Global Information Assurance Certification Paper

GCFW IP, Firewall, and VPN Practical
Version 1.6

Earl Charnick
Fall 2001 – resubmission
Online via
Mary Washington College
James Monroe Center

Assignment 1 – Security Architecture

Requirements

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components:

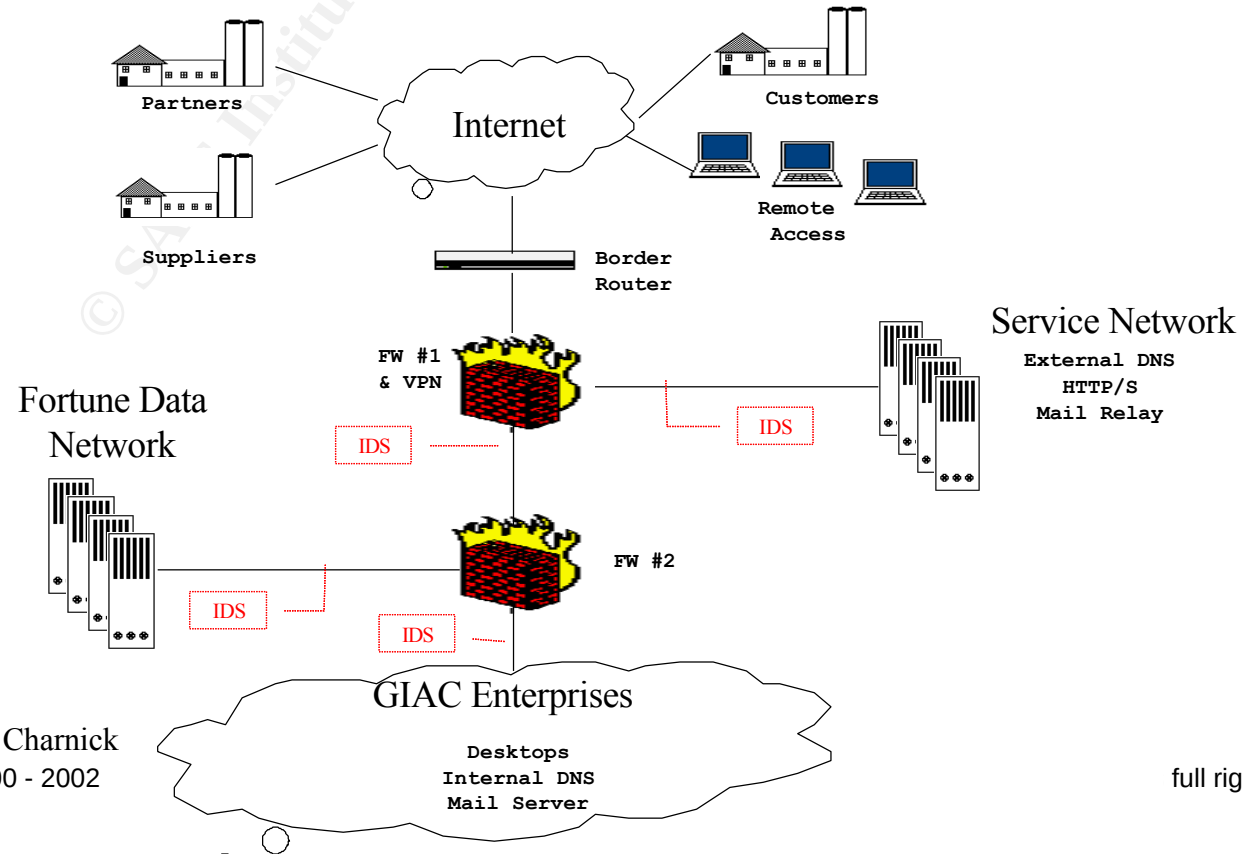
- filtering routers
- firewalls
- VPNs to business partners
- secure remote access
- internal firewalls

Your architecture must consider access requirements (and restrictions) for:

- Customers (the companies that purchase bulk online fortunes)
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes)
- Partners (the international partners that translate and resell fortunes)

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

Proposed Architecture



Abstract

The e-commerce business, GIAC Enterprises, requires secure network communications for day-to-day operations to customers, suppliers, and partners. From a service network, web based applications will provide secure online ordering for customers. Secured VPN connections will allow international partners and suppliers to provide, translate, and resell fortunes from GIAC Enterprises' internal databases. VPN connections also provide remote access for GIAC employees when on the road or at home. A combination of Cisco hardware and at least two types of firewall products, and intrusion detection will provide 'defense in depth' for GIAC Enterprises' computing environment.

Users

General Public

Any outside source will be allowed access to service network for only the services of HTTP/S, DNS, and SMTP.

Customers

Orders are requested through standard SSL web connections to HTML forms via the web server. Customer identification will be verified by using account numbers and passwords during ordering confirmation. General public access to service network is given, all other access is denied.

Partners

International translators and resellers are given access only to the fortune data LAN. Using secured firewall-to-firewall VPN tunnels, GIAC partners have direct access to the fortune database.

Suppliers

Fortune sayings are delivered directly to the fortune database and have access only to the fortune data LAN. Using secured firewall-to-firewall VPN connections, our suppliers have database accounts to maintain delivery of our fortune supply.

GIAC Employees

Full access is granted to internal, fortune data, and service LANs with successful login based on user name and password. Only web access is allowed from the internal LAN to the Internet. Using secured client-to-firewall VPN connections, our employees have full access to internal corporate assets as well as the fortune data LAN when they are away from their desks.

Perimeter

As the first line of defense for GIAC Enterprises, a Cisco 3640 router running IOS Release 12.2 will be used. Packet level filtering will be the primary security role of this device. The router will be configured to drop malformed packets, blocked or unavailable services, and most ICMP coming into or leaving the network. The desired effect is to reduce any extra processing from the primary firewall and aid

prevention of DoS attacks against or from our network. Information about the Cisco 3640 router can be found at http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm

Firewalls

The next layer of protection is provided by our primary and secondary firewalls. Two different firewall products will be required. The idea is to reduce the risk of the same security issue arising in both products at the same time as it is unlikely two different vendors would suffer from a common implementation bug. For the primary firewall, FW#1, a Nokia IP 530 appliance running Check Point Firewall-1 will be used. The primary firewall will also serve a dual purpose as the VPN access to the network using VPN-1 SecuRemote software solution. FW#1 will be responsible for the majority of the load processing from the Internet. Its role is to apply the security policy defined in the next section with regards to the internal and service network. For the secondary firewall, FW#2, a Cisco PIX 525 will be implemented. The internal firewall will be the screen for GIAC Enterprises' internal network and the fortune data network. Below are information links for the previously mentioned products:

- Nokia IP 530: http://www.nokia.com/securitysolutions/platforms/530.html
- Check Point Firewall-1: http://www.checkpoint.com/products/firewall-1/index.html
- VPN-1 SecuRemote: http://www.checkpoint.com/products/vpn1/securemoteds.html
- Cisco PIX 525: http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

Service Network

A service network will provide public services such as HTTP/S, the external part of our split DNS, and SMTP. This network will be implemented off one of the interfaces of FW #1. Strict IDS logging will be enforced.

Fortune Data Network

An interface off FW #2 will provide access to the fortune database network. Only the internal network and VPN accounts of our suppliers, partners, and remote users will have access to this network. Strict IDS logging will be enforced.

Internal Network

Home to the protected corporate assets such as internal DNS, SMTP mail server, syslog server, and local workstations. Complete access to the service and fortune data networks will be granted. Access to the Internet will only be provided for web based services; all other access will be denied. Remote users through a VPN connection have full access to the internal LAN. Split DNS and a mail relay is implemented to prevent compromising the internal network from the service network. Lowering the possible number internal connections to the service network limits proprietary information loss during an attack or compromise of our service network. Strict IDS logging will be enforced.

Intrusion Detection

The combination of ISS Real Secure technical support with snort's open source,

wide distribution and testing will provide a layered and redundant intrusion detection design. Both ISS Real Secure and snort will be configured to monitor the interfaces between the internal, service, and fortune networks. Logging will be sent to a centralized syslog server on the internal network. Logging by a single, dedicated machine will provide an overall point of view as well as synchronizing events as they occur.

Assignment 2 – Security Policy

Requirements
Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

> By 'security policy' we mean the specific Access Control List (ACL), firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

You **must** include the complete policy (ACLs, ruleset, IPSec policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper. (Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

Select **one** of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. A general explanation of the syntax or format of the ACL, filter, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. An general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:
    - the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.
    - Any relevant information about the behavior of the service or protocol on the network.
    - If the **order** of the rules is important, include an explanation of why certain rules must come before (or after) other rules.
5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

Be certain to point out any tips, tricks, or potential problems ("gotchas").

Security Policy

GIAC Enterprises has defined the following security policy in order to maintain the security of proprietary information deemed necessary for the corporation's success:

Border Router

Compliance to the security policy defined within is required when accessing and/or modifying the system. For the current architecture, a Cisco 3640 router with IOS 12.2 is our first layer of defense. Updates to the firmware will be applied in a timely manner, as they become available. Only a select few network engineers will have access to the router and all activity will be logged including access times, backups of configurations, and descriptions of changes made and the reasons those changes were required.

Router configuration

- Enable simple encryption. Force the router to store passwords in a simple encrypted format to prevent an easy discovery.
- Disable Cisco Discovery protocol. Disable services our network doesn't use.
- Disable bootp server. Disable services our network doesn't use.
- Disable http server. Disable services our network doesn't use.
- Disable proxy-arp. Disable services our network doesn't use.
- Disable direct broadcast. Prevent translation of broadcast address to physical addresses.
- Disable ICMP redirect messages. Prevent some network mapping attempts.
- Disable ICMP unreachable messages. Prevent some network mapping attempts.
- Disable source routing. Prevent some network mapping attempts.
- Disable SNMP. Prevent malicious use of this protocol.
- Disable all udp small services. Disable ability to misuse these services, no need to hand out information through 'who'.
- Disable all tcp small services. Disable ability to misuse these services, no need to hand out information through 'finger'.
- Enable logging to syslog server.
- Enable security banner.

Inbound traffic (ingress filtering)

- Log all traffic.
- Deny all traffic originating from private network addresses. This includes the IP of our router and generic loopback test addresses. These address are not routable and thus we shouldn't propagate them into our network.
- Permit traffic destined for the web servers on TCP service ports 80 and 443. Open our web based services for business purposes.
- Permit traffic destined for the mail servers on TCP service port 25. Open our mail services for business purposes.
- Permit traffic destined for the dns servers on TCP and UDP service port 53. Open our external dns services to advertise our public servers.
- Permit traffic destined for FW#1 on TCP service ports 50(ESP) and 51(AH) and 500(isakmp). Need to allow firewall-to-firewall and client-to-firewall VPN connections through.
- Permit established tcp traffic on ephemeral ports 1024 and above. Valid

established tcp traffic
- Deny all other traffic.

Outbound traffic (egress filtering)

- Log all traffic.
- Deny all traffic originating from private network addresses.
- Permit traffic destined for tcp services ports 50, 51, and 500. Allow IPSec traffic to leave.
- Permit traffic destined for tcp services ports 80 and 443 (HTTP/S). Allow internal users to access external web sites.
- Permit established tcp traffic on ephemeral ports 1024 and above. Allow valid established tcp connections.
- Permit recursive DNS queries. Allow for name resolution of outside sites.
- Deny all other traffic.

Router ACL's

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Configuration of router services
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
service password-encryption
no cdp enable
no ip bootp server
no ip http server
no ip proxy-arp
no ip directed-broadcast
no ip redirects
no ip unreachables
no ip source-route
no snmp-server
no service udp-small-servers
no service tcp-small-servers
logging syslog_IP
banner # Restricted Access #

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! Configure the interfaces
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! The interface of the router to the Internet
interface ethernet 0
        ip address IP_and_mask
ip access-group 100 in
!!! The interface of the router to GIAC LAN
interface ethernet 1
        ip address IP_AND_mask
ip access-group 101 out

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Block illegal inbound source addresses (Ingress filtering)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Block private addresses (RFC 1918), never valid coming
!!!     from outside.
access-list 100 deny ip 10.0.0.0      0.255.255.255      any log
access-list 100 deny ip 172.16.0.0    0.15.255.255       any log
access-list 100 deny ip 192.168.0.0   0.0.255.255        any log
!!! Block loopback address coming from outside.
access-list 100 deny ip 127.0.0.0     0.255.255.255      any log
!!! Block the router's IP when seen on the inbound interface.
access-list 100 deny ip host          0.0.0.0            any log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Permit available services and established connections
!!!     HTTP/S  (80/443 tcp), DNS (53 both), SMTP (25 tcp), VPN (50, 51, 500 tcp)
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 100 permit tcp any web_IP_and_mask eq 80 log
access-list 100 permit tcp any web_IP_and_mask eq 443 log
access-list 100 permit tcp any mail_IP_and_mask eq 25 log
access-list 100 permit tcp any dns_IP_and_mask eq 53 log
access-list 100 permit udp any dns_IP_and_mask eq 53 log
access-list 100 permit tcp any FW#1_IP_and_mask eq 50 log
access-list 100 permit tcp any FW#1_IP_and_mask eq 51 log
access-list 100 permit tcp any FW#1_IP_and_mask eq 500 log
access-list 100 permit tcp any any gt 1023 established log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Apply default deny rule for inbound interface
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 100 deny ip any any log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Block illegal outbound source addresses (Egress filtering)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Block private addresses (RFC 1918), never valid leaving our
!!!      network as either source or destination addresses
access-list 101 deny ip 10.0.0.0       0.255.255.255             any log
access-list 101 deny ip 172.16.0.0     0.15.255.255              any log
access-list 101 deny ip 192.168.0.0    0.0.255.255               any log
access-list 101 deny ip any 10.0.0.0          0.255.255.255      log
access-list 101 deny ip any 172.16.0.0        0.15.255.255       log
access-list 101 deny ip any 192.168.0.0       0.0.255.255        log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Allow IPSec traffic to leave
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 101 permit tcp FW#1_IP_and_mask any eq 50 log
access-list 101 permit tcp FW#1_IP_and_mask any eq 51 log
access-list 101 permit tcp FW#1_IP_and_mask any eq 500 log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Give external web access  to outbound connections
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 101 permit any any eq 80 log
access-list 101 permit any any eq 443 log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Allow web/dns/vpn server responses
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 101 permit tcp any web_IP_and_mask gt 1023 established log
access-list 101 permit tcp any dns_IP_and_mask gt 1023 established log
access-list 101 permit tcp any smtp_IP_and_mask gt 1023 established log
access-list 101 permit tcp any FW#1_IP_and_mask gt 1023 established log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Allow DNS recursive queries
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 101 permit udp dns_IP_and_mask any eq 53 log
access-list 101 permit tcp dns_IP_and_mask any eq 53 log

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Apply default deny rule for outbound interface
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
access-list 101 deny ip any any log
```

Testing configuration

- Verify line by line of the ACL is working with the aid of an address spoofing tool such as nmap and a network sniffer like tcpdump.
- Denied services and addresses should be logged as such and the network

sniffing tool should not report that traffic as transcending through to the prohibited interface.
- Permitted services and address should be logged as such and verified as working.
- Verify logging to syslog server is working and valid.

Primary Firewall

The primary firewall is the next layer in GIAC Enterprises' defense. For the current architecture, a Nokia IP 530 device running Check Point Firewall-1 is implemented. Upgrades to the Nokia firmware will be made in a timely manner, as they become available. Check Point Firewall-1 software upgrades will be made in a timely manner, also as they become available. Only a select few individuals will have access to the device as well as the necessary privileges required to change the firewall's ruleset.

Firewall Security Policy

All traffic that is determined to be blocked will be dropped verses rejected. The action of rejecting traffic generates reset packets and clearly announces the presence of the firewall.

1. Firewall administrator rule. *** Note *** This rule must always be above the lockdown rule in rule processing. Connection from a predetermined firewall administrator workstation to the firewall must be allowed.
2. Noise reduction rule. Eliminate noisy protocols like NBT to reduce unnecessary processing and logging by the firewall.
3. Firewall Lockdown rule. Drop all traffic directed at the firewall and alert administrators of the connection attempt. This could be a sign of a network scan or spoofing attempt.
4. A VPN rule to define partners connections to have access to fortune data LAN.
5. A VPN rule to define remote users connections to have access to both fortune and data LAN. Allow any internal addresses access to service network HTTP/S server.
6. Allow any internal addresses access to service network HTTP/S server.
7. Allow internal mail server access to service network SMTP server.
8. Allow internal dns server access to service network DNS server.
9. Allow any internal address access to external HTTP/S.
10. Allow any external addresses access to service network HTTP/S, SMTP and DNS.
11. Deny everything rule. *** Note *** Since this is the default rule, should always be last in rule processing.

Firewall Ruleset

#	Source	Destination	Service	Action	Track
1	fw-admin	FW #1	Firewall1	Accept	Long
2	any	FW #1	NBT	Drop	

3	any	FW #1	any	Drop	Alert
4	FW partners	fortune	IPSEC-AH, IPSEC-ESP, IPSEC-IKE	Accept	Long
5	remote users FW	internal, fortune	IPSEC-AH, IPSEC-ESP, IPSEC-IKE	Accept	Long
6	internal	service web server	HTTP/S	Accept	Long
7	internal mail server	service mail server	SMTP	Accept	Long
8	internal dns server	service dns server	DNS	Accept	Long
9	internal	external	HTTP/S	Accept	Long
10	external	service	HTTP/S, SMTP, DNS	Accept	Long
11	any	any	any	Drop	Long

Testing configuration

- Verify administrator workstation can connect and administer the firewall and other workstations cannot.
- Verify line by line of the ACL is working with the aid of an address spoofing tool such as nmap and a network sniffer like tcpdump.
- Verify each type of drop packet gets logged except for the noisy NBT protocol.
- Verify fragmentation of packets doesn't bypass ruleset defined in firewall.

VPN

For the current architecture, it was decided to use the Check Point FW-1 firewall for a dual purpose, VPN. With VPN-1 SecuRemote, standard-industry encryption and authentication algorithms are available and can be configured differently for different users. This should allow international partners access to the necessary software and not violate export regulations. IPSec will be implemented and security associations will decide with encryption algorithm and/or authentication algorithm that will be used and their respective keys. Remote users must connect with HMAC MD5 authentications and 3DES 168 bit encryption in order to provide the highest security possible. ISAKMP key management will be implemented in order to reduce manual configurations of each remote device. International partners will use DES encryption instead as export laws restrict the use of triple DES overseas.

Miscellaneous

Users

Authorized users will be assigned user ids of 8 alphanumeric characters and are required to maintain strong passwords. These passwords will be forced to change every 2 to 3 months. The passwords will be 8 or more characters in length and must also be alphanumeric. Account and/or password sharing is strictly prohibited. A database of all accounts created will be kept with all

privileges assigned to the individual ids. At the time of an employee's termination, network privileges will be revoked within 24 hours or earlier depending on type of departure. Signed documentation from recognized department personnel will be required when adding privileges, removing privileges, or creating a user account.

Software upgrades

Application software, operating system, and virus upgrades will be applied and maintained by the GIAC Enterprises' help desk personnel, as they become available. These restricted individuals must be allowed to have administrator privileges.

Incident Handling

In the event of an incident the following steps should be followed:

- Gather as much information as possible. The mail subject that contained the virus, the account that was compromised, the logs from the network or IDS that signaled a problem.
- Determine if action should be taken and at what level. Is it something that can wait until the next business day or does it require the network to be taken off line based on what data was/could be compromised? Is a restore needed?
- Notify the appropriate points of contact. Customer relations, support staff, corporate partners, help desk.
- Follow up with log and statistical analysis and suggestions for future prevention. If necessary, any procedural changes required?

Tutorial

Configuring your router can be done through command line interface. A command reference can be found at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm. In addition, Cisco has a free software tool, Config Maker, available for download at http://www.cisco.com/public/sw-center/sw-netmgmt.shtml. With this tool, an initial ACL can be created from a click and drag interface. Once the ACL has been defined, following the steps below, you can configure your router to comply with your security policy.

1. type 'telnet *router_ip_here'*
   From an administrator box, bring up a telnet session to the router. This step will open a window to the router and prompt for user name and password. However, this puts the router into a view/user exec mode. Enter user name and password to complete the login.
2. type 'enable'
   This allows the user to change from a view role to a administrative role. Another user name and password will be needed to complete this step.
3. type 'erase nvram:'
   This step clears the configuration of the router. This guarantees we start fresh

with a fresh configuration.

4. type 'no cdp enable'
   Turns off the Cisco discovery protocol behavior of the router, limiting possible reconnaissance information.
5. type 'no ip bootp server'
   Turns off the BOOTP service, not used so turn it off.
6. type 'no ip directed-broadcast'
   Prevents broadcast address translation into our network.
7. type 'no ip http server'
   Prevents web interface to router from being used.
8. type 'no ip proxy-arp'
   Turns off proxy ARP on the interface
9. type 'no ip redirects'
   Turns off ability to send ICMP redirects messages.
10. type 'no ip source-route'
    Drops IP packets marked as source routed, as these could be used to map out internal network layout.
11. type 'no ip unreachables'
    Turns off ability to send ICMP unreachable messages, another form of possible reconnaissance.
12. type 'no snmp-server'
    Turns off ability to use SNMP which is allows remote administration of the router and other reconnaissance techniques.
13. type 'no service finger'
    Turns off the finger protocol, another source of reconnaissance.
14. type 'no service udp-small-servers'
    Turns off services from trusted, low number ports like chargen and echo.
15. type 'no service tcp-small-servers'
    Turns off services from trusted, low number ports like finger.
16. type 'service password-encryption'
    Encrypts password information on the router. Although not stringent, every little bit helps.
17. type 'configure terminal'
    This enters the interface configuration, which allows the user to assign IPs, netmasks, and other parameters for each interface.
18. type 'interface eth0'
    This places the user into interface configuration mode for the specific interface given. From this point on, the following commands will be applied to this interface until CTRL-Z is typed.
19. type 'ip address *ip_addr_of_interface netmask_of_interface*'
    This assigns the specified IP address and netmask to this interface. This must be done for each and every interface used on the router.
20. type CTRL-Z
21. *Use Previous ACL list to complete the setup.*
22. type 'exit'

Exits out of interface control mode.

Assignment 3 – Security Audit

Requirements

You have been asked to conduct a technical audit of the **primary firewall** (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

1. Plan the audit. Describe the technical approach you recommend to assess the firewall. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Evaluate the audit. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but you must annotate/explain the output.

Plan

The time has come for the scheduled security audit against the external firewall. As described in GIAC Enterprises security policy, a rigorous audit is to be performed against key network assets on a quarterly basis. The following procedure was created for the external firewall audit and approved by management who leveraged possible downtime and business impacts against security concerns:

1. Obtain approval in writing of audit notification and awareness forms before starting the planned security audit against any part of GIAC Enterprises' network.
   - Official approval forms located within security bulletin board.
   - Management signatures required from Sales, Development, and Network departments.
2. Determine exact timeframe of security audit.
   - Place emphasis on performing the security audits during off peak business hours.
   - Send corporate email notification to employees with times of the audit.
3. Research potential vulnerabilities with GIAC Enterprises' firewall's hardware, software, operating system and/or firmware before conducting audit and focus on issues that apply.
   - Check vendor web sites.
   - Check security forums.
4. Perform necessary steps to minimize risk of compromise and downtime as a result of the audit before and during the audit.

- Perform backup of firewall configuration.
- Perform tests during the audit of provided services to ensure their availability.
- Verify IDS are logging appropriately

5. Conduct the audit.
   - Use port scanner (nmap) to probe firewall interfaces for available services.
   - Use port scanner (nmap) to probe firewall interfaces for blocked services.
   - Use vulnerability scanner (Internet Security Scanner or nessus).
   - Use sniffer (tcpdump) to monitor behavior of firewall.
6. Review results of the audit.
   - Collect and analyze logs from IDS and syslog servers as well as the vulnerability scanners, network sniffers, and port scanners.
   - Inform departmental management of network security status.
   - Schedule times to apply patches, upgrades, and configuration changes if required and approved by management.
   - Suggest tools and procedural changes for the next security audit.
   - Suggest improvements to network design to increase bandwidth, security, and of course profit.

Cost Estimate: Total of 40 hours (~$2,000 / 8 hrs) = $10,000 approx.

1) 2 hours to obtain necessary signatures and approval.
2) 1 hour to choose timeframe of audit based on personnel scheduling and management input.
3) 8 hours to devote to vulnerability research and vendor contact.
4) 5 hours to backup configuration and setup service tests.
5) 16 hours to conduct audit.
6) 8 hours to review data, draw conclusions, and brief management of recommendations, improvements, and impacts.

Conduct

After spending reasonable time acquiring the necessary signatures of approval, we send out sufficient notice that the planned security audit will begin on a Wednesday evening from 5pm to Thursday 9am. Network data shows this to be the best window of opportunity during a given week to have the least impact on commercial business. At least five hours before the test begins, we will begin backing up the firewall configuration, setting up the necessary tools that will be used, and verifying proper logging levels of the IDs. Tcpdump will be used on all interfaces of the firewall and setup to log the data to a file for later analysis. Run tcpdump as:

tcpdump –i *interface* –n –v –X *expression* > outputfile

-i (*interface*): the name of the interface to put in promiscuous mode.
-n: don't convert ip addresses to host names.
-v: show a little more output.
-X: show ASCII text next to hex dump of packet.
(*expression*): where appropriate, this is specified to filter output.

Testing available services

DNS

- Use tcpdump expression 'port 53' to filter output for this test.
- Request name resolution of GIAC's website from an external Internet connection using nslookup. Verify authoritative answer is correct and comes from the service DNS server.
- Request name resolution of GIAC's website from an internal workstation using nslookup. Verify resolution is correct and comes from internal DNS server.
- Verify zone transfers are working between internal DNS server and service DNS server.

HTTP/S

- Use tcpdump expression 'tcp port 80' to filter output for this test.
- Navigate GIAC website from an external Internet connection. Verify web server is responding properly with requested URLs.
- Navigate GIAC website from an internal workstation. Verify web server is responding properly with requested URLs.
- Navigate external websites from an internal workstation. Verify external web sites are responding properly with request URLs.

SMTP

- Use tcpdump expression 'tcp port 25' to filter output for this test.
- Send mail to internal GIAC address from external mail system and verify it is received on the service SMTP server.
- Send mail to external Internet address from internal workstation and verify it is received on the internal mail relay, then forwarded to service SMTP server.

VPN

- Use tcpdump expression 'tcp port 50 or tcp port 51 or tcp port 500' to filter output for this test.
- Establish remote VPN from external Internet connection. Verify connection to internal LAN is working as expected and access internal services are available.
- Verify partners' and suppliers' firewall properly establish VPN tunnel and they have access just to the data fortune LAN.

Testing blocked features

Router

- Verify ingress filtering is working. For a subset of each private address space, attempt connecting to an available public service on GIAC from an external site and verify connection attempts fail.
  nmap –S 192.168.10.20 –p 80
- Verify egress filtering is working. Try to pass traffic from internal interface of the router to the external interface again spoofing private addresses.

Firewall

- Verify traffic directed at the firewall is dropped. Use nmap against the firewall's IP address on all of its interfaces.

- Verify traffic directed at service ports other than SMTP, DNS, IPSEC, and HTTP/S is dropped on all interfaces.
- Verify firewall behaves as expected when dealing with fragmented packets. To assure the firewall assembles and filters packets that fall into this category. To test this situation, use a fragmenting tool such as hping2.

  hping2 –I *interface* –V **–f** –c *count* –d *bytes* –p *dest_port host*

  -I *interface*: use this interface to send packets.
  -V: show more output.
  -f: fragment packets, guarentee firewall reassembles and filters packets.
  -c *count*: how many packets to send.
  -d *bytes*: how large each packet will be.
  -p *port*: destination port for the packets.

Services

- Verify from external Internet connection that the only public services seen are those of DNS, SMTP, HTTP/S and IPSec using nmap in the following fashion:

  nmap -sT -P0 -O -v -o tcp_output -p 1-65535 -g 53 *ip_addresses*
  nmap -sU -P0 -O -v -o udp_output -p 1-65535 -g 20 *ip_addresses*

  -s (*type of scan*): T for TCP scan, U for UDP scan.
  -P0: don't ping host before the scan to determine if exists.
  -O: try to determine hosts' operating system via TCP/IP fingerprinting.
  -v: provide more than the default level of output
  -o *filename*: filename to store output.
  -p *ports*: port range to scan
  -g *port*: source port to use in scans, most firewalls will allow traffic through for TCP ftp-data and UDP DNS.
- Verify from service LAN connection that hosts and services on the fortune data LAN are not visible using the same technique.
- Verify from the internal LAN that hosts and services other than DNS, SMTP, and HTTP/S on the service network are not available using the same technique.

Finishing Tasks

- Run nessus against the GIAC Enterprise network and verify any vulnerabilities reported.
- Check logging of router, firewall, and IDS before, during, and after each type of test in order to capture and verify test results to analysis later.

Review

Testing Output

Network trace outputs and firewall logging verify proper path configuration of GIAC Enterprise's public DNS, SMTP, HTTP/S, and VPN. IDS logging and nessus report everything as nominal. For example, VPN is correctly negotiating keys and encrypting data. Below is a sample network connection trace of the negotiation established. (Several intermediate packets within the phases are omitted to conserve

space).

VPN Phase 1

ISAKMP key exchange (negotiation which algorithms to use and their properties). This example show an aggressive exchange implementation. Notice that tcp port 500 is used thus verifying VPN connectivity.

```
18:11:17.968610 192.168.1.111.500 > 192.91.173.52.500: isakmp 1.0 msgid 00000000: phase 1 I agg: [|sa] (ttl
128, id 28357)
0x0000    4500 012c 6ec5 0000 8011 9b54 c0a8 016f    E..,n......T...o
0x0010    c05b ad34 01f4 01f4 0118 1b80 0dd8 b62e    .[.4............
0x0020    f488 c528 0000 0000 0000 0000 0110 0400    ...(............
0x0030    0000 0000 0000 0110 0400 004c 0000 0001    ...........L....
0x0040    0000 0001 0000 0040 0101 0002 0300 001c    .......@........
0x0050    0101                                       ..
```

VPN Phase 2

Exchange private information.

```
18:11:18.264630 192.91.173.52.500 > 192.168.1.111.500: isakmp 1.0 msgid bb061552: phase 2/others R
#6[E]: [|hash] (ttl 56, id 62474)
0x0000    4500 0060 f40a 0000 3811 5edb c05b ad34    E..`....8.^..[.4
0x0010    c0a8 016f 01f4 01f4 004c 3342 0dd8 b62e    ...o.....L3B....
0x0020    f488 c528 c54a e8aa 86a2 8677 0810 0601    ...(.J.....w....
0x0030    bb06 1552 0000 0044 cc2e 9687 6097 f137    ...R...D....`..7
0x0040    0c3f f4fa 97ef 65be a94f 201e e03f 163b    .?....e..O...?.;
0x0050    e467                                       .g

18:11:19.979658 192.91.173.52.500 > 192.168.1.111.500: isakmp 1.0 msgid 29dd19f3: phase 2/others R
oakley-quick[E]: [|hash] (ttl 56, id 62501)
0x0000    4500 01e8 f425 0000 3811 5d38 c05b ad34    E....%..8.]8.[.4
0x0010    c0a8 016f 01f4 01f4 01d4 fcea 0dd8 b62e    ...o............
0x0020    f488 c528 c54a e8aa 86a2 8677 0810 2001    ...(.J.....w....
0x0030    29dd 19f3 0000 01cc 46c3 73c8 c609 9010    ).......F.s.....
0x0040    590a 1448 ec77 0c3f a2ed fbdb b80a e190    Y..H.w.?........
0x0050    829f                                       ..
```

VPN Phase 3

Secure encrypted connection established. A longer snapshot of the network traffic on this connection verifies that the encapsulated packets are encrypted as their header information is garbled.

```
18:11:20.332665 192.168.1.111 > 192.91.173.52: ESP(spi=1337485,seq=0x1) (ttl 128, id 29893)
0x0000    4500 0098 74c5 0000 8032 95c7 c0a8 016f    E...t....2.....o
0x0010    c05b ad34 0014 688d 0000 0001 3b15 3e8d    .[.4..h.....;.>.
0x0020    d3a6 fd06 d13d 9916 eb39 7827 5146 6cd3    .....=...9x'QFl.
0x0030    3039 d6a3 65d3 bba4 aa8e 892c f953 1de4    09..e......,.S..
0x0040    ddbd daaf ce10 0869 1ab0 8d9b 17fe f2e4    .......i........
0x0050    e713                                       ..
```

Review Summary

It was determined that GIAC Enterprises network architecture was designed sufficiently to handle today's traffic; however, several improvements could be made to increase bandwidth and security which have direct impact to the company's profit.

Changes to Perimeter

- Recommend additional border router.
  This would provide an alternative route to the Internet and eliminate the router as

a single point of failure. Balancing load between the two routers would increase Internet traffic.

- Recommend IDS between border router and primary firewall.
  Additional tracking information at this point would guarantee the router is correctly packet filtering and the primary firewall is correctly filtering flow of the service and corporate subnets.
- Require internal audit for modem access of corporate workstations, desktops, servers, and any other network component.
  *** We can only design defense against what we know about the network. As direct dial-up is a viable remote access method, it is not part of this network. Thus, any access through the perimeter via modem bypasses the router and firewall configurations and violates the security policy. The best way to prevent this is to disable any modem through hardware methods. Current network assets should be checked routinely.

Changes to Primary Firewall

- Recommend moving VPN off firewall if performance becomes a problem

Changes to Network Architecture

- Recommend a web proxy for GIAC Enterprises' internal subnet.
- Suggest separating internal network into departmental groupings.

Assignment 4 – Design Under Fire

Requirements

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

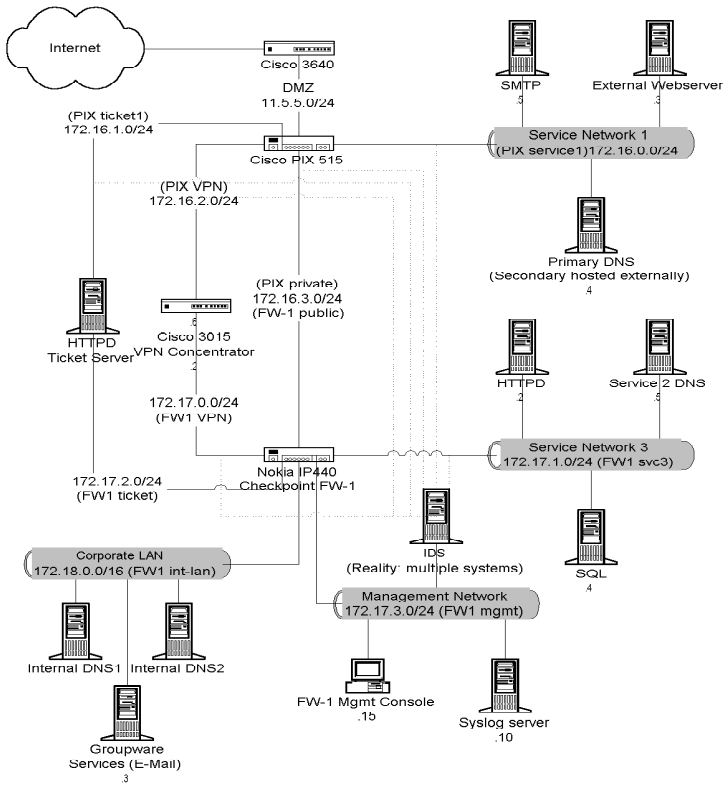
1. An attack against the firewall itself. Research and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

In designing your attacks, keep the following in mind:

- The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.
- The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)
- You **must** supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.
- The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

Architecture Chosen

For my attack network, I chose Christopher Kellogg's design found at http://www.sans.org/y2k/practical/Christoper_Kellogg_GCFW.doc. The following network excerpt was taken from his paper:



Vulnerabilities of PIX Firewall

Kellogg's design was to implement a Cisco PIX (515) as service network 1's firewall. Since no mention of software version was made in the contents of the paper, I am assuming from the references sited that it should be running software version 4.4. The following three vulnerabilities have been found with this firewall:

Cisco PIX TACACS+ Denial of Service Vulnerability

http://www.securityfocus.com/bid/2551

ISSUE:

Repeated requests for TACACS+ authentication uses up all available resources and kills the firewall. This denial of service attack can come from any of the firewall's interfaces and only affects the firewall if configured for 'aaa authentication'.

ATTACK:

From inside network, run the following command:

while(1); do (wget http://external.system 2> /dev/null &); done

SOLUTION:

Don't use aaa authentication configuration.

Firmware upgrade.

Cisco Secure PIX Firewall Forged TCP RST Vulnerability

http://www.securityfocus.com/bid/1454

ISSUE:

If a hostile party has knowledge of a connection established (source and

destination IP's as well as ports) and forges a TCP/RST packet, the firewall closes the connection. In other words, the firewall immediately drops all state table information about the connection and considers it terminated.

ATTACK:

Use software such as hping to form packet with known source, destination addresses and ports.

SOLUTION:

Firmware upgrade.

Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability Re-Introduction

http://www.securityfocus.com/bid/3365
http://www.securityfocus.com/bid/1698

ISSUE:

A connection that is allowed through the firewall to a SMTP server doesn't maintain the proper state in certain error conditions. In some cases, certain SMTP commands are filtered when seen as a security issue (i.e. EXPN, VRFY, and HELP); however, anything in the DATA section is considered the mail messages and let through until the following key sequence is seen:

"<CR><LF><CR><LF>.<CR><LF>"

The problem arises when the SMTP server reports an error but the firewall doesn't recognize it should end the DATA section since it hasn't seen the ending key sequence. In the DATA mode, the firewall allows everything through thus opening the SMTP connection to any command; even the ones that are considered security risks.

ATTACK:

A simple telnet to the SMTP port from an external address and sending the following commands to the server:

helo ciao
mail from: user@outside.net
data ⇐ firewall no longer filtering commands
expn guest/help/any other command

SOLUTION:

Upgrade firmware if affected.

Using this last method, the SMTP Content Filtering Evasion Vulnerability, an attack against the firewall could be constructed in the following manner:

1. Login to a compromised host or computer at a local public library to hide our identity.
2. Establish a telnet connection to the SMTP port 25 of 40.30.20.10, the assumed public address of this network.
   Command:
   > telnet 40.30.20.10 25
   Response:
   220 40.30.20.10 ESMTP Sendmail 8.10.2+Sun/8.10.2; Sat, 11 Nov 2001 22:51:54 -0500 (EST)
3. Verify firewall working by trying some restricted commands, i.e. help and

expand.
Command:
> expn guest
Response:
none (indicates firewall is filtering commands.)

4. Setup initial steps to attack using the helo and mail commands.
   Command:
   > helo dummy.net
   Response:
   250 65.20.2.1 Hello [40.30.20.10], pleased to meet you
   Command:
   > mail from: unk@home.net
   Response:
   250 2.1.0 duke@home.net... Sender ok
5. Issue the data command to force an error condition. The recipients of the mail must be specified before the data section is encountered.
   Command:
   > data
   Response:
   503 5.0.0 Need RCPT (recipient)
6. Issue any restricted commands. At this point, the firewall considers the connection in the data section and should allow everything through; however, the SMTP server never entered the data state.
   Command:
   > expn guest
   Response:
   550 5.1.1 guest... User unknown
   Command:
   > help
   Response:
   214-2.0.0 This is sendmail version 8.10.2+Sun
   214-2.0.0 Topics:
   214-2.0.0 HELO EHLO MAIL RCPT DATA
   214-2.0.0 RSET NOOP QUIT HELP VRFY
   214-2.0.0 EXPN VERB ETRN DSN
   214-2.0.0 For more info use "HELP <topic>".
   214-2.0.0 To report bugs in the implementation contact Sun Microsystems
   214-2.0.0 Technical Support.
   214-2.0.0 For local information send email to Postmaster at your site.
   214 2.0.0 End of HELP info

Distributed Denial of Service Attack

1. Choose type of attack. I would implement a TCP SYN flood attack against the GIAC Enterprise network. This type of attack has two benefits, not only bandwidth consumption with large coordinated attacks, but resource consumption since successful TCP connections require state to be maintained.
2. Compromise 50 cable modem/DSL systems. With today's boom in high speed Internet access through DSL and cable modems, there is a large pool of vulnerable home systems with huge bandwidth potential. With my attack, I

would use the latest variant of mail virus, the "I Hate You" virus. The effect of running this virus is the installation of a Tribe Flood Network server on the local machine. The Tribe Flood Network tool allows for a TCP SYN flood with the aid of spoofing source IP addresses to hide the valuable compromised systems. More information on the Tribe Flood Network distributed attack tool can be found at http://www.cert.org/incident_notes/IN-99-07.html.

3. Run the attack. Once fifty or more systems respond with successful server installations, I would instruct my client program to send attack instructions to the list of compromised systems. These systems would receive instructions to send TCP SYN packets at high rates to GIAC Enterprises web server.
4. Monitor the attack. Using any web browser, requesting public web sites from GIAC Enterprises should be a simple enough sign to indicate if the attack is succeeding. If a significant impact to server response time is noticed, then the attack is potentially impacting all of GIAC Enterprises since there is one route in and out of their network. With the aid of nmap, monitoring available services would indicate if the firewall is impacted. For example, if nmap reports no services available, our attack probably hung the firewall or router. If nmap reports services available such as telnet and rsh that weren't available before the attack, then the attack may have overwhelmed the firewall and it failed open.
5. Apply countermeasures. One step to prevent resource consumption of the firewall would be to limit the number of connections through the firewall or through router, i.e. tcp intercepts. Another step would be to improve the network architecture by eliminating the network bottleneck. Perhaps an alternative route with another router might be in order.

Attack Plan on Targeted Host

I would consider attacking the web server for the following reasons:

- It's the heart and sole of an e-commerce business.
- Web servers have direct access to customer information such as name, address, phone, and credit cards.
- Web servers may reside on service networks with other public services. Eavesdropping on the network may provide network mapping information or clear text passwords if we're lucky.

In order to compromise the web server, I would try the following steps:

1. Probe the web site looking for patterns in structure layout. A little reconnaissance can go a long way once access is gained.
2. Try to determine web server platform and server type (Apache, Microsoft IIS, etc). Look for current exploits in the public domain newsgroups and on hacker and security web sites like http://www.cert.org/advisories. Trying to deduce the web server application type can sometimes be as simple as a telnet to the web server port and read the banner (go Microsoft). One recent example, the "Code Red" worm, can be found at http://www.cert.org/advisories/CA-2001-19.html.
3. If a web site is found that prompts for user authentication, an exploit could be set

up to try a brute force attack against user names and passwords. Sometimes login error responses indicate when a valid username/invalid password is given. For example, trying to login to a mail server with a valid username and invalid password responds with "ERR Password incorrect"; however, invalid username and password responds with "ERR Authentication incorrect". Once again, knowing when were dealing with Microsoft gives that extra little edge. Combinations of usernames exactly 8 characters long would be a great start.

4. Once enough information is gathered, I would try any exploits found against the SSL port 443 on the web server. The idea here is to hide my attempts through the encrypted connection and give me more time to do my dirty work.
5. After achieving successful penetration, I would consider closing the hole I came through but not before leaving a back door, for example Back Orifice, in order to prevent someone else coming through the same security hole. Then, I would be patient and eavesdrop on the network; you never know when a plain text username and password flashes by.

Bibliography – Links and References

Baccam, Tanya. Practical Assignment available at http://www.sans.org/y2k/practical/Tanya_Baccam_GCFW.zip

Comer, Douglas E. "Internetworking with TCP/IP" Volume I Principles, Protocols, and Architecture. Prentice Hall 1995.

Kellog, Christopher. Practical Assignment available at http://www.sans.org/y2k/practical/Christoper_Kellogg_GCFW.doc

Security Focus available at http://www.securityfocus.com/

SANS Resources – How to Eliminate The Ten Most Critical Internet Security Threats available at http://www.sans.org/topten.html

Securing Your Internet Access Router available at http://www.sans.org/infosecFAQ/firewall/router.htm