administrative accounts are re-assigned strong passwords. Members of the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

security team use Nessus to perform vulnerability scans of several important networks including the Admin Network. Results of the vulnerability analysis are used to harden the network. Several servers were found to have redundant and unnecessary services running. These were removed. All server accounts were audited. Default guest and anonymous accounts were removed and administrative accounts got new strong passwords. Updates are performed on critical servers including the campus DNS, FTP Web and admin network servers to make sure that the latest security patches are installed. Failed login lockup was employed using a threshold and time delay.

Friday 9:00 AM

A meeting is held with the head of the IT staff, the security team, the Dean of the engineering dept, and Marty to discuss measure to stop the VPN intrusion. Marty has done research on the aggressive mode brute force attack, and has some answers. " We have two problems. One is the use of aggressive mode. The information the hacker needs is sent in the clear. This information is sent by the gateway to anyone with a VPN client, weather they have valid login credentials or not. There are cracking tools available out there that can crack the pre-shared key this way. The second problem is my fault. I didn't assign a strong pre-shared key. There are two realistic solutions for supporting remote access with dynamically assigned IP addresses, which address our problem.

Option 1: use stronger pre-shared keys.

Unlike using strong passwords which are easy to forget, a strong pre-share key was fairly transparent to the VPN user since it was stored in the .SPD file that most users used to configure their VPN connection and not actually entered by the user. This approach did not eliminate the vulnerability, but would make brute forcing the pre-shared key much more difficult. This is fairly easy to implement, but would require issuing new .SPD files to everyone with remote access accounts. We just need to get a notice out on the website for remote users and informing them to get the new SPD files. Would also need to notify faculty and staff that use the internal network and get the new config out. Andy, head of the IT department quickly interjects: "we have to completely eliminate this thing. I am not going to be satisfied with just creating a stronger pre-shared key. They can still brute-force the pre-shared key, it will just take longer." Marty continued, " agreed!

Option 2: implement use of X509 certificates with Main Mode.

"This is the most secure solution and is used in enterprise networks to secure and authenticate network access. Using certificates with Main Mode allows connections from any IP address while protecting user-id information. This method totally eliminates vulnerability to the attack. We briefly looked into this when we first started setting up the VPN network. At the time, using certificates was deemed too expensive and too complicated. Most of the non-technical managers were totally puzzled by Marty's explanation of Public/private key encryption and X509 certificates. Now, since we have

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

a site license for WIN2000 server there is no associated cost with adopting this solution since we can use the Microsoft CA built into the WIN2000 server package that we already use. Using certificates for our VPN network is not too complicated to implement. We just have to set up a CA server and issue certificates to clients. It will be complicated to explain to users, but they don't have to know exactly how certificates work to be able to use them for VPN access. Also, we will need to let users know that they need to keep their PC clocks set correctly in order to use certificates.

Another benefit of using certificates is that we can revoke certificates if we need to, for example, when a student account expires create a Certificate Revocation List and put the CRL into the VPN gateway so it will no longer accept connection attempts from that certificate holder. It was decided that the best step to secure the VPN would be to implement digital certificates with Main Mode. Suggestions were made to simply add Xauth on the internal network since the existing Radius service could be used. Research showed that it is a bad idea to try to shore up a weak phase 1 authentication with Xauth as indicated in John Pliam's white paper " Authentication Vulnerabilities in IKE and Xauth with Weak pre-shared Secrets". (24) Implementing the PKI system involved setting up Microsoft Certificate Services in a win2000 server. The Microsoft CA server was very simple to set up. A new win2000 server machine was obtained and installed in the IT department. For security reasons, Marty decided temporarily to keep the CA off-line and issue certificates manually. Eventually he would put the CA server on-line and use the MSCEP plug-in to issue certificates with over the network using SCEP. Since remote access users would have to re-new their accounts, the renewal process could incorporate issuance of CA certificates and client certificates. A policy statement and instructions on using certificates was added to the remote access guidelines published on the university's web site.

Recovery:

After setting up the CA and reconfiguring the VPN gateways to use certificates, Marty helped several members of the faculty with the new remote access configuration. It was a painful process resulting in a high number of helpdesk calls, complaints and problems. Many of the problems were caused by a failure to check time and date settings on the client PCs. After installing the certificate config in several machines, Marty verified that the VPN would accept connections from the external network and from clients located on the campus network. Marty also conducted tests with the aggressive mode scanning and attack tools he had found during the study of the incident. Satisfied that the VPN network was no longer vulnerable to the aggressive mode brute force attack, he notified the student records system administrator.

Tuesday 9:00 AM

After a brief meeting including the student records administrator, the manager of the IT department and several members of the incident handling staff, it was agreed that the student records server could be put back on line. Additional measures were implemented to enhance monitoring of remote access and utilization of the admin network. Failed login attempts were logged and the Syslog priority in the VPN gateways

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and routers was increased to provide more information about system activity. This increased the size of the log-files and the work required to review them, but was considered a good measure since the logging information contained in the VPN gateways provided the main clues that revealed the incident.

Lessons learned:

Mark was apprehended and questioned about the Incident. When confronted with the evidence, he not only admitted having carried out the attack, but also provided details about how he did it. Mark's laptop was also confiscated for evidence. The security team was not aware that Enum and remote sharing were actually used to exploit the admin network until it was revealed during Mark's testimony. Log files and other information containing times and dates in the evidence matched Mark's description of the attack process. After the interview, the security team was satisfied that the investigation had been successful in dealing with the incident and had helped boost the security effort for the campus network. While the focus of the attack centered on the VPN exploit, the experience for the university staff brought to light several other security issues:

Lack of physical security: Use of switches may have prevented casual sniffing of network traffic, but free access to the network equipment allowed the attacker to tamper with and reconfigure equipment to allow eavesdropping.

Failure to enforce a password policy: A strong password policy had not been enforced. Even high-level managers used weak passwords, or wrote them down on post-it notes and used the same accounts on multiple machines. Frustrated users calling to have passwords reset were a constant headache for the help desk. This tendency had filtered down to the VPN pre-shared key, which had ended being a common dictionary word. Equipment such as routers and switches used in the campus network were found to have default accounts such as Admin/Admin or Admin /password.

Hardening of Operating Systems and servers: Some basic hardening practices would have greatly complicated the attack approach on the admin server. The easy Admin password problem mentioned above was one factor here as well.

Communications: Marty was commended for his quick response during the early stages of the incident. He correctly identified the unusual traffic patterns as signs of malicious traffic and alerted the security team. Good communications during the event fostered sharing of information and collection of evidence.

Logging: maintaining system logs provided a valuable source of information for the incident investigation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion:

As is the case with other security measures, poor or improper implementation can frequently undermine and circumvent the effectiveness of such measures. Just simply deploying a firewall does not necessarily improve the security stance of an organization. However, the uninformed may gain a false sense of security from doing so. A well thought-out set of firewall policies are required to provide any security benefits. We have seen in this example that improper configuration can open an otherwise secure VPN to vulnerabilities. The attack focused on capturing the unencrypted information exchanged during the VPN session establishment, using a known weakness in the RFC 2409 implementation of aggressive mode. We have also seen how this vulnerability, inherent in the standard is exacerbated by vendor design flaws as was the case with Checkpoint FW-1 and Cisco IOS. Using proper authentication and encryption methods, it is possible to create a very secure VPN network. The brute force attack would have taken orders of magnitude longer to crack a strong pre-shared key. Main mode can be used instead of aggressive mode and makes a similar attack more difficult since the authentication hash is encrypted. Most knowledgeable network administrators using VPN' s know to avoid aggressive mode altogether. Using X509 certificates instead of pre-shared secrets renders the attack altogether useless.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Endnotes:

1. Anton Rager, "IKEProbe source code," Sourceforge.net. Online. Internet. Available http://ikecrack.sourceforge.net/IKEprober.pl

2. Roy Hill, "NTA Monitor UDP Backoff Pattern Fingerprinting White Paper," NTA Monitor LTD. Online. Internet. January 2003. Available http://www.nta-monitor.com/ike-scan/whitepaper.pdf

3. Ibid.

4 Massimiliano Montoro, "Download site for Cain & Abel," Oxid.it. Online. Internet. 2003. Available http://www.oxid.it/cain.html

5 Anton Rager, "IKEProbe source code," Sourceforge.net. Online. Internet. Available http://ikecrack.sourceforge.net/IKEprober.pl

6. Michael Thurman and Enno Rey, “PSK Cracking Using IKE Aggressive Mode,” ERNW Enno Rey Netzwerke GmbH. Online. Internet. Available http://www.ernw.de/download/pskattack.pdf

7. Cisco Systems, Inc. "Cisco Response to Internet Key Exchange Issue," Cisco Systems, Inc. Online. Internet. April 2003. Available http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html

8. NTA Monitor, "Checkpoint FW-1 Flaw Background," NTA Monitor LTD. Online. Internet. Available http://www.nta-monitor.com/news/checkpoint/checkpoint-background.htm

9. CERT Coordination Center (CERT/CC), "Vulnerability Note VU#886601," Carnegie Mellon Software Engineering Institute. Online. Internet. Available http://www.kb.cert.org/vuls/id/886601

10. James S. Tiller, A Technical Guide to IPSec Virtual private Networks (Washington, D.C.:Auberbach Publications, 2001) 179.

11. Ibid, 182

12. Ibid, 192

13. Ibid, 75

14. NTA Monitor, "Checkpoint FW-1 flaw technical details," NTA Monitor, LTD. Online. Internet. Available http://www.nta-monitor.com/news/checkpoint/checkpoint-tech.htm

15. Ibid.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

16. Michael Thurman and Enno Rey, “PSK Cracking Using IKE Aggressive Mode,” ERNW Enno Rey Netzwerke GmbH. Online. Internet. Available http://www.ernw.de/download/pskattack.pdf

17. James S. Tiller, A Technical Guide to IPSec Virtual private Networks (Washington, D.C.: Auberbach Publications, 2001) 192.

18. Michael Thurman and Enno Rey, “PSK Cracking Using IKE Aggressive Mode,” ERNW Enno Rey Netzwerke GmbH. Online. Internet. Available http://www.ernw.de/download/pskattack.pdf

19 John Pilam, “Authentication Vulnerabilities in IKE and Xauth with Weak Preshared Secrets,” Institute for Mathematics and its Applications. Online. Internet. Available http://www.ima.umn.edu/~pliam/xauth/

20 John Chirillo, Hack Attacks Revealed (Washington, D.C.: Wiley, 2002) 557-610.

21 University of Wyoming IT Home, "Blueprint for UW Firewall Implementation Plan," The University of Wyoming. Online. Internet. February 2003. Available http://uwadmnweb.uwyo.edu/InfoTech/firewall/

22 Queen's University IT Services, "Queen’s University Network Security Policy," Queen's University. Online. Internet. March 2002. Available http://www.its.queensu.ca/network/policy/netsecpol.shtml

23 UALR Computing Services, "UALR Campus AUP and Network Security Policies & Procedures," University of Arkansas at Little Rock. Online. Internet. Available http://www.ualr.edu/isdept/instructions/policy/escalproc.html

24 John Pilam, “Authentication Vulnerabilities in IKE and Xauth with Weak Preshared Secrets,” Institute for Mathematics and its Applications. Online. Internet. Available http://www.ima.umn.edu/~pliam/xauth/

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

CERT Coordination Center (CERT/CC). "Vulnerability Note VU#886601." Carnegie Mellon Software Engineering Institute. Online. Internet. Available http://www.kb.cert.org/vuls/id/886601

Chirillo, John. Hack Attacks Revealed. Washington, D.C.: Wiley, 2002.

Cisco Systems, Inc. "Cisco Response to Internet Key Enchange Issue." Cisco Systems, Inc. Online. Internet. April 2003. Available http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html

Hill, Roy. "NTA Monitor UDP Backoff Pattern Fingerprinting White Paper." NTA Monitor LTD. Online. Internet. January 2003. Available http://www.nta-monitor.com/ike-scan/whitepaper.pdf

Montoro, Massimiliano. "Download site for Cain & Abel." Oxid.it. Online. Internet. 2003. Available http://www.oxid.it/cain.html

NTA Monitor. "Checkpoint FW-1 Flaw Background." NTA Monitor LTD. Online. Internet. Available http://www.nta-monitor.com/news/checkpoint/checkpoint-background.htm

Pilam, John. "Authentication Vulnerabilities in IKE and Xauth with Weak Preshared Secrets." Institute for Mathematics and its Applications. Online. Internet. Availalbe http://www.ima.umn.edu/~pliam/xauth/

Queen's University IT Services. "Queen's University Network Security Policy." Queen's University. Online. Internet. March 2002. Available http://www.its.queensu.ca/network/policy/netsecpol.shtml

Rager, Anton. "IKEProbe source code." Sourceforge.net. Online. Internet. Available http://ikecrack.sourceforge.net/IKEprober.pl

SecurityFocus Vulnerabilities. "IKE Aggressive Mode Shared Secret Hash Leakage Weakness." SecurityFocus. Online. Internet. Available http://www.securityfocus.com/bid/7423/info/

SourceForge.net. "Project: IKEcrack: Summary." SourceForge.net. Online. Internet. 2004. Available http://sourceforge.net/projects/ikecrack

Thurman, Michael and Enno Rey. "PSK Cracking Using IKE Aggressive Mode." ERNW Enno Rey Netzwerke GmbH. Online. Internet. Available http://www.ernw.de/download/pskattack.pdf

Tiller, James S. A Technical Guide to IPSec Virtual private Networks. Washington, D.C.:Auberbach Publications, 2001.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

UALR Computing Services. "UALR Campus AUP and Network Security Policies & Procedures." University of Arkansas at Little Rock. Online. Internet. Available http://www.ualr.edu/isdept/instructions/policy/escalproc.html

University of Wyoming IT Home. "Blueprint for UW Firewall Implementation Plan." University of Wyoming. Online. Internet. February 2003. Available http://uwadmnweb.uwyo.edu/InfoTech/firewall/

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.