Global Information Assurance Certification Paper

Network Security Assessment

Ovi Caravan
GSEC Practical ver 1.4b option 2
July 2004

Table of Contents

ABSTRACT

During the third quarter of 2003, the company I am working for (MyComp) acquired another company (NewComp) which is competing in the same field. After long deliberations the higher management decided to let the new acquired company to work independently for the next year – the reasons were more regarding the clients database, plus some software deployments they did during the last years. Short, all of their applications (ERP, CRM, FIS, etcetera) were totally different than what we use, so we thought a slow migration will bring less pain.
However, for same of the departments it was much easier to migrate (HR, Legal, …). In order to facilitate the collaboration between this department, plus to prepare for the migration of main applications, we needed to bring them on our network.

In the last 3, 4 years, when the number of viruses, and hackers attacks increased dramatically, we managed to stay safe.
How we did? We had respected the basic rules: password policy, patched systems, update antivirus at the servers, desktop, and email server level, firewalls, secure VPN's, email policy, educate local and remote.

After we got the higher management approval, we decided to go and inspect the security on the NewComp network and at the final to run a Network Security Assessment on their computer (hardware infrastructure) – the assessment was run mostly against their hosts or ports which were exposed to the Internet.

Information is a critical business asset and must be safeguarded against attack. A properly implemented information security strategy provides protection against threats to this information, helps to ensure business continuity in the event of a disaster, maximizes return on investment, and mitigates liability and risk.

We used several vulnerability assessment tools to evaluate the exposure of each host to external threats – each separate vulnerability assessment tool has particular strengths and weaknesses. We thought that only by combining several tools can the most accurate and comprehensive list of vulnerabilities be determined.

Care is taken during the preparation of a network security assessment report to avoid obvious false positive alarms caused by automated network scanning tools. Manual validation of all vulnerabilities is performed to provide a detailed analysis of security issues inherent in an organization's network and their implications should these vulnerabilities be exploited.

Threats to information security today come in many forms. It is no longer true that the vast majority of the incidences, or the largest monetary losses, are coming

from the anonymous “war-gaming” hacker on the Internet. According to a recent FBI survey approximately half of all incidences involving computer crime and information compromises relate to employee abuses of internal corporate systems. It is not adequate security policy to stringently protect the corporate network from external attacks and deemphasize the threat from possibly unwitting users operating on corporate intranet.

A formal security assessment is a vital process in any connected infrastructure. The checklist outlines the important areas that should be included in every Network Security Assessment. Following I’ll list the checklist we used to do the security assessment on the exposed node to Internet:

- Assess the External Network / Perimeter Network
- Assess Name Servers
- Assess Firewalls
- Assess VPNs
- Assess Internet Web Servers
- Assess Messaging Servers / Messaging Gateways – External / Intranet
- Assess Routers
- Assess Intranet Servers

Composing this checklist, guidance was used from Microsoft Security Risk Assessment:
http://members.microsoft.com/certpartner/projectguides/system_security/

also some other guidance, and inspiration was used from the following sites

NIST Computer Security Resource Center
http://csrc.nist.gov/

The National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/

Much of this report contains suggestions for improving a functional IT environment that do not require a large capital expenses. These initiatives include implementing consistent procedures involving all information security assets, improving and enforcing reasonable policies throughout the network environment, and generally striving towards best-practice network maintenance and monitoring.
In the report the IP addresses, company name, etc, were sanitized.

At the technical level, we stress the defense-n-depth paradigm and begin with suggestions involving strengthening the security of the network perimeter. Some extraneous services were found to represent vulnerabilities on machines that are available to the Internet. Also, many mission critical Internet services were found to have configuration errors that would allow information leaks. This creates a

large opportunity for random hackers, script kiddies, and also for the malicious attacker interested in accessing (stealing) corporate information.

Internally they are a number of improvements that can be made that will severe reduce the risk and exposure and minimally effect user convenience and satisfaction. These improvements include: the complete segregation of critical network segments; maintaining all software at current patch levels; the consistent enforcement of strong security log policies on all critical servers, with the possible addition of a centralized log server; the enforcement of appropriate user password history, complexity and lifetime; and finally, the consistent application of anti-virus software at the gateway, server, and host levels.

Results at a Glance

The following information was gathered during Network Security Assessment of NewComp. Manual validation was performed to determine the impact of vulnerabilities, eliminate false positives and to assign appropriate security levels. Below is a summary of the results gathered during the Network Security Assessment:

SUMMARY OF FINDINGS	
Category	**Description**
Date	March 2004 – April 2004
Address Ranges	10.121.116.32/27
	10.121.116.128/27
	10.116.78.76/30
	10.113.236.100/32
Number of Reportable Systems	12
Total Vulnerabilities	96
Total Warnings	66
Total Holes	30

SYSTEMS ANALYZED		
System IP Address	Name	OS
10.113.236.100	Adsl-10.113.236.100.newcomp.com	NEtscreen 5 running ScreenOS 4..r1
10.116.78.76	10.116.78.76	Netscreen 10 running ScreenOC 4.0.r2
10.116.78.77	10.116.78.77	unknown
10.121.116.33	10.121.116.33	Cisco 7500 running IOS12.2
10.121.116.34	10.121.116.34	Netscreen 25 running ScreenOS 4.0.r2
10.121.116.40	Mail.newcomp.com	Microsoft
10.121.116.49	Ssh.newcomp.com	Linux
10.121.116.145	10.121.116.145	Netscreen 25 running ScreenOS 4.0.r2
10.121.116.150	Newcomp.info	Microsoft
172.16.188.1	172.16.188.1	Netscreen 25 running ScreenOS 4.0.r2
172.16.188.49	Uroam.newcomp.com	Linux
172.16.188.254	172.16.188.254	Netscreen 10 running ScreenOS 4.0.r2

SUMMARY OF VULNERABILITIES BY SYSTEM			
System IP Address	Holes	Warnings	Open Ports
10.113.236.100	1		1
10.116.78.76	1		1
10.116.78.77			
10.121.116.33		3	5
10.121.116.34		1	1
10.121.116.40		2	3
10.121.116.49	7	8	4
10.121.116.145		1	1
10.121.116.150	7	28	24 (3 from the Internet)
172.16.188.1		1	1
172.16.188.49	13	22	8
172.16.188.254	1		1

Recommendations

The Action Items, section below describes steps to efficiently and effectively mitigate security risks associated with Company's information assets.

Action Items

1. Disallow administrative access to routers and firewalls from the Internet

   Access to routers and firewalls could allow a hacker to completely change the logical network configuration and allow access to virtually any service. A hacker could also perform a Denial of Service attack by deleting the configuration. If access can not be restricted, a strong password policy can be enforced.

2. Ensure that the corporate firewall settings do not unnecessarily risk access to the corporate LAN by "dual-homing" DMZ servers.

   A dual homed host is one that has an interface in two separate security zones – such as DMZ and LAN. A host configured in this manner destroys the integrity of the DMZ and may allow a hacker who successfully compromise a DMZ server access to the entire corporate LAN.

3. Implement egress filters on the firewall to restrict unwanted traffic.

NewComp should implement egress filters to restrict unwanted traffic such as KaZaA, and Morpheus or, if relevant, outbound FTP and/or SFTP. Allowing these services creates security holes by allowing unrestricted file transfers and may introduce viruses. Furthermore, these are significant liability concerns with copyrighted material. One host on NewComp network was found running KaZaA.

4. Update the version of Uroam

NewComp should upgrade its version of Uroam (now F5 Networks) from version 2.4 to 3.x when F5 Networks releases their first release this month. Although no specific vulnerabilities relating to the Uroam server were found, the server appear to have vulnerabilities associated with older versions of the Appache web server, OpenSSL and SSH.

5. Update the applications for critical services (mail and web).

Exchange should be upgraded from 5.0 to 2003; IIS from 5.1 to 6.1. Support fro Exchnage 5.0 has been ended in December 2003. These upgrades will require an upgrade to Windows 2003.

6. Update the operating system on the CISCO routers

The version of IOS should be upgraded from 12.1(1) to 12.2 (1). Also NewComp should consider replacing the router as it has reached end-of-life status at CISCO. Hardware support ended in May 2003 and software support will end in May 2004. The recommended substitute product is CISCO 2610.

7. Lockdown servers on the corporate LAN.

While testing the LAN was outside the scope of this assessment, tests of the LAN IP addresses of several of the DMZ servers showed significantly more vulnerabilities than the DMZ (Internet routable) address. For example server1.newcomp.info has three ports available from the internet and from the LAN to the DMZ address. Unused services should be disabled on critical hosts. NewComp should strongly consider an assessment of all of its corporate servers – to include DNS, Domain Controllers, Database Servers, Financial Servers, HR Servers, etcetera.

8. Run the IIS Lockdown tool on web-enabled Windows Servers

NewComp should run thee IIS Lockdown tool, which is available from Microsoft. All of the web-enabled servers showed evidence of standard configuration errors like .IDA extensions, Front Page extensions, WebDAV, and the Internet Printing Protocol. A related issue is that the host at server2.newcomp.info accepts the login credentials of “guest” / “guest”. The DHCP server (10.16.0.10) accepted as valid the username “mc2” with no password.

9. Ensure that the policy for patch application is relevant and enforced.

NewComp should ensure that critical security patches are tested and rolled out as soon as possible, and generally within one month of their release unless hacker activity dictates a quicker response.

10. Ensure that the password policy is relevant and enforced.

NewComp should develop and enforce a strong password policy. Passwords are the first line of defense against hackers. Evidence of a weak password policy was found with “default” logins of “guest/guest” on Internet-accessible web servers and username “lc2” and no password on the DHCP server (letter it proves that it was a video camera, which was feeding with images a web page).

Furthermore, there is evidence that the domain policy is not particularly strong as accounts were found that their password, had never logged in, and passwords that never expire. A full review of the policy and the settings on the Domain Controller were outside the scope of this assessment.

Technical Summary

The network perimeter at NewComp is reasonably secure, with a minimum of services available from the Internet. The corporate network is protected by a Netscreen 25 firewall that has a current version of ScreenOS installed. We recommend that administrative access to routers and firewalls be disabled from the Internet. Currently, all of the firewalls have SSL-enabled connections to administrative functions available from anywhere on the Internet. The Netscreen 10s have reached end-of-life and are not longer supported by Netscreen. As one of the Netscreen 10s is a home firewall and the other is the firewall for the backup DSL, this is satisfactory. The other home firewalls are Netscreen 5s and an upgrade to ScreenOS 5.0.0r1 should be considered. We strongly recommend that NewComp implement egress filtering on its corporate LAN. The recent upsurge in KaZaA and other P2P file sharing inhibits valid uses of the Internet. Furthermore, these are serious questions of corporate liability. A brief scan of NewComp's internal LAN (10.16.0.0/24) showed at least one host that had the KaZaA service running.

The CISCO 2520 router has telnet access enabled – on five different ports. Furthermore, it has reached end-of-life status. CISCO no longer offers hardware support on this device and software support will not longer be available after June 30, 2004. The recommended substitute product is the 2610. Furthermore, the version of IOS that is installed on the device is out of date.

The Windows servers that are accessible from the Internet are fairly well protected. NewComp should continue to ensure that these systems are patched in a timely manner. We recommend that NewComp should upgrade the email servers to Exchange 2003, and upgrading the Domain Controllers, and the other servers to Windows 2003 would also allow NewComp to upgrade the Web servers from IIS 5.0 to IIS 6.1, which is more secure. It should be noted, however that the Windows servers are much less protected from the LAN as is shown in the vulnerability data below. NewComp should carefully examine the availability of its DMZ servers to its LAN. For example, the host at 10.121.116.150 (newcomp.info) has only three ports open from the Internet – smtp, http, and https. However, from the corporate LAN, 24 ports are accessible.

The Firepass SSL-based VPN server from Uroam (recently acquired by F5 Networks) is running a version that was released in February of 2002. Thought there are no known vulnerabilities with this release, we recommend upgrading the software by purchasing a software support contract from F5 Networks. F5 Networks first release of the OS for the FirePass 1000 will be available this month.

There is evidence that some hosts are dual-homes – or at least that there exist multiple paths. For example, the VPN server – 10.121.116.49 shows the following traits. From the Internet the following ports are accessible: 80, 443, 10000, 10001. From the corporate LAN, port 2020 – a control center that purports to allow a user to shut the host down –is also available.
Our tests of the 10.16.0.10/24 network suggested that 10.16.0.49 is the same host (Uroam). Tests of this IP address showed that the following additional ports were open: 22, 81, and 7777.

We recommend that NewComp consider a full review of its LAN corporate security policies. A cursory review of 10.16.0.10 – which appears to be the DHCP server – showed 26 open ports. Furthermore, we were able to log into its web server by using the login “lc2” without a password (it proves to be an Internet video camera). We found additional file servers, databases, and web servers that are used on the corporate LAN and should have their security investigated. Furthermore, we did not examine computers belonging to the financial, legal, or human resources departments – which can be targeted for hacking by disgruntled employees – or by a hacker who compromise a DMZ server that has access to the LAN.

Vulnerability Details by Host

The following sections provide details vulnerability information for each of the hosts discovered during the Perimeter Security Assessment. Each section provides a quick summary of the security risks for each host and associated risk mitigation strategies. A list of open ports is provided as a checklist for the reader to compare with required services. Each vulnerability is treated separately to provide a detailed understanding of security issues.

Vulnerability Details for 10.113.236.100 – adsl-10-113-236-100.xyz.com

Name: adsl-10-113-236-100.xyz.com
OS: Netscreen 5XP running ScreenOS 4.0.r3

Vulnerabilities		
HOLES	WARNINGS	OPEN PORTS
1	0	1

Open Ports		
SERVICE	PORT NUMBER	PROTOCOL
unknown	6552	tcp

This host is a home DSL firewall. We recommend that access to its administrative web port be restricted from the Internet. NewComp should maintain this host at current patch levels. The hosts that this firewall protects were outside the scope of this assessment.

Details Of Vulnerabilities

Denial of Service – Netscreen ScreenOS has been reported prone to a vulnerability that may allow a remote user to trigger a denial of service condition in an affected appliances. It has been reported that by modifying system configuration values that control the TCP windows size, an attacker may connect to and trigger a denial of service in an appliance that is running a vulnerable version of ScreenOS.

Solution: The vendor has addressed this issue in ScreenOS 4.0.3r3 released an later. User are advised to upgrade
Type: Confirmed security hole
Risk Factor: Low

Unknown (6552/tcp) – The remote web server type is: Virata-EmWeb/R6_0_1

Solution: We recommend that the server web configuration to be changed to return a bogus Server header in order to not leak information.
Type: Security note
Risk Factor: Low

Vulnerability Details for 10.116.78.76

Name:10.116.78.76
OS: Netscreen 10 running ScreenOS 3.0.3r1.1

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
1	0	0

This host is a remote DSL firewall. It is a Netscreen 10, which has reached end-of-life status from Netscreen. It should eventually been replaced. No vulnerabilities were found for this host except for the bypass authentication vulnerability below – obtained from securityfocus.com.

Details of Vulnerabilities

Bypass Authentication – Netscreen ScreenOS may allow authentication to be bypassed under some circumstances. In particular, if a user accesses a device from the same source IP address as a previously authenticated user, then they will not be required to authenticate.

Solution: None available
Type: Confirmed security hole
Risk Factor: Low

Vulnerability Details for 10.116.78.77

Name:10.116.78.77
OS: Unknown

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
0	0	0

No information was available for this host.

Vulnerability Details for 10.121.116.33

Name:10.121.116.33
OS: CISCO 2520 Running 12.1(1)

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
0	3	0

Open Ports		
Service	Port Numbers	Protocol
telnet	23	tcp
Dc	2001	tcp
Unknown	4001	tcp
X11:1	6001	tcp
Unknown	9001	tcp

CISCO 2520 routers have reached end-of-life status. Specifically, end of hardware support occurred on May 31st, 2003, and software supports ended May 31st, 2004. In June of 2006, the product will be classified obsolete and even security patches will not be made available for the device. The CIWSCO 2610 is the substitute product. NewComp router is currently running IOS 12.1(1) and there is an upgrade to 12.2(1) available. Administrative access via telnet to this device is available from the Internet on ports 23, 2001, 4001, 6001, and 9001. Administrative access should be limited to the LAN, or require VPN connectivity. The non-standard ports running telnet should be disabled altogether.

Details of Vulnerabilities

General/tcp – The remote host does not discard TCP SYN packets, which have the FIN flag set. Depending on the kind of firewall, an attacker may use this flaw to bypass its rules.

Solution: Contact your vendor for a patch BID: 7487
Type: Security Warning
Risk Factor: Medium

General/tcp – The remote host use non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in replay to another request. This may be used for port scanning and other things.

Solution: Contact your vendor for a patch

Type: Security Warning
Risk Factor: Low

Telent (23/tcp), dc (2001/tcp), unknown (4001/tcp), X11:1 (6001/tcp), & unknown (9001/tcp) – The telnet service is running. This service is dangerous in the sense that it is not ciphered – that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

Solution: Disable telnet access from the Internet
Type: Security Warning
Risk Factor: Low
Telent (23/tcp), dc (2001/tcp), unknown (4001/tcp), X11:1 (6001/tcp), & unknown (9001/tcp) – Remote telnet banner: User Access Verification Password

Type: Security Note
Risk Factor: Low

Vulnerability Details for 10.121.116.34

Name:10.121.116.34
OS: Netscreen 25 WAN running ScreenOS 4.0.3r3

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
0	1	1

Open Ports		
SERVICE	PORT NUMBER	PROTOCOL
unknown	6552	tcp

This is the WAN IP address of NewComp's corporate firewall. We recommend that access to its administrative web port be restricted from the Internet. NewComp should maintain this host at the current patch levels.

Details of Vulnerabilities

General/tcp – The remote host use non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in replay to another request. This may be used for port scanning and other things.

Solution: Contact your vendor for a patch
Type: Security Warning
Risk Factor: Low

Unknown (6552/tcp) - The remote web server type is: Virata_EmWeb/R6_0_1

Solution: We recommend that you configure (if possible)your web server to return a bogus Server header in order to not leak information
Type: Security Node
Risk Factor: Low

Unknown (6552/tcp) – A web server is running on this port

Type: Security Node
Risk Factor: Low

Vulnerability Details for 10.121.116.40 – mail.newcomp.com

Name:10.121.116.40 mail.newcomp.com
OS: Microsoft OS

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
0	2	3

Open Ports		
SERVICE	PORT NUMBER	PROTOCOL
Smtp	25	tcp
http	80	tcp
https	443	tcp

This host is the primary mail server for NewComp. There is a web server available from the Internet, but it does not seem to serve any pages. The https port (443) is open to the Internet, but does not seem to be a secure web server. This host appears to be available from the LAN as mail.newcomp.com (10.16.0.9) with significantly more vulnerabilities – see below. The mail server is running Microsoft Exchange 2000.

Detail of Vulnerabilities

General/tcp – The remote host use non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in replay to another request. This may be used for port scanning and other things.

Solution: Contact your vendor for a patch
Type: Security Warning
Risk Factor: Low

General/tcp – The remote host does not discard TCP SYN packets, which have the FIN flag set. Depending on the kind of firewall, an attacker may use this flaw to bypass its rules.

Solution: Contact your vendor for a patch BID: 7487
Type: Security Warning
Risk Factor: Medium

Smtp (25/tcp) - A SMTP server is running on this port; here is its banner: 220 mail.newcomp.com Microsoft ESMTP MAIL Service

Type: Security Node
Risk Factor: Mediu

Smtp (25/tcp) – This server could be fingerprinted as being Microsoft ESTMP Mail Service

Type: Security Node
Risk Factor: Mediu

http(80/tcp) – The remote server type is Microsoft-IIS/5.0

Solution: Urlscan can be used to change reported server for IIS
Type: Security Node
Risk Factor: Medium

http(80/tcp) – A web server is running on this port

Type: Security Node
Risk Factor: Medium

https(443/tcp) – An unknown service is running on this port. It is usually reserved for HTPPS

Type: Security Node
Risk Factor: Medium

Vulnerability Details for 10.121.116.49 – new.uroam.com

Name:10.121.116.49 mc.uroam.com
OS: Linux OS

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
7	8	4

Open Ports		
SERVICE	PORT NUMBER	PROTOCOL
http	80	tcp
https	443	tcp
Snet-sensor-mgmt	10000	tcp
unknown	10001	tcp

This host is NewComp's Uroam SSL-based VPN server. Uroam has recently aquired by F5 Networks. The version of the Uroam application (Server Version 2.3) is dated from February 2002, and should be upgraded by purchasing software support from F5 Networks. There appear to be several of the standard Linux vulnerabilities with this host. It appears that this server is available from the LAN as mc.uroam.com (10.16.0.49) – and many ports are available from the LAN.

Details of Vulnerabilities

General/icmp - The remote host is vulnerable to an 'icmp leak' – when it receive a packet that raise an ICMP destination unreachable), the ICMP packet is supposed to contain the original message. Due to a bug in the remote TCP/IP stack, it will also contain fragments of the content of the remote kernel memory. An attacker may use this flaw to remotely sniff what is going on into the host's memory, especially network packets that it sees, and obtain useful information such as POP passwords, HTTP authentication fields, and so on.

Solution: Contact your vendor for a fix. If the remote host is running Linux 2.0, upgrade to Linux 2.0.40
Type: Security Warning
Risk Factor: High

General/icmp – The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in replay to another request. This amay be used for portscanning and other things.

Solution: Contact your vendor for a patch
Type: Security Warning
Risk Factor: Low

General/tcp – The remote host does not discard TCP SYN packets, which have the FIN flag set. Depending on the kind of firewall, an attacker may use this flaw to bypass its rules.

Solution: Contact your vendor for a patch BID: 7487
Type: Security Warning
Risk Factor: Medium

http (80/tcp) – The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36 are vulnerable, the remote server may be running a patched version of Apache.

Solution: Upgrade to version 1.3.26 or 2.0.39, or newer
Type: Confirmed Security Hole
Risk Factor: High

http (80/tcp) – Your web server supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracking', 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 this methods
Type: Security Warning
Risk Factor: Medium

http (80/tcp) – A web server is running on this port.

Type: Security Node
Risk Factor: Medium

http (80/tcp) – The remote server type is: Apache and the 'ServerTokens' directive is ProfductOnly. Apache does not permit to hide the server type.

Type: Security Note
Risk Factor: Medium

http (80/tcp) – The following directories were discovered: /cgi-bin

Type: Security Node
Risk Factor: Medium

https (443/tcp) – The remote host seems to be using a version of OpenSSL, which is older than 0.9.6e or 0.9.7-beta3. This version is vulnerable to buffer overflow which may allow an attacker to obtain a shell on this host.

Solution: Upgrade to version o.9.6e or newer.
Type: Confirmed Security Node
Risk Factor: High

https (443/tcp) – The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36 are vulnerable, the remote server may be running a patched version of Apache.

Solution: Upgrade to version 1.3.26 or 2.0.39, or newer
Type: Confirmed Security Hole
Risk Factor: High

https (443/tcp) – Your web server supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracking', 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 this methods
Type: Security Warning
Risk Factor: Medium

https (443/tcp) – The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack.

Security: Disable those ciphers and upgrade your client software if necessary
Type: Security Warning
Risk Factor: Medium

https (443/tcp) – This TLSv1 server also accepts SSLv2connections. This TLSv1 server also accepts SSLv3 connections.

Type: Security Node
Risk Factor: Medium

Snet-sensor-mgmt (10000/tcp) – The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running a patched version of Apache.

Solution: Upgrade to version 1.3.26 or 2.0.39 or newer.
Type: Confirmed Security Hole

Unknown (10001/tcp) - The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36 are vulnerable, the remote server may be running a patched version of Apache.

Solution: Upgrade to version 1.3.26 or 2.0.39, or newer
Type: Confirmed Security Hole
Risk Factor: High

Unknown (10001/tcp) - The remote host seems to be using a version of OpenSSL, which is older than 0.9.6e or 0.9.7-beta3. This version is vulnerable to buffer overflow which may allow an attacker to obtain a shell on this host.

Solution: Upgrade to version o.9.6e or newer.
Type: Confirmed Security Node
Risk Factor: High

Vulnerability Details for 10.121.116.145

Name:10.121.116.145
OS: Netscreen 25 DMZ running ScreenOS 4.0.3r3

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
0	1	1

Open Ports		
unknown	6552	tcp

This is the DMZ, IP address of NewComp's corporate firewall. We recommend that access to its administrative web port be restricted from the Internet. NewComp should maintain this host at the current patch levels.

Details of Vulnerabilities

Unknown (6552/tcp) – The remote web server type is: Virata-EmWeb/R6_0_1

Solution: We recommend that the server configuration to be changed to return a bogus Server header (if possible), in order not to leak information.
Type: Security Node
Risk Factor: Medium

Unknown (6552/tcp) – A web server is running on this port

Type: Security Node
Risk Factor: Medium

Vulnerability Details for 10.121.116.150 – upinfo.newcomp.info

Name:upinfo.newcomp.info
OS: Microsoft OS

Vulnerabilities		
HOLE	WARNINGS	OPEN PORTS
7	28	24

Open Ports		
SERVICE	PORT NUMBER	PROTOCOL
Smtp	25	tcp
Domain	53	tcp
http	80	tcp
Loc-serv	135	Tcp
Netbios-ssn	139	tcp
https	443	tcp
Snpp	444	tcp
Microsoft-ds	445	tcp
Lanserver	637	Tcp
Unknown	1002	tcp
NFS-or-IIS	1025	tcp
Ms-Isa	1029	tcp
Isd3	1032	tcp
Netinfo	1033	tcp
Unknown	1035	tcp
Ms-sql-s	1433	tcp
Wms	1755	tcp
Compaqdiag	2301	tcp
Msdtc	3372	tcp
Ms-term-serv	3389	tcp
Irc-serv	6666	tcp

While this host – the secondary email server – has 24 ports open from the LAN, only the mail, web and secure web ports are open from the Internet. The data served on both the normal web and the secure web appears to be the same. There are many unneeded services running on this host, and they should be disabled. There is a high duplication of services with several ports running web servers – most of which appear to be unused. There are some configuration changes that should be made to the web server to reduce vulnerability level. This host is running multiple web sites, a DNS server, MS SQL, and Terminal Services. If these are not used, they should be disabled. The web server is

running IIS 5.0 and have many of the expected vulnerabilities if the IIS server has not been adequately locked down.

Details of Vulnerabilities

General/tcp – The remote host does not discard TCP SYN packets, which have the FIN flag set. Depending on the kind of firewall, an attacker may use this flaw to bypass its rules.

Solution: Contact your vendor for a patch BID: 7487
Type: Security Warning
Risk Factor: Medium

General/tcp – The remote host use non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in replay to another request. This may be used for port scanning and other things.

Solution: Contact your vendor for a patch
Type: Security Warning
Risk Factor: Low

Smtp (25/tcp) - A SMTP server is running on this port; here is its banner: 220 mail.newcomp.info Microsoft ESMTP MAIL Service

Type: Security Node
Risk Factor: Mediu

Smtp (25/tcp) – This server could be fingerprinted as being Microsoft ESTMP Mail Service

Type: Security Node
Risk Factor: Mediu

Domain (53/udp) – A DNS server is running on this port. If it is not used, please disabled it.

Type: Security Node
Factor Risk: Low

http (80/tcp) – The remote FrontPage server may leak information on the anonymous user.

Type: Confirmed Hole
Risk Factor: Low

http (80/tcp) – The remote host has FrontPage Extensions (FPSE) installed. There is a denial of service / buffer overflow conditions in the program 'shtml.exe' which comes with it. Please see the Microsoft Security Bulletin MS02-053 to determine if the server is vulnerable or not.

Solution Please see http://www.microsoft.com/technet/security/bulletin/ms02-053.asp BID : 5804
Type: Confirmed security hole
Risk Factor: High

http (80/tcp) – The IIS server appears to have .IDA ISAPI (filter mapped). At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033 and gives remote SYSTEM level access to the web server.

Solution: Patch the system, and unmap the .IDA extensions and any other unused ISAPI extensions
Type: Security warning
Risk Factor: Medium

http (80/tcp) – Your web server supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracking', 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 this methods
Type: Security Warning
Risk Factor: Medium

http (80/tcp) – The remote server is running with WebDAV enabled. WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If this extension is not used, it should be disabled.

Solution: If you use IIS, refer to Microsoft KB article Q241520
Type: Security warning
Risk Factor: Medium

http (80/tcp) – IIS 5 has support for the Internet Printing Protocol (IPP) which is enabled in the default install – we recommend to disable, is this functionality is not used.

Solution: Unmap the .printer extension
Type: Security warning

Risk Factor: Low

http (80/tcp) – The remote server appears to be running with the FrontPage extension. You should check the configuration since a lot of security problems has been found with FrontPage when the configuration file is not well set up.

Type: Security warning
Risk Factor: High

http (80/tcp) – The remote Web server type is: Microsoft-IIS/5.0

Solution: Use urlscan to change reported server for IIS
Type: Security note
Risk Factor: High

Loc-serv (135/tcp) – DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host.

Solution: Filter incoming traffic to the host
Type: Security Warning
Risk Factor: Low

https (80/tcp) – The IIS server appears to have .IDA ISAPI (filter mapped). At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033 and gives remote SYSTEM level access to the web server.

Solution: Patch the system, and unmap the .IDA extensions and any other unused ISAPI extensions
Type: Security warning
Risk Factor: Medium

https (80/tcp) – The remote server is running with WebDAV enabled. WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If this extension is not used, it should be disabled.

Solution: If you use IIS, refer to Microsoft KB article Q241520
Type: Security warning
Risk Factor: Medium

https (443/tcp) – The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak “export class” ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack.

Security: Disable those ciphers and upgrade your client software if necessary
Type: Security Warning
Risk Factor: Medium

Snpp (444/tcp) – The remote host has FrontPage Server Extensions (FPSE) installed. There is a denial of service / buffer overflow condition in the program 'shtml.exe' which come with it – an attacker may use it to crash your web server (FPSE2000) or execute arbitrary code (FPSE2002). Microsoft Security Bulletin MS02-053

Solution Please see http://www.microsoft.com/technet/security/bulletin/ms02-053.asp BID : 5804
Type: Confirmed security hole
Risk Factor: High

Snpp (444/tcp) – The remote server is running with WebDAV enabled. WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If this extension is not used, it should be disabled.

Solution: If you use IIS, refer to Microsoft KB article Q241520
Type: Security warning
Risk Factor: Medium

Microsoft-ds (445/tcp) – It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password which grants the user the 'guest' access.

Type: Confirmed Security hole
Risk Factor: Low

Microsoft-ds (445/tcp) – The host SID can be obtained remotely. An attacker can use it to obtain the list of the local users of this host.

Type: Security warning
Risk Factor: Low

Microsoft-ds (445/tcp) – Some users have passwords, which never expire.

Solution: Disable password non-expiry
Type: Security warning
Risk factor: Medium
Ms-sql-s (1433/tcp) – Microsoft SQL server is running on this port – never let any unauthorized users establish connections to this service.

Solution: Block this port from outside communication
Type: Security node
Risk Factor: Medium

Compaqdiag (2301/tcp) – Remote Compaq HTTP server version 4.2

Type: Security warning
Risk Factor: Medium

Msdtc (3372/tcp) – Unknown server is running on this port

Type: Security node
Risk Factor: Medium

Ms-term-serv (3389/tcp) – The terminal Services are enabled on the remote host. Note that RDP (Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackersto steal the credentials of legitimates users by impersonating the Windows server.

Solution: Disable the Terminal Services – do not allow this service to run across the Internet
Type: Security warning
Risk Factor: Medium

REFERENCES

[1] Security Policy, Assessment, and Vulnerability Analysis

http://www.microsoft.com/technet/security/topics/assess/default.mspx

[2] Security Assessment Methodology

http://www.networkmagazineindia.com/200112/cover2.htm

[3] Network security

http://www.itprc.com/security.htm

[4] UC Davis Informational & Educational Technology

http://security.ucdavis.edu/security101.cfm

http://security.ucdavis.edu/assess.cfm

[5] Library Computer and Network Security

http://www.infopeople.org/howto/security/index.html

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event