PERPOS Information Assurance

Jason Kau
Georgia Tech Research Institute
Georgia Tech Information Security Center

Son Nguyen
Army Research Lab

PERPOS Technical Report ITTL/CSITD 05-1

May 31st 2005

The Army Research Laboratory (ARL) and the National Archives and Records Administration (NARA) sponsored this research under Army Research Office Cooperative Agreement DAAD19-03-2-0018. The findings in this paper should not be construed as an official ARL or NARA position unless so indicated by other authorized documentation.

Abstract

Electronic record archives that are a part of any computer network, and especially those that are connected to the Internet, are at risk of attack by hackers. This report describes three security technologies that are used to mitigate these risks – firewalls, vulnerability assessment tools, and antivirus software. Two firewall products are evaluated with regard to their depth of inspection, hardware/software platform, and performance. Among our conclusions with regard to firewalls are:

- Firewalls should be classified by the degree to which they do deep packet inspection and on a per protocol basis.
- Firewall appliances should be used instead of firewall software on a general purpose operating system in order to provide increased security, reduced management costs, optimized configurations, and higher performance.
- NIAP certification of firewall products, while a Federal requirement, is not sufficient to control access to protected systems.

Two vulnerability assessment network scanner products were evaluated on their ability to detect vulnerabilities and the usefulness and depth of their reports. These vulnerability assessment tools were also used to provide vulnerability assessment for PERPOS project systems and firewalls. We illustrate from the vulnerability assessment reports why “outside the firewall” vulnerability assessment scanning is necessary in order to verify that firewall rules are configured correctly/working as expected, that inadvertent external access to internal resources has not occurred, and that the firewall is not leaking information about the internal network or the firewall products themselves that could be used by hackers trying to penetrate the firewall. We illustrate from the vulnerability assessment reports why "inside the firewall" vulnerability scanning is necessary in order to determine operating system and DBMS vulnerabilities, identify unnecessary network servers, and suggest enhanced security configuration for necessary network servers.

Among our conclusions regarding vulnerability assessment tools are:

- More than one vulnerability assessment scanner should be used in order to compare results to ensure that one of the scanners is not missing vulnerabilities due to configuration errors, lack of updated signatures, or differences in detection methods.
- Vulnerability assessment scanners can return false positives. Administrator knowledge about the scanned systems, comparison of results with another scanner, and consultation with the vendors of the target systems must be performed in order to distinguish false positives from true positives.

Table of Contents

1. Introduction

Background

All IT security products purchased by the US Government for National Security Systems, which handle classified and some non-classified information, are required to be Common Criteria certified under the National Security Telecommunications and Information Systems Security Policy #11 (NSTISSP #11). Additionally, the Department of Defense 8500 directive and instructions (8500.1 and 8500.2) both indicate the DoD systems should be composed of evaluated products. NIST Special Publication 800-23 is a directive containing guidelines for Federal organizations concerning purchasing or acquiring IT products. It also states that security products must be evaluated, and provides guidance for selecting the appropriate level of validation. The directive specifically calls out the National Information Assurance Program (NIAP) Common Criteria Evaluation and Validation Program for evaluation of security products.

The Presidential Electronic Records Pilot System (PERPOS) project has developed a prototype electronic records repository and services for processing records in this repository. The project also has a PERPOS project web portal. These resources are shared with other repositories on a Federated data grid. The security policy for this prototype system requires that it be protected with a firewall, anti-virus software, and an intrusion detection system. It also requires that its vulnerabilities be assessed.

Purpose

The purpose of this report is: (1) to describe an evaluation of two NIAP-certified firewalls with regard to their depth of inspection, hardware/software platform and performance, and (2) to describe an assessment of the vulnerability of the PERPOS project systems and firewalls.

Scope

In the next section, firewall network inspection architectures are reviewed, firewall hardware/software platforms are analyzed, and of two NIAP-certified firewalls are evaluated.

In the third section, two vulnerability assessment tools are evaluated on their ability to detect vulnerabilities and the usefulness and depth of their reports. These vulnerability assessment network scanners are also used to provide vulnerability assessment for PERPOS project systems and firewalls.

Section four discusses the need for multiple anti-virus solutions.

For the reader who is not an Information Security professional, a glossary of technical terms is appended.

2 Firewall Evaluation

Firewalls inspect network traffic to make access control decisions (discard, forward, redirect) based on administrator defined rules. With the advent of deep packet inspection (DPI) firewalls that implement some degree of intrusion detection/intrusion prevention system (IDS/IPS) functionality, these rules can specify signatures of attacks to block, specify restrictions on protocol functionality, and perform protocol anomaly detection in order to prevent unknown attacks. A full IDS/IPS product looks for suspicious network activity based on a combination of signatures, statistical analysis, heuristics, protocol and network-based anomaly detection and sends alerts, instructs the firewall to block the suspicious activity or blocks the suspicious activity itself when used in an in-line configuration.

2.1 Firewall Products Evaluated

Two firewall products were evaluated:

- Check Point Firewall-1 Next Generation-Application Intelligence (NG-AI) R55 on a Nokia IP350 appliance (256 MB RAM, Pentium 3 700 MHz) running Nokia IPSO 3.8.1.

- Symantec Enterprise Firewall 8.0 for Windows on a Dell PowerEdge 1750 (2GB RAM, dual Pentium 4 Xeon 3.06 GHz) running hardened Windows 2000 Server SP4.

2.2 Firewall Selection Process

These two firewall products were selected based on a product literature evaluation of 30 NIAP-validated firewall products from vendors such as Cisco, Netscreen, Check Point, Symantec, Secure Computing, Watchguard, Microsoft, Nortel, 3Com, Borderware, CyberGuard, Lucent, StoneSoft, etc.

The criteria used to select these two firewalls included:

- NIAP-validated, compliant with NIAP Common Criteria requirements, EAL4
- Conforms with the technical requirements of the PERPOS Security Policy
- Uses the latest technologies
- Is Widely Supported and Deployed

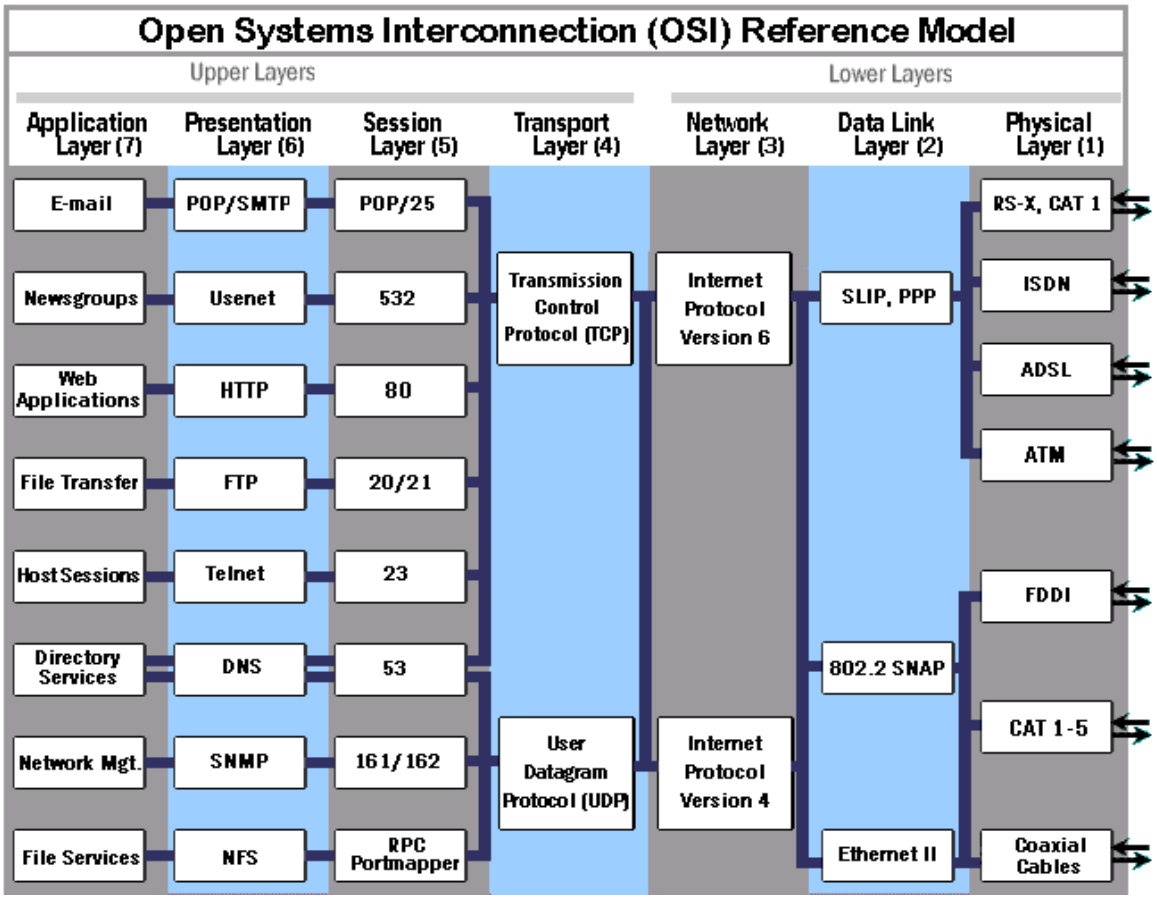
For the full evaluation report, see *Summary Report on Firewall Selection for the PERPOS System*, Son Nguyen, May 26, 2004.

A product literature evaluation is a not an ideal method for selecting a firewall product as it often becomes a comparison of vendor marketing ability rather than firewall ability. An in-house evaluation or "bake off" of the top three or four products selected by a product literature evaluation is preferable. However, budget and time constraints often prevent this type of evaluation, as was the case with the PERPOS Information Assurance project. Additionally, firewall vendors are unlikely to provide long-term loaners of firewalls products when only a single firewall acquisition may result from the loaner.

2.3 Firewall Network Inspection Architecture Overview

Traditionally, firewall network inspection architectures have been placed into four broad categories by network and security literature: 1) packet filters, 2) stateful packet filters, 3) circuit-level gateways or proxies, and 4) application proxies[1][2][3].

To understand firewall products, one should be acquainted with the OSI (Open Systems Interconnection) Reference Model. The OSI Reference Model describes seven layers of related functions that are needed at each end when a message is sent from one party to another party in a network. An existing network product or program can be described in part by where it fits into this layered structure. The figure below shows the OSI Reference Model and examples of communications functions performed in each layer.



The layers are in two groups. The upper four layers are used whenever a message passes to or from a user. The lower three layers are used when any message passes through the host computer. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed up to the upper layers but are forwarded to another host. The seven layers are:

Layer 7: The application layer - This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.

Layer 6: The presentation layer - This layer is usually part of an operating system. It converts incoming and outgoing data from one presentation format to another.

Layer 5: The session layer - This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end.

Layer 4: The transport layer - This layer manages the end-to-end control and error-checking. It ensures complete data transfer.

Layer 3: The network layer - This layer handles the routing and forwarding of data.

Layer 2: The data-link layer - This layer provides synchronization for the physical level. It furnishes transmission protocol knowledge and management.

Layer 1: The physical layer - This layer conveys the bit stream through the network at the electrical and mechanical level.

2.3.1 Packet Filters

Packet filters operate at OSI layer 3 (network) and 4 (transport) of the OSI network model and the decision to forward or discard a packet is made solely on the source or destination IP address or the source or destination port (one or more or all) and sometimes stateless information like packet length and checksums. Every packet is individually inspected against the firewall's rules and the firewall does not consider the packet's relationship to prior packets. Cisco IOS extended access control lists are an example of a packet filter[4].

2.3.2 Stateful Packet Filters

A stateful packet filter inspects packets against a dynamically updated state/connections table in addition to the firewall's rules. The initial packet of a network connection (assuming it is allowed by the firewall's rules) creates a connection entry in the state/connections tables. This connection entry contains the details from the initial packet's OSI layer 3 and 4 headers (e.g. for a TCP packet, the source and destination IP address and source and destination port) and the allowed state for the next packet in the

network connection. The state information held in the table varies among stateful packet inspection architecture implementations but it generally includes OSI Layer 4/5 details such as the TCP sequence number for the next packet, the acceptable set of TCP flags for the next packet, and possibly details from higher OSI network layers. The second packet in the network connection is matched against the connection entry to verify that it conforms to the allowed state. If it conforms, the packet is forwarded, and the connection entry is updated with the allowed state for the next packet. And so on. Linux iptables/netfilter is an example of a stateful packet filter operating at OSI layer 3 and 4[5].

2.3.3 Circuit-level Gateways or Proxies

Circuit-level gateways or proxies are usually implemented at OSI Layer 4 (transport) and 5 (session), inspecting the session establishment process (e.g. the TCP handshake) of a network connection and creating a circuit table with a limited amount of state information about that connection. Data packets in the network connection, i.e., those packets not belonging to session establishment, are not forwarded until the session establishment process is complete. The data packets are generally passed through the "circuit" without any additional inspection beyond OSI layer 4/5 headers. Circuit-level gateways or proxies were not implemented as a standalone firewall product but rather were available as generic proxy servers in application proxy firewall products that act as intermediaries in the network intercepting a network connection from the source and making a new connection on the source's behalf to the destination[6]. The GSP (Generic Services Proxy) in the Symantec Enterprise Firewall and the plug-gw (proxy plug) in Network Associates Gauntlet are examples of circuit-level gateways or proxies[7].

2.3.4 Application Proxies

Application proxies are similar to circuit-level proxies in that they act as intermediaries in the network intercepting a network connection from the source and making a new connection on the source's behalf to the destination. However, application proxies inspect the network connection up through the application layer (OSI layer 7), i.e., each packet must pass checks performed at each layer of the OSI model. Thus, an application proxy is able to differentiate, for example, an email being sent via SMTP on TCP port 25 vs. telnet connection using TCP port 25[2]. Application proxy implementations vary as to the degree or depth of application inspection they do and the types of applications they support.

2.3.5 Hybrid Firewalls

Firewalls today use a mix of the four network inspection architectures. Symantec Enterprise Firewall is marketed as a hybrid security gateway implementing packet filters, stateful inspection, application proxies, and content security[8]. Check Point Firewall-1

is marketed as an application inspection firewall and uses a combination of stateful inspection (and at layers higher than OSI Layer 4 for some protocols) and application proxies (Check Point calls its proxies "Security Servers")[9]. However, modern firewalls still show their network inspection architecture heritage. For example, Check Point uses stateful inspection for most protocols and only has proxies for a few protocols, specifically FTP, HTTP, Common Internet File System (CIFS), and SMTP, and generally only suggests using those proxies for FTP, HTTP, CIFS, and SMTP inspection functionality or checks that cannot be performed by the stateful packet inspection engine[10]. Symantec Enterprise Firewall primarily uses application proxies for protocols and suggests using packet filters or circuit-level proxies for protocols for which it does not have a native application proxy[11].

2.3.6 Deep Packet Inspection Firewalls

As security threats have evolved in sophistication over time, moving largely into the application layer, the firewall, regardless of the types of network inspection architectures it implements, needs to perform inspection at OSI layers 3-7 and integrate some degree of intrusion detection/intrusion prevention system (IDS/IPS) functionality[12]. For example, in 1998, a firewall was expected to protect networks from a LAND attack which operates purely at OSI layer 4 and lower[13]. In 2005, a firewall is expected to protect networks from Microsoft worms spreading via HTTP or CIFS (Windows Networking) or block the Microsoft ASN1.library heap overflow exploit by looking for ASN.1 encoding of GSSAPI structures in the GSSAPI security service (a signature) in protocols such as LDAP, CIFS, SMB, Kerberos, and RPC-DCE[14]. In order to prevent Nimda (a Microsoft worm) from spreading via CIFS, the firewall must inspect the CIFS protocol (OSI layer 7) and look for a specific file pattern (an intrusion signature much like an IDS/IPS product would have).

Firewalls that mix OSI layer 3-7 packet inspection and some degree of IDS/IPS functionality are called "deep packet inspection" (DPI) firewalls[15]. Classifying firewalls by the network inspection architecture they implement (i.e., stateful packet inspection vs. application proxy) was a meaningful comparison in the past as it generally revealed at what layers of the OSI model the firewall performed inspection and thus to some degree the depth of the inspection and the firewall performance. Now that firewalls use a mix of network inspection architectures along with some degree of integrated IDS/IPS functionality to achieve deep packet inspection at OSI layers 3-7, the important classification becomes the depth of inspection. As we shall see, not all firewall products provide the same depth of inspection on each protocol and thus depth of inspection on a per protocol basis should be evaluated.

2.1.4 Firewall Platform Analysis

We discuss three general categories for firewall hardware/software platforms.

2.4.1 Firewall+GPOS

Firewall+GPOS is firewall software that has been installed on a general purpose operating system (GPOS) and commodity computer hardware.

Examples include Symantec Enterprise Firewall 8.0 on a Dell PowerEdge 1750 running Windows 2000 Server or Check Point Firewall-1 NG-AI R55 on a Sun Fire V210 running Solaris 9. How the underlying general purpose operating system is hardened varies from software firewall to software firewall. Some firewall software hardens the GPOS as part of its install process, some firewall vendors leave that process to the end-user, and some firewall software can examine the GPOS in real-time to ensure it stays hardened (e.g., Symantec Enterprise Firewall on Windows has a "vulture" service that disables services and processes that are not strictly needed by Symantec Enterprise firewall or the underlying GPOS and any additional services and processes not specified in the Symantec Enterprise Firewall configuration)[16].

Firewall software installed on GPOS and commodity computer hardware does allow the end-user to achieve relatively good performance numbers at a low cost by leveraging low-cost but high-performance commodity computer hardware. However, the accounting or dollar cost of the GPOS, commodity computer hardware, and firewall software combination does not represent the total cost of ownership since it fails to include management costs associated with performing the actual initial hardening of the OS, the management cost associated with ensuring that the real-time hardening and protection mechanisms are functioning properly and are updated to take into account changes in the underlying GPOS, the security risk cost associated with improper or incomplete hardening, and, because there is a lose coupling of the firewall software and the underlying GPOS, the cost of updating two separate software platforms.

2.4.2 Firewall+HOS

Firewall+HOS is firewall software that has been coupled with a hardened operating system (HOS), often offered on hardware appliances, and may use network processors or Application-Specific Integrated Circuits (ASICs) to greatly enhance performance.

Firewall vendors may offer the firewall software + hardened OS on a vendor-supplied appliance (e.g. Secure Computing Sidewinder G2 appliances are Sidewinder G2 firewall software on top of a hardened BSDI OS installed on a hardware appliance made for Secure Computing by Dell[17]), may offer the firewall software + hardened OS as a software product that can be installed on commodity PC hardware (e.g. Check Point SecurePlatform which is Check Point Firewall-1 on Check Point's version of a hardened Linux OS[18]), or available for install on third-party appliances (e.g. Check Point SecurePlatform on Corrent appliances). There are some variations on this category. For example, Crossbeam and Nokia sell appliances bundled with a hardened OS (hardened, Linux-based OS called XOS/COS and hardened FreeBSD-based OS called Nokia IPSO respectively[19][20]) and Check Point Firewall-1 is installed onto these appliances.

These firewall platforms may use ASICs and/or network processors to significantly increase performance beyond firewall+GPOS platforms by off-loading certain functions from the main CPU onto ASICs/network processors such as crypto operations, connection establishment, etc[21]. Check Point Firewall-1 on Crossbeam X80 is an example of a firewall+HOS platform that achieves 8 Gbps of performance through the use of network processors[19][22].

With these firewall platforms, no time must be spent hardening the underlying operating system as the appliance or firewall vendor has already provided a hardened OS. This tighter coupling or integration of the firewall software and operating system arguably results in greater security and possibly greater performance as the vendor (or partnerships among vendors) can produce more optimized hardware/software combinations[21]. The degree to which the firewall software and underlying OS are coupled impacts the cost associated with the management of underlying OS. For example, Check Point SmartUpdate can upgrade Nokia IPSO on a Nokia appliance (with the proper license) but certain Nokia IPSO tasks such as defining network interface parameters must be performed via Nokia's web-based interface (Nokia Voyager) or centralized management tool (Nokia Horizon Manager). In this example, there are two distinct management platforms: Check Point SmartTools (which includes SmartUpdate) and Nokia Voyager and/or Horizon Manager. Other firewall platforms, such as Fortinet's appliances, provide a very tight coupling of the underlying hardened OS (Linux-based and called "FortiOS") and the firewall software[23]. With a Fortinet firewall, you only have to update FortiOS. The reason some vendors in this category such as Nokia have not as tightly coupled the operating system to the firewall software is that their platform is used to run multiple third-party security applications rather than just a specific firewall software. For example, Crossbeam appliances can run IDS/IPS products from Enterasys, Snort, and Internet Security Systems and Nokia appliances can run Nokia Secure Access SSL VPN software.

2.4.3 FSOS

FSOS is a firewall/security operating system offered on hardware appliances and may use network processors or ASICs to improve performance.

Cisco PIX and Netscreen firewalls run an operating system specifically designed to perform tasks of a firewall (packet inspection, NAT, routing, etc.) and nothing more. They are not hardened versions of a commercial or open source GPOS. Cisco PIX runs PIX software, sometimes referred to as "PIX OS", and Netscreen firewalls run "ScreenOS". Although programmatically within these FSOS's there could be a separation between the firewall software and OS software (for example, PIX and FWSM run the real-time operating system [RTOS] Finesse), this separation is not perceived by the end-user. Arguably, these types of firewalls are less easily exploited by attacks that target the firewall itself since the underlying OS is nearly completely obscured as it is closed source and is not a derivation of or a hardened version of a widely used commercial or open source GPOS whose source code is widely available. However, the

obscurity advantage is largely moot at least for the Cisco PIX architecture as its source code was leaked[24]. These firewall platforms may also use network processors and/or ASICs to increase performance by off-loading certain functions from the main CPU onto the ASIC/network processors such as crypto operations, connection establishment, etc. The Cisco Firewall Services Module is an example of a FSOS platform that achieves 5 Gbps of throughput through the use of network processors. The Netscreen 5400 is an example of a FSOS platform that achieves 12 Gbps of throughput through the use of ASICs[25].

The fact that these firewalls offer the tightest possible coupling of firewall software and underlying operating system means there is only one piece of software to update and are arguably the most optimized for performance. However, with an increasing number of vendors offering firewall appliances that offer a very tightly coupled and optimized firewall+HOS platform (e.g., Fortinet, Watchguard, and Symantec Security Gateways), there can very little meaningful differences between the FSOS and firewall+HOS platforms from performance and management standpoints.

2.4.4 Choosing a Firewall Platform

Firewalls+HOS and FSOS appliance platforms dominate the firewall platform market and even those vendors that offer both firewall software for installation on a GPOS and appliances such as Symantec are putting more R&D into their appliance platforms[26]. Check Point has reduced the number of GPOS's it supports in recent releases. Secure Computing Sidewinder G2 is only available on appliances when in the past it was available on Windows and Solaris. Table 1 shows the platform offerings from the leading firewall vendors.

Firewall Vendor	**Platforms Offered**
Check Point	Firewall+GPOS and 50% appliances[26]
Cisco	Only appliances
StoneSoft	Firewall+GPOS and appliances
Juniper Netscreen	Only appliances
Nortel	Only appliances
Sonicwall	Only appliances
Watchguard	Only appliances
Fortinet	Only appliances
3Com	Only appliances
Secure Computing	Only appliances
F5	Only appliances
Netgear	Only appliances
Linksys	Only appliances

Table 1: Firewall Platform Offerings by Vendor

There is no reason to select a Firewall+GPOS platform over an appliance platform for new firewall installations since the Firewall+GPOS platform has higher management cost, higher security risk cost, a lack of ASIC/network processor acceleration options, and a dying market share. The choice between a firewall+HOS or FSOS appliance platform should be based primarily on which firewall meets your network security and functionality needs while taking into account the respective management costs.

From a purely firewall platform selection standpoint, Symantec Enterprise Firewall 8.0 on Window 2000 Server was a poor choice for PERPOS for the various reasons discussed above. A significant amount of time was spent hardening the underlying GPOS, Windows 2000 Server, per the Microsoft Windows 2000 Security Hardening Guide[27], including a failed hardening attempt that resulted in an unusable Windows 2000 Server system. A Symantec Security Gateway appliance which uses a hardened version of Linux[28] would have been a better choice if the project budget had permitted its selection.

2.5 Firewall Software Evaluation

2.5.1 Depth of Inspection

Symantec Enterprise Firewall 8.0 and Check Point Firewall-1 NG-AI R55 are marketed as application inspection firewalls but they vary in their depth of inspection on a per protocol basis.

Symantec and Check Point provide deep inspection of the HTTP, SMTP, CIFS, and FTP protocols through the use of protocol anomaly detection (i.e. enforce protocol RFC standards and normal use models to block exploits) and protocol functionality restrictions (e.g. only allow these SMTP commands). However, Check Point's SmartDefense Subscription Services allows Check Point Firewall-1 to receive signature updates for worms, exploits, and malware whereas Symantec relies on the end-user to add patterns to the Symantec firewall proxies to block worms, exploits, and malware. For example, the Check Point SmartDefense Subscription Service provided a signature with the pattern to block the Code Red worm. With Symantec, the end-user had to manually add the Code Red pattern to the HTTP proxy in Symantec[29]. For other exploits, Symantec lacks the flexibility to provide protection even manually. For example, certain versions of Samba (a popular CIFS implementation for UNIX servers) were susceptible to a buffer overflow by using long CIFS passwords[30]. Check Point SmartDefense Subscription Service provided a signature to block overly long passwords. Symantec does not provide a means to restrict the password length on its CIFS proxy.

Symantec arguably provides deeper SMTP inspection than Check Point as it allows emails to be checked against RBL (Realtime Blackhole Lists—public lists of known spammers)[31]. Since most organizations use dedicated hardware/software solutions to handle spam, viruses, and other dangerous content in email, the value of being able to check email against RBL's in the firewall seems limited. If PERPOS is to accept

unsolicited email from the Internet, i.e. run an SMTP mail server, open source and commercial software and appliance-based email filtering solutions should be investigated, e.g. MailScanner, NWTech IronWall, Sophos PureMessage, Barracuda Networks Spam Firewall, Aladdin eSafe Mail, McAfee eShield, SurfControl RiskFilter, ad nauseam.

Symantec does allow for HTTP content filtering by restricting access to URLs based on 13 categories, e.g. Alcohol-Tobacco, Gambling, Sex, etc.. These precompiled URL categories are downloaded from Symantec[32]. Check Point requires that third-party, off-box URL filtering product such as Websense or SurfControl to provide this feature. However, Symantec's URL categories in Symantec Enterprise Firewall 8.0 are out-dated compared to the third-party URL category providers. For example, compared to SurfControl, Symantec lacks a malware/spyware category and phishing/fraud category and Symantec has 13 categories compared to SurfControl's 47 categories[33].

For the Microsoft SQL monitor and server protocols, Check Point provides protection against blank passwords, blocks several buffer/heap overflows, blocks a denial-of-service (DoS) attack, blocks version information leaks, allows you to enforce Windows Authentication, and allows you to block certain stored procedures commands[34]. Symantec does not provide deep inspection of the Microsoft SQL protocols. Since PERPOS is using Oracle database, Check Point's deep packet inspection of Microsoft SQL Server protocols is of little value.

Disappointingly, Symantec and Check Point do not provide deep packet inspection of Oracle database protocols. Although Check Point does appear to have some awareness of the SQLNet Version 2 protocol, it does not provide any Oracle database-specific protections.

A Symantec Security Gateway appliance which uses a hardened version of Linux and integrates IDS/IPS functionality and Symantec anti-virus scanning with Symantec Enterprise Firewall[28] would have been a better choice if the project budget had permitted its selection.

2.5.2 Check Point SecureXL and Symantec Disabled Application Data Scanning: Increased Performance via Reduced Security

Check Point Firewall-1 NG-AI R55 on IPSO 3.8/3.8.1 can make use of the Check Point SecureXL API which allows for increased performance by changing how Check Point does its inspection. Check Point does less inspection on packets in the middle of a connection than packets at the beginning of the connection. With SecureXL enabled, Check Point is not able to do perform TCP sequence number verification and it can't do TTL and IP ID sequence number fingerprint scrambling. With SecureXL enabled, Check Point is arguably a less secure firewall because it does not maintain full TCP state and also allows systems behind the firewall to be identified more easily because it is not scrambling certain aspects of the IP protocol that could reveal the operating system[35].

Symantec, as an application or circuit-level proxy firewall, will always perform TCP sequence number verification because it is intercepting connection and making new connections on behalf of the source. If the TCP sequence numbers of a packet are out of state, Symantec will consider the packet bad and drop it. Symantec is always doing fingerprint scrambling because it always makes a new connection with the TTL and IP ID generated by the firewall itself (assuming packets aren't passing solely through its packet filters). However, if you disable Application Data Scanning, Symantec is bypassing the proxy after the initial packets and cannot perform TCP sequence number verification. It's unclear from the Symantec documentation if the firewall is doing IP-level fingerprint scrambling as this may be done in the Symantec security driver rather than the proxy[36].

Symantec Enterprise Firewall 8.0 has application data scanning enabled by default (more secure) and Check Point Firewall-1 NG-AI R55 on Nokia IPSO has SecureXL enabled by default (less secure) and Check Point performance numbers on a given platform may be quoted with SecureXL enabled. In other words, when evaluating performance or cost/performance of Symantec vs. Check Point, it's important to realize that Check Point's numbers may reflect a reduced security configuration compared to Symantec.

2.6 Firewall Network Configuration

2.6.1 Single firewall

The firewall network configuration or firewall network topology currently used on PERPOS places the web server on a dedicated DMZ interface and the database and archive server on a dedicated internal or inside interface and is shown in Figure 1.

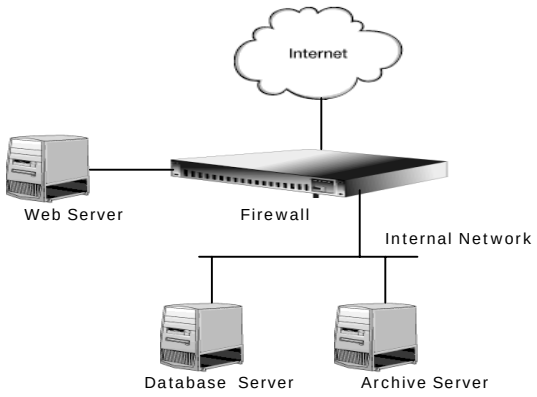


Figure 1: PERPOS Network Configuration

This type of network configuration allows for the best security with a single firewall as it allows you to configure the firewall such that Internet systems cannot initiate connections with internal network systems and optionally DMZ systems cannot initiate connections with inside systems (for PERPOS, the DMZ must talk to the database server on the

internal network). For example, if a system is compromised in the DMZ, the firewall is still providing some degree of protection to the internal systems. If there was only an outside (Internet) interface and inside (internal network) interface, a compromised web server would have unrestricted access to the database and archive servers.

2.6.2 Layered Firewalls create True DMZ

A more secure network configuration involves using two firewalls in a layered approach as shown in Figure 2.

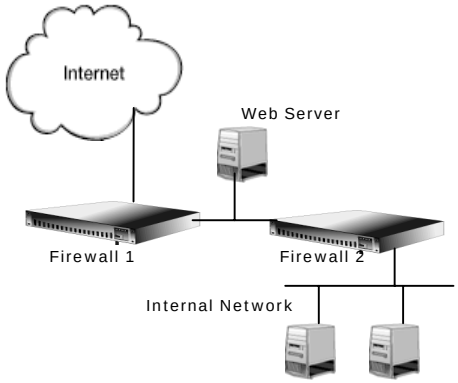


Figure 2: PERPOS Network Configuration with Two Firewalls

This type of network configuration is sometimes called a "true DMZ". From a security standpoint, there is arguably little increase in security if you use the same firewall product for front (Firewall 1) and back (Firewall 2) firewalls as the same configuration errors may be duplicated and any vulnerability which is present on the front firewall will likely exist on the back firewall. Using different vendors for the front and back firewall, especially if one has a greater depth of inspection for those protocols relevant for Internet<->DMZ vs. DMZ<->Internal, provides better security as you obtain deeper protocol inspection only where you need it and possibly avoid vendor-specific vulnerabilities and firewall-specific configuration errors[37]. However, using multiple vendors in a true DMZ configuration causes a dramatic increase in management cost (increased training and/or required skill set of firewall administrator, two different types of log formats to parse/analyze, two or more support contracts to manage, two or more vendors to work with on support issues, etc.).

2.7 Firewall Performance during DDoS attack

Researchers at Emory University made available to the PERPOS project an in-house and unreleased firewall stress tool for Linux called "fw-stress" that they've used to evaluate firewall platforms' ability to deal with distributed denial-of-service (DDoS) attacks.

```
[jkau@linuxbox ~]$ fw-stress
fw-stress> help
TSUNAMI <target> <secs>      = Special packeter that wont be blocked by
                               most firewalls
PAN <target> <port> <secs>   = An advanced syn flooder that will kill most
                               network drivers
```

```
UDP <target> <port> <secs>    = A udp flooder
UNKNOWN <target> <secs>       = Another non-spoof udp flooder
GETSPOOFS                     = Gets the current spoofing
SPOOFS <subnet>               = Changes spoofing to a subnet
KILL                          = Kills the client
GET <http address> <save as> = Downloads a file off the web and saves it onto
                                the hd
VERSION                       = Requests version of client
KILLALL                       = Kills all current packeting
HELP                          = Displays this
QUIT                          = Disconnect (net mode) or
                                End Program (interactive mode)

fw-stress>
```

We ran fw-stress on a Pentium 4 2.4 GHz / 512 MB system connected at 10 Mbps full duplex. fw-stress was configured for "pan" mode with "spoofs" set to the entire Internet (0.0.0.0 – 255.255.255.255). With this configuration, fw-stress simulated a DDoS (distributed denial of service) SYN flood attack. Table 2 shows the results of throughput tests using curl and iperf between a system outside the firewall and a system in the DMZ.

Firewall Product	Curl throughput	Iperf throughput
Symantec	0 Mbps	0 Mbps
Check Point	0 Mbps	0 Mbps

Table 2: Throughput Under Simulated 10 Mbps DDoS Attack

Regardless of SYN flood protection configuration of these firewall products, neither was able to provide any degree of protection from or mitigation of a DDoS SYN flood attack at 10 Mbps. The results were not different when the simulated DDoS attack was directed at the IP address of the external interface of the firewall vs. the IP address of a system in the DMZ.

If either of these two firewall platforms is to be used in a production environment, DDoS protection must be achieved upstream via a router performing SYN flood limiting, via an in-line IPS that provides protection against rate-based attacks, or via a firewall platform with built-in DDoS protection such as Corrent's appliances for Check Point[38]. Some DDoS attacks can only be mitigated by contacting the upstream network provider/Internet service provider and asking for the traffic to be blocked. The likelihood of PERPOS being the target of a DDoS attack is beyond the scope of this report.

2.8 Firewall Conclusions

- Not all firewalls have the same depth of protocol inspection for a given protocol and not all firewalls do deep packet inspection for the same set of protocols. Hence, firewalls should be classified by the degree to which they do deep packet inspection and on a per protocol basis.

- Firewall appliances should be used instead of firewall+GPOS (general purpose operating system) in order to provide increased security, reduced management costs, optimized configurations, and higher performance through the use of ASICs/network processors.
- When evaluating firewall+HOS (hardened operating system) platforms, the degree of coupling and integration of the firewall software and the hardened operating system can impact the management cost of the platform.
- Symantec Enterprise Firewall 8.0 for Windows was a poor choice from both a firewall platform perspective and a security and feature perspective compared to Check Point Firewall-1 NG-AI R55 on Nokia IP350. A Symantec Security Gateway appliance which integrates Symantec Firewall with IDS/IPS functionality and anti-virus would have been a better choice from both perspectives and been a more comparable product to Check Point Firewall-1 NG-AI R55.
- Neither Check Point Firewall-1 NG-AI R55 nor Symantec Enterprise Firewall 8.0 provide for deep packet inspection of Oracle database protocols.
- Neither Check Point Firewall-1 NG-AI R55 on a Nokia IP350 running IPSO 3.8.1 nor Symantec Enterprise Firewall 8.0 on a Dell PowerEdge 1750 running Windows 2000 Server provide any degree of DDoS SYN flood attack protection. If either of these platforms is to be used in a production environment, DDoS protection must be provided by the upstream (e.g., router with SYN rate limiting, in-line IPS with rate-based attack protection, upstream provider) or by choosing a new firewall platform with built-in DDoS attack protection.

2.9 Firewall Future Tasks

- Investigate firewall solutions that provide deep packet inspection of protocols for used on PERPOS, specifically Oracle database protocols.
- More thoroughly investigate solutions to provide DDoS protection.

3. Vulnerability Assessment

3.1 The Need for Vulnerability Assessment

Vulnerability assessment scanners provide a snapshot in time of possible vulnerabilities on the network including those that could exist within a firewall and IDS/IPS product[39]. As firewalls and IDS/IPS products become more complex they are more likely to be susceptible to exploits themselves. The Snort (a popular open source IDS) RPC preprocessing vulnerability and the Check Point Firewall-1 H.323 vulnerability are recent examples of vulnerabilities in deep packet inspection firewall and IDS/IPS products[15]. As a side-effect of their primary function of discovering vulnerabilities, vulnerability assessment scanners also provide an inventory of network system profiles

by identifying MAC addresses, IP addresses, operating systems, services, applications, ports, inferred patch level, etc[41].

Vulnerability assessment scanners can also ensure that end-system security policies and security configurations are followed. For example, it is not inconceivable that end-users or even system administrators will become less vigilant about installing patches, hot fixes, security updates, etc. when they feel their system is protected by a perimeter firewall and/or perimeter IDS/IPS. If this type of behavior occurs and the firewall/IDS/IPS fails to block an exploit or attack at some point, an internal break-out of a worm can occur, taking down end-systems, compromising sensitive information, and possibly adversely impacting the internal network performance and availability. Vulnerability assessment scanners can also help identify unnecessary services running on a system, assisting with the hardening of servers. Shutting down unnecessary services, even if they're not subject to any known vulnerabilities, reduces the chance of being exploited/attacked when the unnecessary services do become vulnerable in the future (and arguably it's only a matter of "when" and not "if"). Thus, regular "inside the firewall" scanning should be performed to minimize these risks. Additionally, we feel that "outside the firewall" scanning should be used to verify that firewall rules are configured correctly/working as expected, that inadvertent external access to internal resources has not occurred, and that the firewall is not leaking information about the internal network or the firewall products themselves that could be used by hackers trying to penetrate the firewall. However, deep packet inspection firewalls can generate false positives when performing "outside the firewall" vulnerability assessment scanning.

The degree to which the PERPOS systems are centrally managed, the size of the networks supporting the PERPOS system, and the types of servers used determines the mix of vulnerability assessment tools that should be used. For example, appliance-based passive assessment devices are designed for large networks and are probably not cost effective if the PERPOS system is comprised of a handful of servers distributed across the Internet. As another example, host-based vulnerability assessment scanners may not provide much value if the server operating system is Linux and the market for host-based scanners has focused on Windows server operating systems.

3.2 Vulnerability Assessment Tools

There are generally two types of vulnerability assessment scanners: 1) network-based scanners that actively scan the network such as Nessus, Internet Security Systems (ISS) Internet Scanner, and Symantec NetRecon and 2) host-based scanners such as Microsoft Baseline Security Analyzer, ISS System Scanner, and Symantec Enterprise Security Manager. Host-based scanners can provide more information about a host by examining system logs and by looking for vulnerabilities not directly tied to network services/servers. Host-based scanners also have a lesser impact on the network as they generally only use the network to report back to a central management server/console whereas network-based scanners use the network to generate simulated attacks and scan the host. Additionally, network-based scanner deployments require careful planning to

avoid conflicts with other security systems such as firewalls and IDS/IPS products and may generate sufficient network traffic to cause network problems. Deployment of host-based scanners are more costly than network-based scanners because the software must be installed on every desktop whereas network-based scanners are installed on a central scanning host or set of scanner hosts and increasingly are available as appliances[40].

There is a new breed of network-based vulnerability assessment products called Passive Assessment Tools (PAT). Instead of actively scanning the network, they passively listen to network traffic as it passes-by much like a traditional IDS deployment and attempt to determine vulnerabilities and network system profiles (MAC addresses, IP addresses, operating systems, services, applications, ports, etc.). Unlike active scanners, passive assessment tools also provide an inventory of changes in the network over time without constant scanning, i.e. when new systems come online, behavioral changes old assets (new services, ports, etc.), when new applications occur on the network, etc.[41]. Additionally, passive assessment can discover vulnerable client applications by inspecting the traffic they generate. Active vulnerability assessment scanners cannot detect client applications because they generally do not respond to the network probes initiated by active scanners [42].

Passive and active network assessment tools often have feedback relationship with IDS/IPS products. Assessment results are often fed into IDS/IPS products to weed out false positives or de-prioritize attacks that won't affect network targets. The relationship can also work in the other direction were alerts from IDS/IPS product can trigger active network scans[40].

3.3 Vulnerability Assessment Selection Process

Two vulnerability assessment network scanner products, Nessus 2.2.4 and Internet Security Systems (ISS) Internet Scanner 7.0 SP2, were evaluated on their ability to detect vulnerabilities and the usefulness and depth of their reports. These vulnerability assessment network scanners were also used to provide vulnerability assessment for PERPOS project systems and firewalls. We selected Nessus and ISS Scanner because Nessus appears to be the most popular open source vulnerability assessment scanners and it's free. We chose ISS Internet Scanner because it appears to be a popular commercial vulnerability assessment scanner, Georgia Tech has a site license, and because ISS Scanner has done well in network trade magazine reviews in the past[43]. Using multiple vulnerability assessment tools reduces the risk that a potentially serious vulnerability will be missed as a scanner's configuration and freshness of signatures can greatly impact its ability to successfully find vulnerabilities. For example, if ISS Scanner is installed on a host system running Windows XP Service Pack 2 (SP2) or the host system is upgraded to SP2, the quality of the scans will be reduced because ISS Scanner uses "raw sockets" which were removed from SP2. The ISS Scanner Console does not produce any error message indicating that the lack of raw sockets has reduced the quality of its scans. Without having an additional scanner to compare ISS Scanner results against, a lot of vulnerabilities may go undetected.

Internet Security Systems says: "Customers will not be able to scan as accurately or as fast due to the changes that Microsoft made to its OS. For example, our tests showed that comparative scans on XP SP2 vs. XP SP1 were as much as four times slower and found approximately 40% fewer vulnerabilities…"

Table 3 is a feature comparison of ISS Scanner and Nessus.

Feature	ISS Scanner	Nessus
Automatic signature updates	Yes	Yes
Custom security checks	No	Yes
Integrates with data management or security manage suite	Yes	No
3rd party references in reports	Yes	Yes
Audience-targeted reports	Yes	No
Pause Active Scans	Yes	No
Limit connections/scan rate	Yes	Yes
Enabling/disabling of DoS scans	Yes	Yes

Table 3: Vulnerability Assessment Network Scanner Feature Comparison

Both support automatic signature updates via the Internet and third-party references (CVE, CERT, product vendor, etc.) in the reports to details on the vulnerability and remediation information, and allow you to limit the simultaneous connections/scan rate in order to adversely impact the network or overload systems, and enable/disable scans that perform DoS tests/attacks.

ISS Scanner is capable of generating audience-targeted reports such as executive reports, line management reports, and technician reports. For example, an execute report is appropriate for an IT executive who needs to know the mix of high vs. medium vs. low vulnerabilities in their organization, their type, and systems impacted, but not the extensive remediation and references. ISS Scanner allows the scans to be paused. This is useful if you only want to run scans after-hours or during a specific time windows and the scan is going to take longer than overnight or during your time window. ISS Scanner can be integrated within a larger data and security management suite called ISS SafeSuite/SiteProtector[44]. However, there are third-party commercial security management suites that use Nessus as their network vulnerability assessment scanner. Nessus allows for custom signatures via its Nessus Attack Scripting Language (NASL).

3.4 "Outside the Firewall" Vulnerability Assessment Results

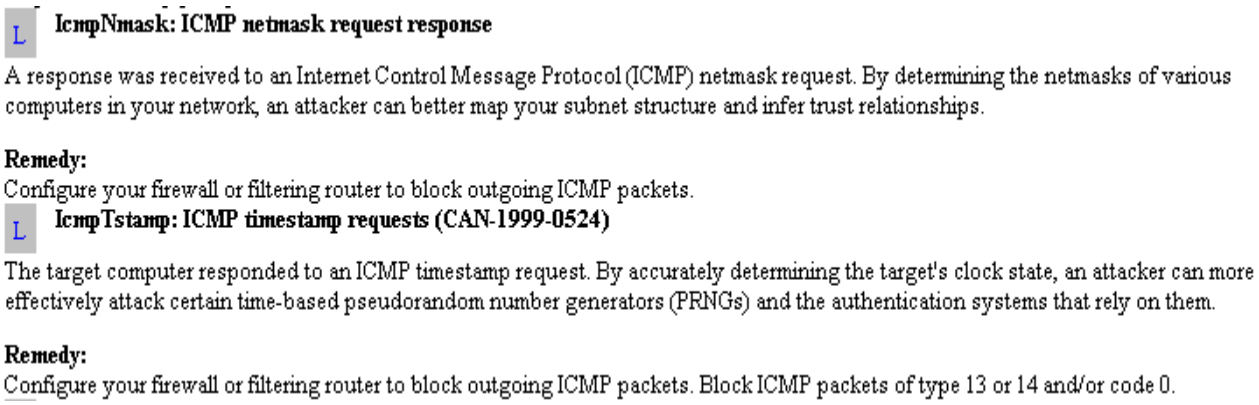
Rather than include the full ISS Scanner and Nessus "outside the firewall" reports which would take up hundreds of pages, we focus on those specific sections of the reports that illustrate why "outside the firewall" vulnerability assessment scanning is necessary in order to verify that firewall rules are configured correctly/working as expected, that inadvertent external access to internal resources has not occurred, and that the firewall is

not leaking information about the internal network or the firewall products themselves that could be used by hackers trying to penetrate the firewall.

3.4.1 ICMP being allowed through Check Point

Both ISS Scanner and Nessus identified that Check Point Firewall-1 was allowing unnecessary ICMP traffic through the firewall that could be used to reveal information about the internal networks and allow hackers to attempt to use time-based attacks. This was surprising as we did not explicitly allow ICMP in the Check Point security rule base. Investigation of the Check Point documentation revealed that Check Point by default allows ICMP traffic in the "implicit rules". Nessus provided better remediation information for blocking ICMP netmask requests as it told us the exact ICMP type to block.

ISS Scanner:



IcmpNmask: ICMP netmask request response

A response was received to an Internet Control Message Protocol (ICMP) netmask request. By determining the netmasks of various computers in your network, an attacker can better map your subnet structure and infer trust relationships.

Remedy:
Configure your firewall or filtering router to block outgoing ICMP packets.

IcmpTstamp: ICMP timestamp requests (CAN-1999-0524)

The target computer responded to an ICMP timestamp request. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

Remedy:
Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 13 or 14 and/or code 0.

Nessus:

Warning found on port general/icmp

The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.0).

An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters.

Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17.

Risk factor : Low
CVE : CAN-1999-0524
Nessus ID : 10113

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

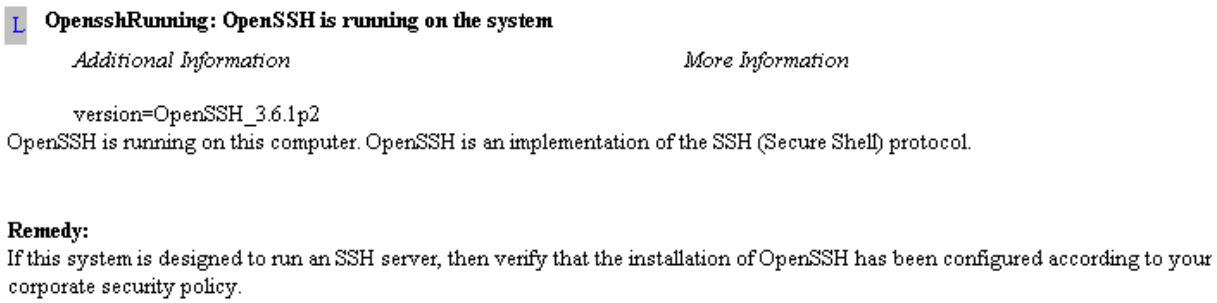
Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524
Nessus ID : 10114

3.4.2 ISS Scanner fails to recommend OpenSSH security enhancements

Both ISS Scanner and Nessus identified that we were allowing SSH access to the web server from the Internet and the SSH server product/version but Nessus suggested better remediation information, i.e. changing to SSH protocol 2 which is technically more secure. Nessus also reports the types of SSH authentication supported by the SSH server.

ISS Scanner:



Nessus:

Warning found on port ssh (22/tcp)

> The remote SSH daemon supports connections made
> using the version 1.33 and/or 1.5 of the SSH protocol.
>
> These protocols are not completely cryptographically
> safe so they should not be used.
>
> Solution :
> If you use OpenSSH, set the option 'Protocol' to '2'
> If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

Risk factor : Low
Nessus ID : 10882

Information found on port ssh (22/tcp)

An ssh server is running on this port
Nessus ID : 10330

Information found on port ssh (22/tcp)

Remote SSH version : SSH-1.99-OpenSSH_3.6.1p2
Remote SSH supported authentication : publickey,password,keyboard-interactive

Nessus ID : 10267

Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the
SSH protocol :

. 1.33
. 1.5
. 1.99
. 2.0

SSHv1 host key fingerprint : 83:2a:9c:ed:84:f3:a3:2d:70:62:ea:5e:b0:fa:18:7c
SSHv2 host key fingerprint : 18:34:74:7c:39:96:c2:7a:b6:ff:3a:a3:c8:d5:c9:5c

Nessus ID : 10881

3.4.3 ISS Scanner reports false positives for Nokia Voyager

The ISS Scanner report indicates the Nokia IPSO web-based management interface, Nokia Voyager, has an Apache cookies vulnerability and several potentially exploitable CGI scripts. After checking Nokia and investigating the IPSO web server directory tree, these appear to be false positives. Also, Nessus does not report any of these potential vulnerabilities lending additional support that these are false positives. Nessus reported the correct Nokia Voyager CGI scripts.

ISS Scanner:

H **Apache cookie: Apache cookies buffer overflow**

The Apache HTTP server has an optional module mod_cookies that could allow a remote attacker to overflow an internal buffer in the Web server and execute arbitrary bytecode on the Web server. The mod_cookies module is compiled into the Web server, and is not installed by default in any versions of Apache. Apache HTTP servers up to v1.1.1 may be vulnerable to this overflow, if this module has been compiled into the server.

Remedy:
This vulnerability only affects sites running Apache 1.1.1 or below with the cookies modules compiled into the server. Upgrade to the latest version of Apache (1.1.2 or later), as listed in Network Associates, Inc. COVERT Labs Security Advisory #02. See References.

M **CGI nphpublish: nph-publish CGI script could allow remote file writing (CVE-1999-1177)**

Lincoln D. Stein's nph-publish script is a Perl CGI script for Apache HTTP servers. A vulnerability in nph-publish versions 1.0 through 1.1 could allow a remote attacker to write to files that would normally not be accessible. Under certain circumstances, this vulnerability could be used to gain access to a vulnerable system.

Remedy:
Remove the vulnerable version of nph-publish from your CGI-BIN directory.

--AND--

Upgrade to the latest version of the nph-publish script (1.2 or later), available from the Lincoln D. Stein Web site. See References.

M **HttpCgiCounterLong: Counter.exe Web hit counter is vulnerable to a denial of service attack (CAN-1999-1031)**

Behold! Software Web Page Counter version 2.7 is vulnerable to a denial of service attack. A vulnerability in the Counter.exe program could allow a remote attacker to send a specially-crafted URL to cause error messages to appear on the console. This will prevent the program from responding to further requests. Until an administrator OKs the error messages on the console, the program will not respond to further requests.

Remedy:
No remedy available as of June 2002.

L **FormmailInstalled: FormMail is installed on this computer**

Matt Wright's FormMail CGI program is a Web-based email gateway written in Perl. FormMail is installed on this computer.

Remedy:
If this system is intended to run FormMail, then verify that the installation of FormMail has been configured according to your corporate security policy. See References.

Nessus:

Information found on port https (443/tcp)

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/cgi-bin (userName [] userPass [] getLock [x] Login [])
/cgi-bin/ (D [A] Login [] userPass [] getLock [x] userName [])
/cgi-bin/home.tcl (Login [] overrideLock [t] userPass [] getLock [x] userName [])

Nessus ID : 10662

3.4.4 Nessus reports false positive for buffer overflow

"Outside the firewall" scanning can result in false positives depending on how the firewall operates. Nessus found that port 80 to the web server was open through the Check Point firewall and sent a long URL as part of its buffer overflow tests. Check Point recognizes this as a Long URL attack and blocks the connection by sending back a TCP RST. This causes Nessus to think the web server was crashed due to a buffer overflow. ISS Scanner did not report a buffer overflow for this service lending additional support that this is a false positive.

Vulnerability found on port http (80/tcp)

It may be possible to make a web server execute
arbitrary code by sending it a too long url after
/jsp.
Ie:
GET /jsp/AAAA.....AAAAA

Risk factor : High
Solution : Contact your vendor for the latest software release.
CVE : CAN-2001-0419
BID : 2569
Nessus ID : 10654

3.4.5 Proxy/Security Server banners allow the firewalls to be identified

Both ISS Scanner and Nessus were able to ID the Check Point Firewall because the Check Point Security Servers (Check Point's term for its application proxies) were set at their defaults for the server banners. Nessus also made an educated guess as to the Check Point version, stating it was "NG FP4" which a knowledgeable network administrator or hacker would realize means "NG-AI" as it was the release following "NG FP3". Nessus was also able to ID the Symantec Firewall as both "Raptor" (the name for Symantec Enterprise Firewall before Symantec acquired it from Axent and rebranded it) and "Symantec Enterprise Firewall" based on information from the DNS proxy.

ISS Scanner:

perpos-gate.gtri.gatech.edu {130.207.204.11} Check Point FireWall Reachable

Service Details:

Service Name	*Short Description*	*Port #*	*Type*
ftp	File Transfer [Control]	21	TCP
https	https MCom	443	TCP
ssh	SSH Remote Login Protocol	22	TCP

Banner Details

Banner Type	*Banner Text*
FTP	220 Check Point FireWall-1 Secure FTP server running on perpos-gate
HTTPS	Apache
ftp	220 Check Point FireWall-1 Secure FTP server running on perpos-gate\0d\0a
ssh	SSH-1.99-OpenSSH_3.1p1\0a
Service	220 Check Point FireWall-1 Secure FTP server running on perpos-gate\0d\0a
Service	SSH-1.99-OpenSSH_3.1p1\0a

Nessus:

Information found on port ftp (21/tcp)

An FTP server is running on this port.
Here is its banner :
220 Check Point FireWall-1 Secure FTP server running on perpos-gate

Nessus ID : 10330

Information found on port smtp (25/tcp)

An SMTP server is running on this port
Here is its banner :
220 Check Point FireWall-1 secure ESMTP server

Nessus ID : 10330

Information found on port smtp (25/tcp)

Remote SMTP server banner :
220 Check Point FireWall-1 secure ESMTP server

This is probably: Check Point FireWall-1
Nessus ID : 10263

Information found on port smtp (25/tcp)

This server could be fingerprinted as being Check Point NG FP4

Nessus ID : 11421

Information found on port http (80/tcp)

The remote WWW host is very likely behind Raptor FW Version 6.5
You should patch the httpd proxy to return bogus version and stop
the information leak

Nessus ID : 10730

Information found on port domain (53/udp)

The remote name server could be fingerprinted as being : Symantec Enterprise Firewall 6

Nessus ID : 11951

3.5 "Inside the Firewall" Vulnerability Assessment Results

Extensive "inside the firewall" scanning of all PERPOS systems has not yet been performed. However, initial "inside the firewall" scans have been performed that show the value of "inside the firewall" vulnerability assessment scanning.

3.5.1 PERPOS development system Oracle vulnerabilities

One of the PERPOS development boxes was intentionally left un-patched and un-updated behind a firewall (to prevent it from infecting other systems or being exploited) in order to test the effectiveness of ISS Scanner and Nessus at detecting Oracle vulnerabilities in this system. Both ISS Scanner and Nessus detected multiple Oracle database and application server vulnerabilities. It's hard to say which scanner has made a more accurate vulnerability assessment but it does appear that Nessus detected more specific Oracle vulnerabilities. ISS Scanner provides more third-party references to the potential vulnerabilities.

ISS Scanner:

H **OracleAppserverLocationBo: Oracle9i Application Server Apache PL/SQL HTTP Location header buffer overflow**

Vuln count = 2

Additional Information *More Information*

port=443

port=80

Oracle9i Application Server version 1.0.2.x is vulnerable to a buffer overflow in the Apache PL/SQL Web module. By sending a specially-crafted request for a Help page without specifying a Database Access Descriptor (DAD), a remote attacker could overflow a buffer in the HTTP Location header and execute arbitrary code on the system or cause the Apache service to crash.

Remedy:

Apply the appropriate patch for your system, as listed in Section 1 of Oracle Security Alert #28. See References.

References:

CERT Vulnerability Note VU#313280, Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP Location header, http://www.kb.cert.org/vuls/id/313280

NGSSoftware Insight Security Research Paper, Hackproofing Oracle Application Server, http://www.nextgenss.com/papers/hpoas.pdf

Oracle Security Alert #28, Vulnerabilities in Oracle mod_plsql and JSP in Oracle9i Application Server, v1.0.2.x, http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

H **OracleAppserverSoapComponents: Oracle9i Application Server SOAP components are enabled and could allow remote unauthorized access**

Additional Information *More Information*

port=80

Oracle9i Application Server version 1.0.2.2.1 enables Simple Object Access Protocol (SOAP) components by default. This vulnerability could allow a remote attacker to access SOAP components on the server and modify or gain access to restricted information without authentication.

Remedy:

No remedy available as of March 2002.

Refer to Oracle Security Alert #22 for workaround information. See References.

References:

CERT Vulnerability Note VU#736923, Oracle 9iAS SOAP components allow anonymous users to deploy applications by default, http://www.kb.cert.org/vuls/id/736923

NGSSoftware Insight Security Research Paper, Hackproofing Oracle Application Server, http://www.nextgenss.com/papers/hpoas.pdf

Oracle Security Alert #22, Security Implications of the Oracle9iAS Default SOAP Configuration, http://otn.oracle.com/deploy/security/pdf/ias_soap_alert.pdf

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

H OracleMultipleFunctionBo: Oracle Database Server multiple functions buffer overflow

Additional Information *More Information*

Oracle9i Database Servers prior to Oracle 9i Database Release 2 version 9.2.0.3 are vulnerable to buffer overflows in the NUMTOYMINTERVAL, NUMTODSINTERVAL, FROM_TZ functions and in the TIME_ZONE environment variable, caused by improper bounds checking. A remote authenticated attacker could supply a long parameter to overflow a buffer and cause the server to crash or to execute arbitrary code on the system.

Remedy:
Apply the appropriate patch to your system, available from the Oracle MetaLink Web site. See References.

References:
Oracle MetaLink Web site, Oracle Corporation - OracleMetaLink, http://metalink.oracle.com

VulnWatch Mailing List, Thu Feb 05 2004 - 14:15:57 CST , Oracle Database 9ir2 Interval Conversion Functions Buffer Overflow, http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0030.html

NGSSoftware Insight Security Research Advisory #NISR12122003d, Oracle NUMTOYMINTERVAL Remote System Overflow, http://www.nextgenss.com/advisories/ora_numtoyminterval.txt

NGSSoftware Insight Security Research Advisory #NISR12122003d, Oracle NUMTOYMINTERVAL Remote System Overflow, http://www.nextgenss.com/advisories/ora_numtoyminterval.txt

NGSSoftware Insight Security Research Advisory #NISR12122003e, Oracle TIME_ZONE Remote System Buffer Overrun, http://www.nextgenss.com/advisories/ora_time_zone.txt

CERT Vulnerability Note VU#819126, Oracle9i Database contains buffer overflow in NUMTOYMINTERVAL() function, http://www.kb.cert.org/vuls/id/819126

CERT Vulnerability Note VU#846582, Oracle9i Database contains buffer overflow in NUMTODSINTERVAL() function, http://www.kb.cert.org/vuls/id/846582

CERT Vulnerability Note VU#240174, Oracle9i Database contains buffer overflow in TIME_ZONE session parameter, http://www.kb.cert.org/vuls/id/240174

CERT Vulnerability Note VU#399806, Oracle9i Database contains buffer overflow in FROM_TZ() function, http://www.kb.cert.org/vuls/id/399806

CIAC Information Bulletin O-093, Oracle9i Database Buffer Overflow Vulnerabilities, http://www.ciac.org/ciac/bulletins/o-093.shtml

H OracleTnsListenerEmptyPassword: Oracle TNS Listener has an empty password

Additional Information *More Information*

port=1521
Transparent Network Substrate (TNS) Listener handles all remote client connection requests for Oracle services. By default, the TNS Listener has an empty password. This could allow an unauthorized remote user to gain access and shut down the TNS Listener, which would result in a denial of service.

Remedy:
Refer to the Oracle Database Listener Security Guide PDF for information on properly securing the Oracle TNS Listener. See References.

References:
Oracle Database Listener Security Guide PDF, Oracle Database Listener Security Guide, http://www.integrigy.com/info/Integrigy_OracleDB_Listener_Security.pdf

SAINT Corporation Web site, Vulnerability Tutorial • Oracle TNS Listener, http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Oracle_TNS_Listener.html&fact_color=doc&tag=

SecurityFocus PenTest Mailing List, Fri, 11 Jan 2002 15:33:35 -0500, RE: Oracle TNS Listener, http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-01/0038.html

OracleAppserverApacheServices: Oracle9i Application Server default installation could allow an attacker to access certain Apache Services (CAN-2002-0563)
Vuln count = 2

Additional Information *More Information*

port=443

port=80

Oracle9i Application Server version 1.0.2.x includes several Apache HTTP Server services by default that can be accessed without requiring authorization. A remote attacker could access one of these services, such as Dynamic Monitoring Services, to gain sensitive information about the server.

Remedy:
Refer to Section 4 of Oracle Security Alert #28 for instructions on editing httpd.conf to prevent access to vulnerable services. See References.

References:

CERT Vulnerability Note VU#168795, Oracle 9iAS allows anonymous remote users to view sensitive Apache services by default, http://www.kb.cert.org/vuls/id/168795

NGSSoftware Insight Security Research Paper, Hackproofing Oracle Application Server, http://www.nextgenss.com/papers/hpoas.pdf

Oracle Security Alert #28, Vulnerabilities in Oracle mod_plsql and JSP in Oracle9i Application Server, v1.0.2.x, http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

OracleAppserverConfigFileAccess: Oracle9i Application Server XSQLConfig.xml and soapConfig.xml configuration file access

Additional Information *More Information*

port=80

Oracle9i Application Server version 1.0.2.x could allow a remote attacker to gain unauthorized access to configuration files. By default, no authentication is required in order to access the XSQLConfig.xml and soapConfig.xml configuration files. An attacker could use this vulnerability to gain access to sensitive information about the server.

Note: If these files have permissions set, an attacker may still gain unauthorized access by using the XSQL Servlet to access the file.

Remedy:
No remedy available as of March 2002.

Users should refer to Section 3 of Oracle Security Alert #28 for workaround information. See References.

References:

CERT Vulnerability Note VU#476619, Oracle 9iAS default configuration allows arbitrary users to view sensitive configuration files, http://www.kb.cert.org/vuls/id/476619

NGSSoftware Insight Security Research Paper, Hackproofing Oracle Application Server, http://www.nextgenss.com/papers/hpoas.pdf

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

Oracle Security Alert #28, Vulnerabilities in Oracle mod_plsql and JSP in Oracle9i Application Server, v1.0.2.x, http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf

CERT Vulnerability Note VU#977251, Oracle 9iAS XSQL Servlet ignores file permissions allowing arbitrary users to view sensitive configuration files, http://www.kb.cert.org/vuls/id/977251

M **OracleAppserverOraclejspViewInfo: Oracle9i Application Server OracleJSP could allow a remote attacker to view sensitive information**
Vuln count = 2

Additional Information	*More Information*
port=443	
port=80	

Oracle9i Application Server could allow a remote attacker to view sensitive information about the server, caused by a vulnerability in the OracleJSP environment. When a user requests a Java Server Page (JSP) from the server, three files are created in the /_pages directory based on the filename of the requested file. The three files are created with the extensions $__jsp_StaticText.class, .class, and .java. The .java file contains certain sensitive information stored in plaintext, including the database User ID and password. A remote attacker who can guess the path to the .java file could view this information and use it to gain unauthorized access to the database. In cases where a globals.jsa file is being used for program settings, an attacker could also access this file to obtain sensitive information.

Remedy:

No remedy available as of February 2002.

As a workaround, refer to NGSSoftware Insight Security Research Advisory #NISR06022002C for instructions on protecting the affected files. See References.

References:

NGSSoftware Insight Security Research Advisory #NISR06022002C, OracleJSP, http://www.nextgenss.com/advisories/orajsp.txt

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

CERT Vulnerability Note VU#698467, Oracle 9iAS default configuration allows access to "globals.jsa" file, http://www.kb.cert.org/vuls/id/698467

CERT Vulnerability Note VU#547459, Oracle 9iAS creates temporary files when processing JSP requests that are world-readable, http://www.kb.cert.org/vuls/id/547459

CIAC Information Bulletin M-048, Oracle 9iAS Default Configuration Vulnerability, http://www.ciac.org/ciac/bulletins/m-048.shtml

M **OracleAppserverPlsqlWebInterface: Oracle9i Application Server PL/SQL gateway administration Web interface has no authentication (CAN-2002-0561)**

Additional Information	*More Information*
port=80	

Oracle9i Application Server could allow a remote attacker to access the PL/SQL gateway administration Web interface, caused by the failure to perform authentication under default configuration. A remote attacker could use this vulnerability to access the PL/SQL module and modify Database Access Descriptors (DAD) and cache settings, which would allow the attacker to access PL/SQL programs to cause a denial of service against certain programs.

Remedy:

Refer to CERT Vulnerability Note VU#611776 and Oracle Security Alert #28 for instructions on restricting access to the PL/SQL gateway administration Web pages. See References.

References:

CERT Vulnerability Note VU#611776, Oracle9i Application Server PL/SQL Gateway web administration interface uses null authentication by default, http://www.kb.cert.org/vuls/id/611776

NGSSoftware Insight Security Research Paper, Hackproofing Oracle Application Server, http://www.nextgenss.com/papers/hpoas.pdf

Oracle Security Alert #28, Vulnerabilities in Oracle mod_plsql and JSP in Oracle9i Application Server, v1.0.2.x, http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf

CERT Advisory CA-2002-08, Multiple vulnerabilities in Oracle Servers, http://www.cert.org/advisories/CA-2002-08.html

Nessus:

Vulnerability found on port https (443/tcp) & port http (80/tcp)

In a default installation of Oracle 9iAS, it is possible to access the Dynamic Monitoring Services pages anonymously. Access to these pages should be restricted.

Solution:
Edit httpd.conf to restrict access to /dms0.
Risk factor : High
CVE : CAN-2002-0563
BID : 4293
Nessus ID : 10848

Vulnerability found on port https (443/tcp) & port http (80/tcp)

In a default installation of Oracle 9iAS v.1.0.2.2, it is possible to deploy or undeploy SOAP services without the need of any kind of credentials. This is due to SOAP being enabled by default after installation in order to provide a convenient way to use SOAP samples. However, this feature poses a threat to HTTP servers with public access since remote attackers can create soap services and then invoke them remotely. Since SOAP services can contain arbitrary Java code in Oracle 9iAS this means that an attacker can execute arbitray code in the remote server.

Solution:
Disable SOAP or the deploy/undeploy feature by editing $ORACLE_HOME/Apache/Jserver/etc/jserv.conf and removing/commenting the following four lines:
ApJServGroup group2 1 1
$ORACLE_HOME/Apache/Jserv/etc/jservSoap.properties
ApJServMount /soap/servlet ajpv12://localhost:8200/soap
ApJServMount /dms2 ajpv12://localhost:8200/soap
ApJServGroupMount /soap/servlet balance://group2/soap

Note that the port number might be different from 8200.
Also, you will need to change in the file $ORACLE_HOME/soap/werbapps/soap/WEB-INF/config/soapConfig.xml:
<osc:option name='autoDeploy' value='true' />
to
<osc:option name='autoDeploy' value='false' />

More information:
http://otn.oracle.com/deploy/security/pdf/ias_soap_alert.pdf

http://www.cert.org/advisories/CA-2002-08.html
http://www.kb.cert.org/vuls/id/476619

Also read:
Hackproofing Oracle Application Server from NGSSoftware:
available at http://www.nextgenss.com/papers/hpoas.pdf

Risk factor : High
CVE : CVE-2001-1371
BID : 4289
Nessus ID : 11227

Vulnerability found on port https (443/tcp) & port http (80/tcp)

In a default installation of Oracle 9iAS, it is possible to access the
Java Process Manager anonymously. Access to this page should be restricted.

Solution:
Restrict access to /oprocmgr-status in httpd.conf

Risk factor : High
CVE : CAN-2002-0563
BID : 4293
Nessus ID : 10851

Vulnerability found on port oracle (1521/tcp)

The remote Oracle Database, according to its version number,
is vulnerable to a buffer overflow in the query CREATE DATABASE LINK.

An attacker with a database account may use this flaw to gain the control
on the whole database, or even to obtain a shell on this host.

Solution : See http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf
Risk factor : High
CVE : CAN-2003-0222
BID : 7453
Nessus ID : 11563

Vulnerability found on port oracle (1521/tcp)

According to its version number, the installation of Oracle on the remote
host is reportedly subject to multiple directory traversal
vulnerabilities that may allow a remote attacker to read, write, or
rename arbitrary files with the privileges of the Oracle Database
server. An authenticated user can craft SQL queries such that they

would be able to retrieve any file on the system and potentially retrieve and/or modify confidential data on the target's Oracle server.

See also : http://www.argeniss.com/research/ARGENISS-ADV-030501.txt
Solution : http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf
Risk Factor : Medium
BID : 12749
Nessus ID : 17654

Vulnerability found on port oracle (1521/tcp)

The remote Oracle tnslsnr has no password assigned.
An attacker may use this fact to shut it down arbitrarily,
thus preventing legitimate users from using it properly.

Solution: use the lsnrctrl SET PASSWORD command to assign a password to, the tnslsnr.
Risk factor : High
Nessus ID : 10660

Vulnerability found on port oracle (1521/tcp)

According to its version number, the installation of Oracle on the remote host is reportedly subject to multiple unspecified vulnerabilities.
Some vulnerabilities don't require authentication. It may allow an attacker to craft SQL queries such that they would be able to retrieve any file on the system and potentially retrieve and/or modify confidential data on the target's Oracle server.

Solution : http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
Risk Factor : High
BID : 13145, 13144, 13139, 13238, 13236, 13235, 13234, 13239
Nessus ID : 18034

Vulnerability found on port oracle (1521/tcp)

The remote Oracle Database, according to its version number,
is vulnerable to a remote command execution vulnerability which may allow an attacker who can execute SQL statements with certain privileges to execute arbitrary commands on the remote host.

Solution : http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf
Risk Factor : High
CVE : CAN-2004-0637, CAN-2004-0638

BID : 10871, 11091, 11100, 11099, 11120
Other references : IAVA:2004-A-0014
Nessus ID : 14641

Vulnerability found on port oracle (1521/tcp)

The remote Oracle Database, according to its version number, is vulnerable to a buffer overflow in the query SET TIME_ZONE.

An attacker with a database account may use this flaw to gain the control on the whole database, or even to obtain a shell on this host.

Solution : Upgrade to Oracle 9.2.0.3 - http://metalink.oracle.com
See Also : http://www.nextgenss.com/advisories/ora_time_zone.txt
Risk factor : High
BID : 9587
Nessus ID : 12047

Vulnerability found on port oracle (1521/tcp)

The remote Oracle Database, according to its version number, is vulnerable to a denial of service related to SOAP and XML.

An attacker may use these flaws to disable the remote database remotely.

Solution : Upgrade to Oracle 9.0.2.3 - http://metalink.oracle.com
See Also : http://otn.oracle.com/deploy/security/pdf/2004alert65.pdf
Risk factor : High
BID : 9703, 9705
Nessus ID : 12067

3.5.2 PERPOS development system Microsoft Windows vulnerabilities

Both ISS Scanner and Nessus detected two Microsoft vulnerabilities. ISS Scanner supplied more detail about the LSASS buffer overflow whereas Nessus was inexplicably vague. ISS Scanner also provides more third-party references to the potential vulnerability.

ISS Scanner:

H **WinAsn1BoNtlmDetected: Microsoft Windows ASN.1 buffer overflow packet using NTLM has been detected**

Additional Information *More Information*

A specially-crafted ASN.1 packet containing an invalid length that has been sent to an smb port has been detected. Microsoft Windows NT, Windows 2000, Windows XP, and Windows Server 2003 are vulnerable to a buffer overflow in Microsoft's implementation of the Abstract Syntax Notation 1 (ASN.1) Library. ASN.1 is the language used to standardize data across multiple platforms. A remote attacker could exploit this vulnerability to overflow a buffer and execute arbitrary code on the system with system privileges.

Remedy:
Apply the appropriate patch for your system, as listed in the Microsoft Security Bulletin MS04-007. See References.

References:

Microsoft Security Bulletin MS04-007, ASN.1 Vulnerability that Could Allow Code Execution (828028), http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx

Internet Security Systems X-Force Database, Microsoft Windows ASN.1 Library buffer overflow, http://xforce.iss.net/xforce/xfdb/15039

H **WinLsassBo: Microsoft Windows LSASS buffer overflow**

Additional Information *More Information*

Microsoft Windows 2000, XP, Windows Server 2003 and Windows XP 64-Bit Edition 2003 are vulnerable to a buffer overflow in the Local Security Authority Subsystem Service (LSASS), caused by improper bounds checking. LSASS is a management interface for local security, domain authentication, and Active Directory processes. By sending a specially-crafted message to the affected system, a remote attacker could overflow a buffer and execute arbitrary code on the system.

The Sasser worm exploits this security issue. Sasser propagates by scanning randomly selected IP addresses for vulnerable systems.

Note: Only a local administrator could exploit this vulnerability on Microsoft Windows Server 2003 and Windows XP 64-Bit Edition 2003.

Remedy:

For vulnerability detection:

Enable the following checks in the ISS Protection Platform:

WinMs04011Patch (http://xforce.iss.net/xforce/xfdb/15818)

For Virtual Patch (see http://xforce.iss.net/xforce/riskindex/#vp):

Enable the following checks in the ISS Protection Platform:

MSRPC_LSASS_Bo

MSRPC_LSASS_Request_Detected (http://xforce.iss.net/xforce/xfdb/15830)

Sasser_Propogation(http://xforce.iss.net/xforce/xfdb/16045)

For Manual Protection:

Apply the appropriate patch for your system, as listed in the Microsoft Security Bulletin MS04-011. See References.

References:

Microsoft Security Bulletin MS04-011, Security Update for Microsoft Windows (835732), http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

CIAC Information Bulletin O-114, Microsoft Security Update for Microsoft Windows, http://www.ciac.org/ciac/bulletins/o-114.shtml

CERT Vulnerability Note VU#753212, Microsoft LSA Service contains buffer overflow in DsRolepInitializeLog() function, http://www.kb.cert.org/vuls/id/753212

Internet Security Systems Security Alert, April 13, 2004, Multiple Vulnerabilities in Microsoft Products, http://xforce.iss.net/xforce/alerts/id/169

Packet Storm Web site, billybastard.c,

http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=billybastard&type=archives&%5Bsearch%5D.x=14&%5Bsearch%5D.y=8

Packet Storm Web site, sasserftpd.c, http://packetstormsecurity.nl/0405-exploits/sasserftpd.c

Packet Storm Web site, win_msrpc_lsass_ms04-11_Ex.c, http://packetstormsecurity.nl/0405-exploits/win_msrpc_lsass_ms04-11_Ex.c

CIAC Information Bulletin O-114, Microsoft Security Update for Microsoft Windows [REVISED 25 Jun 2004], http://www.ciac.org/ciac/bulletins/o-114.shtml

Nessus:

Vulnerability found on port microsoft-ds (445/tcp)

The remote Windows host has a ASN.1 library which is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths.

This particular check sent a malformed NTLM packet and determined that the remote host is not patched.

Solution : http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx
Risk factor : High
CVE : CAN-2003-0818
BID : 9633, 9635, 9743, 13300
Other references : IAVA:2004-A-0001
Nessus ID : 12054

Vulnerability found on port microsoft-ds (445/tcp)

The remote host seems to be running a version of Microsoft OS which is vulnerable to several flaws, ranging from denial of service to remote code execution. Microsoft has released a Hotfix (KB835732) which addresses these issues.

Solution : Install the Windows cumulative update from Microsoft

See also : http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

Risk factor : High

Other references : IAVA:2004-A-0006
Nessus ID : 12209

3.5.3 Identifying unnecessary network servers

On an "inside the firewall" scan of the PERPOS web server, both ISS Scanner and Nessus identified two unnecessary network servers: identd and fam. The ISS Scanner remedy and references are not shown because it was inadvertently not included when saving the report. Nessus noted that the fam service has been subject to vulnerabilities in the past whereas ISS Scanner noted that the fam service can be used by an attacker to obtain a list of files on the system. In other words, each scanner reported a slightly different reason for disabling this service.

ISS Scanner:

IdentdUsers: Ident daemon can be used to remotely gather servers' running usernames (CAN-1999-0629)

The ident daemon is intended to advertise the username of a system's clients to remote servers. Many identds advertise the usernames of local servers to remote clients. This allows attackers to better understand your system configuration.

irixfam: FAM server lists files on IRIX systems (CVE-1999-0059)

The IRIX File Alteration Monitor (fam) daemon is used by networked IRIX systems to track file modifications. The fam service, which runs as RPC program 391002, is used by other programs to keep track of file modifications.

When a program initially connects to the fam server, it passes the name of a file or directory to watch. If the fam server receives a directory name, it returns the client a complete list of files and subdirectories in that directory. By passing the fam server a request to list the root directory, and by systematically following the subdirectories, an attacker can remotely obtain a complete list of files on the system.

Nessus:

Warning found on port auth (113/tcp)

The remote host is running an ident (also known as 'auth') daemon.

The 'ident' service provides sensitive information to potential attackers. It mainly says which accounts are running which services. This helps attackers to focus on valuable services (those owned by root). If you do not use this service, disable it.

Solution : Under Unix systems, comment out the 'auth' or 'ident' line in /etc/inetd.conf and restart inetd

Risk factor : Low
CVE : CAN-1999-0629
Nessus ID : 10021

Warning found on port unknown (32769/tcp)

The fam RPC service is running.
Several versions of this service have a well-known buffer overflow condition that allows intruders to execute arbitrary commands as root on this system.

Solution : disable this service in /etc/inetd.conf
See also : http://www.nai.com/nai_labs/asp_set/advisory/16_fam_adv.asp
Risk factor : High
CVE : CVE-1999-0059
BID : 353
Nessus ID : 10216

3.5.4 Suggesting enhanced security configurations for necessary network servers

On an initial "inside the firewall" of the PERPOS web server, both ISS Scanner and Nessus suggested configuration changes for the web server. Nessus offered very specific configuration information for Apache and Sun One Web server to achieve this enhanced security configuration and extensive references. ISS Scanner didn't offer very specific configuration information and didn't even mention Sun ONE Web Server.

ISS Scanner:

HttpTraceEnabled: HTTP TRACE is enabled

Additional Information *More Information*

port=443

HTTP TRACE support is enabled on the Web server. The HTTP TRACE method as described in RFC 2616 of the HTTP 1.1 standard is typically used for debugging and network analysis purposes to request the contents of HTTP request messages received by the Web server. On Web servers with HTTP TRACE support enabled, a remote attacker could leverage this functionality with known cross-site scripting and other Web browser vulnerabilities to obtain sensitive information about the Web server, including server cookies and authentication information. This information could then be used by the attacker to launch further attacks against the affected Web server.

Remedy:
Administrators should disable HTTP TRACE support on the Web server. HTTP TRACE support can be disabled on Apache HTTP Server using the mod_rewrite module and on Microsoft Internet Information Services (IIS) using the URLScan tool.

References:
Internet Security Systems X-Force Database, Multiple vendor Web servers HTTP TRACE method information disclosure, http://xforce.iss.net/xforce/xfdb/11149
Internet RFC/STD/FYI/BCP Archives, Hypertext Transfer Protocol -- HTTP/1.1, http://www.faqs.org/rfcs/rfc2616.html

Nessus:

Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for

"Cross-Site-Tracing", when used in conjunction with
various weaknesses in browsers.

An attacker may use this flaw to trick your
legitimate web users to give him their
credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE
requests or to permit only the methods needed to meet site requirements
and policy.

If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the
following to the default object section in obj.conf:
<Client method="TRACE">
AuthTrans fn="set-variable"
remove-headers="transfer-encoding"
set-headers="content-length: -1"
error="501"
</Client>

If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile
the NSAPI plugin located at:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603
http://www.kb.cert.org/vuls/id/867593

Risk factor : Medium
BID : 9506, 9561, 11604
Nessus ID : 11213

3.6 Vulnerability Assessment Conclusions

- More than one vulnerability assessment scanner should be used in order to compare results to ensure that one of the scanners is not missing vulnerabilities due to configuration errors, lack of updated signatures, or differences in detection methods.
- Vulnerability assessment scanner can return false positives. Administrator knowledge about the scanned systems, comparison of results with another scanner, and consultation with the vulnerability assessment vendors must be performed in order to distinguish false positives from true positives.
- Both ISS Scanner and Nessus were able to detect multiple Oracle and Microsoft Windows vulnerabilities on our un-patched PERPOS development system.
- ISS Scanner generally provides more third-party references for information and details on vulnerabilities. However, Nessus provided more references and more detailed configuration information for disabling the HTTP TRACE method on web servers.
- The results from Nessus and ISS Scanner show that vulnerability assessment scanners are useful in identifying unnecessary network services, suggesting enhanced security configurations for necessary network services, and revealing inadvertent external access to internal resources.

3.7 Vulnerability Assessment Future Tasks

- Perform more thorough "inside the firewall" scanning of PERPOS systems to ensure the systems do not contain vulnerabilities, unnecessary services, and identify enhanced security configurations
- Investigate application-specific vulnerability assessment tools for the type of applications used on PERPOS. For example, vulnerability assessment tools that are more geared towards databases (e.g. ISS Database Scanner) or Oracle database/application server.
- Investigate host-based vulnerability assessment scanners and compare their results/effectiveness to network-based vulnerability assessment scanners.

3 Anti-virus Evaluation

4.1 The need for multiple anti-virus solutions

Like vulnerability assessment scanners, multiple anti-virus scanners should be used to ensure that one scanner isn't missing viruses due to configuration errors or lack of updated virus signatures. Reports in network magazines have shown that anti-virus vendors vary greatly in their response time to viruses that require signatures (i.e., when

their heuristic approaches fail to detect a new virus) and this response time may vary on a virus-by-virus basis[45]. Use of multiple anti-virus scanners minimizes this risk.

4.2 Anti-Virus Selection Process

Three anti-virus products have been selected for the PERPOS Linux servers: 1) McAfee Viruscan, 2) ClamAV, and 3) BitDefender. We've selected the CLI (command-line scanner) versions of these anti-virus products. We selected McAfee Viruscan because Georgia Tech has a site license and because it is a well-known and established commercial anti-virus vendor. ClamAV was selected because it is the leading open source anti-virus project[46]. Other GTRI projects have used ClamAV as an email anti-virus scanner with better detection success than leading commercial anti-virus vendors. Specifically, ClamAV detected more anti-phishing and dangerous content emails than either Sophos or McAfee. However, some industry experts dispute open source's ability to deliver anti-virus products[46]. BitDefender was selected because it is a newer commercial anti-virus vendor and because its Linux version is currently free.

All three of these anti-virus products primarily use signatures and heuristics as opposed to behavior-based detection to identify/block viruses, which has not been heavily adopted by anti-virus vendors and organizations[47]. With the exception of Aladdin eSafe[48], which is not available for Linux, most anti-virus vendors do not clearly disclose if viruses were detected without a signature update.

4.3 Where to implement anti-virus

Layering of anti-virus scanning, i.e., anti-virus scanning implemented in the network on those protocols that allow viruses to be transferred (SMTP, FTP, HTTP, CIFS, etc.), on servers, and on end-user systems, has become commonplace and recommended as long as it does not entail serious additional cost or an excessive focus on one technique vs. another technique (i.e., pattern matching vs. heuristics vs. behavior based detection)[49]. For example, as email became the primary vehicle for the spread of viruses and worms, end-system anti-virus protection was deemed inadequate and anti-virus scanning was added to the email server/gateway. Additionally, many organizations are beginning to scan web-based traffic at the perimeter firewall or proxy server.

Because the vast majority of viruses or worms target Windows systems rather than UNIX servers and because UNIX servers typically don't run services with root/administrator privileges, there hasn't been much market demand for UNIX anti-virus products that inspect files as they are written to disk or accessed from disk, i.e., at the kernel level[50]. Rather, anti-virus products for Linux have been released that target specific UNIX services or servers on a Linux server that Windows systems may access. For example, BitDefender makes a Linux command-line scanner that scans specified files when launched (which could be integrated into applications developed in-house), a version for Linux to be used within Samba (a CIFS server implementation for UNIX), a version for

Linux to be used within sendmail or postfix (SMTP server implementations for UNIX), but not a kernel-level anti-virus program that scans files as they are written to disk or accessed from disk. However, some vendors have recently released kernel-level anti-virus inspection for Linux, for example McAfee LinuxShield.

Currently the PERPOS project only performs end-system anti-virus file system scanning via the McAfee, BitDefender, and ClamAV CLI scanners. These anti-virus CLI scanners are automatically launched every 24 hours, scan the entire file system, and send an email alert if there is a virus found. Cleaning or disinfection must be done manually.

4.4 Anti-Virus Future Tasks

- Investigate available behavioral-based anti-virus detection options.
- Determine if there is a need for network-based anti-virus scanning in the PERPOS system and if so evaluate network-based anti-virus solutions.
- Implement anti-virus scanning of file uploads to the PERPOS systems using the current Linux CLI scanners: McAfee, ClamAV, and BitDefender.
- Implement more advanced anti-virus scanning solutions on PERPOS systems if necessary.

5 Future Areas of Research

In addition to the future tasks itemized at the end of each of the prior sections, there are a number of issues that need to be investigated with regard to Network-based intrusion detection system/intrusion protection systems (IDS/IPS). Is a separate IDS/IPS device needed if some degree of IDS functionality has been integrated into firewalls? What are the differences between an IPS product and an IDS product. Is IDS technology dead as the Gartner Group declared in 2003 [51]? Is host-based intrusion detection necessary with all the other forms of security?

We also need to investigate the use of clientless Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) to provide access to the PERPOS web portal and front-end authentication.

Remote end-point security (REPS) refers to any centralized managed security system that enforces all or part of enterprise security policies on an end-point. End-points can include laptops, desktops, and PDAs. Methods of access include wired local network, dial-up, broadband or wireless. Types of policies enforced include anti-virus definitions, personal firewall, location, authentication, content filtering, application access control and patch levels. Can REPS be enforced for the PERPOS system?

References

[1] Cisco, *Evolution of the Firewall Industry*, September 29, 2002.
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm
[2] MOREnet, *An Introduction to Network Firewalls and the Firewall Selection Process*, March 23, 2004.
http://www.more.net/technical/netserv/tcpip/firewalls/
[3] Steve Steinke, *Firewalls*, Network Magazine, June 14, 2000
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8702843
[4] Cisco, *Access Control Lists and IP fragments*, January 26, 2004.
http://www.cisco.com/warp/public/105/acl_wp.html
[5] NetFilter Project, http://www.netfilter.org/
[6] Steve Leggett, *Firewalls Explained – Part 1*, WebHostGear.com, November 19, 2003
http://www.webhostgear.com/37_print.html
[7] D. Brent Chapman & Elizabeth D. Zwicky, *Building Internet Firewalls*, Chapter 7: Proxy Systems, November 1995.
http://www.unix.org.ua/orelly/networking/firewall/ch07_03.htm
[8] Symantec, *Symantec Security Gateways Reference Guide*, Version 8, 2004, pp. 18-19.
[9] Check Point, *Firewall-1 and SmartDefense: NG with Application Intelligence*, July 2003, pp. 9-42
[10] Check Point, *Firewall-1 and SmartDefense: NG with Application Intelligence*, July 2003, pp. 63-110
[11] Symantec, *Symantec Security Gateways Reference Guide*, Version 8, 2004, pp. 59-60, 66.
[12] Ido Dubrawsky, *Firewall Evolution - Deep Packet Inspection***,** SecurityFocus, July 29, 2003.
http://www.securityfocus.com/infocus/1716
[13] Annaliza Savage, *TCP Bug Threatens Networked Computers*, Wired News, November 21, 1997.
http://wired-vig.wired.com/news/technology/0,1282,8707,00.html
[14] Common Vulnerabilities and Exposures, *CAN-2003-0818: Multiple integer overflows in Microsoft ASN.1 library (MSASN1.DLL), as used in LSASS.EXE, CRYPT32.DLL, and other Microsoft executables and libraries on Windows NT 4.0, 2000, and XP, allow remote attackers to execute arbitrary code via ASN.1 BER encodings with (1) very large length fields that cause arbitrary heap data to be overwritten, or (2) modified bit strings*, September 18, 2003.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818
[15] Thomas Porter, *The Perils of Deep Packet Inspection*, SecurityFocus, January 11, 2005
http://www.securityfocus.com/infocus/1817
[16] Symantec, *Symantec Enterprise Firewall: Installation Guide*, Version 8, March 10, 2004, pp. 27-28.
[17] Secure Computing, *The Origin of Sidewinder G2 Firewall*
http://www.securecomputing.com/index.cfm?skey=1024

[18] Jorg Fritsch, Check Point SecurePlatform with Firewall-1, Linux Magazine, March 2003, pp. 44-47
http://www.linux-magazine.com/issue/28/Check PointSecurePlatform.pdf
[19] Crossbeam Systems, *Crossbeam X80: Security Services Switch datasheet*, October 2003.
[20] Nokia, *Nokia Network Voyager for IPSO 3.8 Reference Guide*, April 2004.
[21] Paul Stamp, *Security Appliances Unwrapped*, CSOonline.com, April 6, 2005.
http://www.csoonline.com/analyst/report3501.html
[22] Craig Matsumoto, *Crossbeam taps net processors for central-office systems*, EE Times, August 28, 2001.
http://www.eetimes.com/story/OEG20010828S0047
[23] Peter Galli, *Fortinet Under Fire for Allegedly Violating GPL Terms*, eWeek.com, April 14, 2005.
[24] Dennis Fisher, *For Sale: Cisco Firewall Source Code*, eWeek.com, November 3, 2004.
http://www.eweek.com/article2/0,1759,1710415,00.asp
[25] Juniper Networks, *Juniper Networks Netscreen-5200/54000 datasheet*, November 2004.
http://www.juniper.net/products/integrated/dsheet/110007.pdf
[26] Monash Technology Report, *The Future of Security Technology, Part 1*, Monash Information Services, November 25, 2002.
[27] Microsoft, *Microsoft Windows 2000 Server Hardening Guide*, April 11, 2003.
http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/default.mspx
[28] Andrew Conry-Murray, *Symantec's Five-in-One Security Gateway*, Nework Magazine, April 5, 2002.
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703310
[29] Symantec, *How to configure Symantec Enterprise Firewall to block Nimda and Code Red worms*, Symantec Enterprise Firewall 8.0 for Windows Knowledge Base Document ID:2002092413323954, October 9, 2003.
[30] Common Vulnerabilities and Exposures, *CVE-1999-0182: Samba has a buffer overflow which allows a remote attacker to obtain root access by specifying a long password*, September 11, 1999.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0182
[31] Symantec, *Symantec Enterprise Firewall: Administrator's* Guide, Version 8.0, March 10, 2004, pp. 159, 197.
[32] Symantec, *Symantec Enterprise Firewall: Administrator's* Guide, Version 8.0, March 10, 2004, pp. 221-231.
[33] SurfControl, *URL Category List*
http://www.surfcontrol.com/Default.aspx?id=355&mnuid=1.4.1.1
[34] Check Point, *SmartDefense Attacks Blocked*, May 29, 2005.
http://www.Check Point.com/defense/advisories/public/blocked.html
[35] Nokia, *Getting Started Guide and Release Notes for Nokia IPSO 3.8.1*, January 2005, pp. 26-28.
[36] Symantec, *Symantec Security Gateways Reference Guide*, Version 8, 2004, pp. 19-20, 46-47.

[37] Robert Shimonski, Thomas Shinder, and et al., *Best Damn Firewall Book Period*, Syngress, 2003, pp. 74-90.
[38] Corrent, *Corrent Appliances Provide Multiple Defenses Against DDoS Attacks*. http://www.corrent.com/technology/technology_ddos.html
[39] Ellen Messmer, *Feeling Vulnerable? Try assessment tools*, Network World, April 24, 2005.
http://www.networkworld.com/news/2004/0405specialfocus.html
[40] Andrew Conry-Murray, *Vulnerability Assessment Tools Find New Uses*, Network Magazine, April 4, 2003.
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=14400061
[41] Andrew Conry-Murray, *Sourcefire's Real-Time Network Awareness*, Network Magazine, April 1, 2004.
http://www.networkmagazine.com/showArticle.jhtml?articleID=159900441
[42] Marcus Ranum, *Vulnerability Scanning*, LOOP, January 31, 2005.
http://loop.interop.com/comments.php?id=254_0_1_0_C
[43] Jeff Forristal and Greg Shipley, *Vulnerability Assessment Scanners*, Network Computing, January 8, 2001
http://www.networkcomputing.com/1201/1201f1b1.html
[44] Internet Security Systems, *Internet Scanner User Guide Version 7.0, Service Pack 2*, 2005.
[45] Brian Livingston, *How Long Must You Wait for an Anti-Virus Fix?*, EarthWeb, February 23, 2004.
http://itmanagement.earthweb.com/columns/executive_tech/article.php/3316511
[46] Larry Seltzer, *Open Source Not Ready for Anti-Virus*, eWeek.com, August 9, 2004.
http://www.eweek.com/article2/0,1759,1633423,00.asp
[47] Ellen Messmer, *Behavior blocking repels new viruses*, Network World, January 1, 2002.
http://www.networkworld.com/news/2002/0128antivirus.html
[48] http://www.aladdin.com/esafe/default.asp
[49] Jan Sudgren, *Deploying Multiple Antivirus Scanners Is Not a High Priority*, Forrester Research, February 3, 2003.
[50] Iain Thomson, *Antivirus vendors await major Linux worm*, vunet.com, June 10, 2004.
http://www.vnunet.com/2125189
[51] Richard Stiennon. "IDS is Dead. Long Live IPS". Gartner Group, 2003.

Glossary

Many of these definitions are taken from http://isp.webopedia.com/

ARP - Acronym for Address Resolution Protocol, a network layer protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. ARP is described in RFC 826.

ASIC - Application-Specific Integrated Circuit

CERT/CC - Acronym for Computer Emergency Response Team Coordination Center. CERT/CC studies Internet security vulnerabilities, provides services to Web sites that have been attacked and publishes security alerts.

CIFS - Common Internet File System

CVE - Acronym for **C**ommon **V**ulnerabilities and **E**xposures. CVE is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures.

Domain name - a name that identifies one or more IP addresses. For example, the domain name *microsoft.com* represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages.

DoS attack - abbreviation for *denial-of-service attack*, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks.

DDoS - distributed denial of service

DMZ - Abbreviation for *demilitarized zone*, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

DNS - Short for Domain Name Server, an Internet service that translates domain names into IP addresses.

DPI - Deep Packet Inspection

EAL - Abbreviation for Evaluation Assurance level, and International Common Criteria IT product security testing evaluation level. EAL1 is the lowest level of testing; EAL7 is the highest. An EAL can be considered a level of confidence in the security functions of an information-technology product or system.

FSOS - a firewall/security operating system offered on hardware appliances and may use network processors or ASICs to improve performance.

FTP - Short for File Transfer Protocol, the protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

GPOS - general purpose operating system

HOS - hardened operating system

HTTP - Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

ICMP - Internet Control Message Protocol, an extension to the Internet Protocol (IP). ICMP supports packets containing error, control, and informational messages

IDS - Abbreviation for intrusion prevention system, a system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

IP address - An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.150.1.240 could be an IP address.

IPS - Abbreviation for intrusion prevention system. Some compare an IPS to a combination of IDS and an application layer firewall for protection.

LDAP - Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP supports TCP/IP, which is necessary for any type of Internet access. LDAP should eventually make it possible for almost any application

running on virtually any computer platform to obtain directory information, such as email addresses and public keys.

MAC address - media access control address

NIAP - Acronym for the National Information Assurance Partnership, a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

phishing - a scam where the perpetrator sends out legitimate-looking e-mails appearing to come from some of the Web's biggest sites in an effort to phish (pronounced "fish") for personal and financial information from the recipient.

RBL - Abbreviation for Realtime Blackhole Lists, i.e, public lists of known spammers.

REPS - Acronym for remote end-point security, which is used broadly to refer to any centralized managed security system that enforces all or part of enterprise security policies on an end-point. End-points can include laptops, desktop and PDAs. Methods of access include wired local network, dial-up, broadband or wireless. Types of policies enforced include anti-virus definitions, personal firewall, location, authentication, content filtering, application access control and patch levels.

SMTP - Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

SOAP - Short for Simple Object Access Protocol, a lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. SOAP messages may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.

Spoof - In networking, the term is used to describe a variety of ways in which hardware and software can be fooled. *IP spoofing*, for example, involves trickery that makes a message appear as if it came from an authorized IP address.

SSH - Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing.

SSL - Abbreviation for Secure Sockets Layer, a protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer

support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http*:.

TCP/IP - Abbreviation for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system, making it the de facto standard for transmitting data over networks.

TTL - Abbreviation for *Time to Live*, a field in the Internet Protocol (IP) that specifies how many more hops a packet can travel before being discarded or returned.

URL - Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

VPN - Abbreviation for virtual private network, a system , a *network* that is constructed by using public communication channels such as the Internet, with encryption and other security mechanisms to ensure that only authorized users can access the network.

worm - a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.