Host Report

Introduction

This report provides detailed information about all the different hosts that were tested as part of this penetration test. Each one of the reported vulnerabilities was actively exploited in order to obtain control, elevate privileges or obtain information about the vulnerable host. None of these results are potential, all of them were practically tested as part of this test.

The report also provides information about the exposures found on hosts, which are system configuration issues that allow access to information that can be used as a stepping-stone towards gaining access to the systems themselves.

Additionally, this report includes information gathered via the network as well as by executing code on the compromised

Workspace Summary

Name: Report2
Started: 5/1/2012 10:14:46AM
Finished: 5/1/2012 11:16:52AM
Exact Time: 1 hour 2 minutes 6 seconds
Running Time: 28 minutes 9 seconds

Workspace Summary of discovered hosts

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total amount of hosts:</td>
<td>5</td>
</tr>
<tr>
<td>Total compromised hosts:</td>
<td>3</td>
</tr>
<tr>
<td>(hosts with known vulnerabilities)</td>
<td></td>
</tr>
<tr>
<td>Total exposed hosts:</td>
<td>5</td>
</tr>
<tr>
<td>(hosts with known exposures)</td>
<td></td>
</tr>
<tr>
<td>Average number of exploited vulnerabilities per compromised host:</td>
<td>2.00</td>
</tr>
<tr>
<td>Average number of exposures per exposed host:</td>
<td>5.60</td>
</tr>
</tbody>
</table>
Hosts per Operating System

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>linux</td>
<td>1</td>
</tr>
<tr>
<td>solaris</td>
<td>1</td>
</tr>
<tr>
<td>windows</td>
<td>3</td>
</tr>
</tbody>
</table>

Total 5

Hosts per Operating System Version

<table>
<thead>
<tr>
<th>Operating System &amp; Version</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>linux 2.4</td>
<td>1</td>
</tr>
<tr>
<td>solaris 8</td>
<td>1</td>
</tr>
<tr>
<td>windows 2000</td>
<td>2</td>
</tr>
<tr>
<td>windows 2003</td>
<td>1</td>
</tr>
</tbody>
</table>

Total* 5

(*) "Unknown" Operating Systems are not shown
Compromised Hosts per Operating System

- Total: 3
  - linux: 1
  - windows: 2

Exposed Hosts per Operating System

- Total: 5
  - linux: 1
  - solaris: 1
  - windows: 3
Compromised Hosts per Operating System Version

(*) "Unknown" Operating System versions are not shown

Exposed Hosts per Operating System Version

(*) "Unknown" Operating System versions are not shown
### Most Exploited Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.36.22</td>
<td>2K3622</td>
<td>3</td>
</tr>
<tr>
<td>192.168.36.26</td>
<td>2K3626</td>
<td>2</td>
</tr>
<tr>
<td>192.168.36.23</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>192.168.36.30</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>192.168.36.28</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>

(*) At most ten hosts are shown, and ties with the last shown host are not included.
**Most Exposed Hosts**

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Host Name</th>
<th>Exposures</th>
</tr>
</thead>
<tbody>
<tr>
<td>/192.168.36.22</td>
<td>2K3622</td>
<td>7</td>
</tr>
<tr>
<td>/192.168.36.30</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>/192.168.36.23</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>/192.168.36.26</td>
<td>2K3626</td>
<td>5</td>
</tr>
<tr>
<td>/192.168.36.28</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td>28</td>
</tr>
</tbody>
</table>

(*) At most ten hosts are shown, and ties with the last shown host are not included.

**Host - 192.168.36.22**

- **Host Name:** 2K3622
- **Visibility Path:** /192.168.36.22
- **Operating System:** Windows 2000 (i386)

**TCP Ports in state listen**

80, 135, 139, 443, 445, 1025, 1028-1029, 3372, 3389

**UDP Ports in state listen**

161

**Services Found**

- http (80-tcp)
- microsoft-ds (445-tcp)
- solid-mux (1029-tcp)
- https (443-tcp)
- msdcm (3372-tcp)
- msrdp (3389-tcp)
- loc-srv (135-tcp)
- loc-srv (1025-tcp)
- netbios-ssn (139-tcp)

**Vulnerabilities**

- A NETBIOS/SMB share password is the default, null, or missing. (CVE-1999-0519)
- Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms. (CVE-2003-0352)
- The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability." (CVE-2008-4250)

**Exposures**

- **Visibility:** External
- **Title:** NetBIOS Active on Internet Device
- **Severity:** HIGH
- **Service:** netbios-ssn
- **Exptype:** service
- **Description:** NetBIOS (Network Basic Input/Output System) is a protocol utilized in Microsoft networks. NetBIOS provides the remote interface that enables file and print sharing. These services are commonly found in Internal Networks for workgroup and/or domain structures. NetBIOS has many known...
Vulnerabilities associated with it and should never be found in Legitimate Internet traffic. Most NetBIOS vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. These vulnerabilities receive high security threat violation status.

Visibility: External
Title: SVRLOC Active on Internet Device
Severity: HIGH
Service: loc-srv
Exptype: service
Description: The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks. It has been defined in RFC 2608 and RFC 3224 as Standards Track document.

Visibility: External
Title: NetBIOS-DS Active on Internet Device
Severity: HIGH
Service: microsoft-ds
Exptype: service
Description: NetBIOS-DS (Network Basic Input/Output System Directory Service) is a protocol utilized in Microsoft 2000/2003 networks. NetBIOS-DS provides the remote interface that enables file and print sharing. These services are commonly found in Internal Networks for workgroup and/or domain structures. NetBIOS-DS has many known vulnerabilities associated with it and should never be found in Legitimate Internet traffic. Most NetBIOS-DS vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. These vulnerabilities receive high security threat violation status.

Visibility: External
Title: HTTP Active on Internet Device
Severity: LOW
Service: http
Exptype: service
Description: Hypertext Transfer Protocol (HTTP) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.

Visibility: External
Title: HTTPS Active on Internet Device
Severity: LOW
Service: https
Exptype: service
Description: Hypertext Transfer Protocol Secure (HTTPS) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages. HTTPS utilizes SSL (Secure Sockets Layer) to encrypt connections between the client and server.

Visibility: External
Title: MS-RPC Active on Internet Device
Severity: HIGH
Service: loc-srv
Exptype: service
Description: MS-RPC (Microsoft Remote Procedure Call) is a protocol utilized in Microsoft networks. MS-RPC provides a remote interface that allows process execution. This service is commonly found on Internal Networks and is designed for workgroup and/or domain structures. MS-RPC has many known vulnerabilities associated with it and should never be found in legitimate Internet traffic. Most MS-RPC vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. This vulnerability receives a high security threat violation status.

Visibility: External
Title: Internet Device Responded to ICMP
Severity: MEDIUM
Service: n/a
Exptype: icmp-responded
Description: ICMP is a protocol that network professionals utilize to troubleshoot Internet connectivity problems. ICMP Echo requests (or PING) send network traffic toward a specific IP host. The IP host then responds to the request with a reply. This proves that network connectivity between two network hosts is functional. On the Internet, devices should never have ICMP enabled or should be protected behind a firewall. When ICMP is accessible from the Internet, intruders can potentially flood the device with constant large ICMP packets. ICMP flooding has the potential to cause a DOS (Denial of Service) attack. Internet devices running ICMP can also provide intruders with the knowledge of the OS (Operating System) that the remote device is running. This process is known as ICMP-fingerprinting. Since ICMP may allow for a DOS attack or OS determination it receives a medium security violation status.

Host - 192.168.36.23

Visibility Path: /192.168.36.23
Operating System: Linux 2.4  (i386)

TCP Ports in state listen
22, 80, 111, 443, 1024, 6000

UDP Ports in state listen
111

Services Found
http (80-tcp)  https (443-tcp)  ssh (22-tcp)  status (1024-tcp)
status (1024-udp)  sunrpc (111-tcp)  sunrpc (111-udp)  x11 (6000-tcp)

Vulnerabilities
- Double free vulnerability in OpenSSL 0.9.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding. (CVE-2003-0545)

Exposures

Visibility: External
Title: SSH Active on Internet Device
Severity: MEDIUM
Service: ssh
Exptype: service
Description: SSH (Secure SHell) is a network protocol that allows creation of a secure channel between a local and remote computer. It uses public-key cryptography to authenticate the remote computer and optionally, to allow the remote computer to authenticate the user. SSH provides confidentiality and
integrity of data exchanged between the two computers using encryption and message authentication codes (MACs). SSH is typically used to log into a remote machine and execute commands. SSH also supports tunneling or forwarding of arbitrary TCP and X11 connections; it can transfer files using the associated SFTP or SCP protocols. An SSH server, by default, listens on the standard TCP port 22.

Visibility: External
Title: HTTP Active on Internet Device
Severity: LOW
Service: http
Exptype: service
Description: Hypertext Transfer Protocol (HTTP) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.

Visibility: External
Title: HTTPS Active on Internet Device
Severity: LOW
Service: https
Exptype: service
Description: Hypertext Transfer Protocol Secure (HTTPS) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages. HTTPS utilizes SSL (Secure Sockets Layer) to encrypt connections between the client and server.

Visibility: External
Title: ONC-RPC Active on Internet Device
Severity: HIGH
Service: sunrpc
Exptype: service
Description: ONC-RPC (Open Network Computing Remote Procedure Call also known as portmapper or SUN-RPC) is a protocol utilized in UNIX networks. This service is commonly found on Internal Networks and is designed for mapping RPC applications. ONC-RPC has many known vulnerabilities associated with it and should never be found in legitimate Internet traffic. Most ONC-RPC vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. This vulnerability receives a high security threat violation status.

Visibility: External
Title: Internet Device Responded to ICMP
Severity: MEDIUM
Service: n/a
Exptype: icmp-responded
Description: ICMP is a protocol that network professionals utilize to troubleshoot Internet connectivity problems. ICMP Echo requests (or PING) send network traffic toward a specific IP host. The IP host then responds to the request with a reply. This proves that network connectivity between two network hosts is functional. On the Internet, devices should never have ICMP enabled or should be protected behind a firewall. When ICMP is accessible from the Internet, intruders can potentially flood the device with constant large ICMP packets. ICMP flooding has the potential to cause a DOS (Denial of Service) attack. Internet devices running ICMP can also provide intruders with the knowledge of the OS (Operating System) that the remote device is running. This process is known as ICMP-fingerprinting. Since ICMP may allow for a DOS attack or OS determination it receives a medium security violation status.
Visibility                  External
Title                      Version Disclosure on a Service
Severity                    MEDIUM
Service                     n/a
Exptype                     banner
Description                 A service is providing a banner that might be revealing too much information. Services: ssh

Host - 192.168.36.26

Host Name:                2K3626
Visibility Path:          /192.168.36.26
Operating System:         Windows 2000  (i386)

TCP Ports in state listen
135, 139, 445, 1025, 1030, 3372, 3389

UDP Ports in state listen
161

Services Found
iad1 (1030-tcp)           loc-srv (135-tcp)           loc-srv (1025-tcp)           microsoft-ds (445-tcp)
msrdp (3389-tcp)           netbios-ssn (139-tcp)         tip2 (3372-tcp)

Vulnerabilities
- A NETBIOS/SMB share password is the default, null, or missing. (CVE-1999-0519)
- Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms. (CVE-2003-0352)

Exposures

Visibility                  External
Title                      NetBIOS Active on Internet Device
Severity                    HIGH
Service                     netbios-ssn
Exptype                     service
Description                 NetBIOS (Network Basic Input/Output System) is a protocol utilized in Microsoft networks. NetBIOS provides the remote interface that enables file and print sharing. These services are commonly found in Internal Networks for workgroup and/or domain structures. NetBIOS has many known vulnerabilities associated with it and should never be found in Legitimate Internet traffic. Most NetBIOS vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. These vulnerabilities receive high security threat violation status.

Visibility                  External
Title                      SVRLOC Active on Internet Device
Severity                    HIGH
Service                     loc-srv
Exptype                     service
Description                 The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows computers
and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks. It has been defined in RFC 2608 and RFC 3224 as Standards Track document.

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>NetBIOS-DS Active on Internet Device</td>
</tr>
<tr>
<td>Severity</td>
<td>HIGH</td>
</tr>
<tr>
<td>Service</td>
<td>microsoft-ds</td>
</tr>
<tr>
<td>Exptype</td>
<td>service</td>
</tr>
<tr>
<td>Description</td>
<td>NetBIOS-DS (Network Basic Input/Output System Directory Service) is a protocol utilized in Microsoft 2000/2003 networks. NetBIOS-DS provides the remote interface that enables file and print sharing. These services are commonly found in Internal Networks for workgroup and/or domain structures. NetBIOS-DS has many known vulnerabilities associated with it and should never be found in Legitimate Internet traffic. Most NetBIOS-DS vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. These vulnerabilities receive high security threat violation status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>MS-RPC Active on Internet Device</td>
</tr>
<tr>
<td>Severity</td>
<td>HIGH</td>
</tr>
<tr>
<td>Service</td>
<td>loc-srv</td>
</tr>
<tr>
<td>Exptype</td>
<td>service</td>
</tr>
<tr>
<td>Description</td>
<td>MS-RPC (Microsoft Remote Procedure Call) is a protocol utilized in Microsoft networks. MS-RPC provides a remote interface that allows process execution. This service is commonly found on Internal Networks and is designed for workgroup and/or domain structures. MS-RPC has many known vulnerabilities associated with it and should never be found in legitimate Internet traffic. Most MS-RPC vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. This vulnerability receives a high security threat violation status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Internet Device Responded to ICMP</td>
</tr>
<tr>
<td>Severity</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Service</td>
<td>n/a</td>
</tr>
<tr>
<td>Exptype</td>
<td>icmp-responded</td>
</tr>
<tr>
<td>Description</td>
<td>ICMP is a protocol that network professionals utilize to troubleshoot Internet connectivity problems. ICMP Echo requests (or PING) send network traffic toward a specific IP host. The IP host then responds to the request with a reply. This proves that network connectivity between two network hosts is functional. On the Internet, devices should never have ICMP enabled or should be protected behind a firewall. When ICMP is accessible from the Internet, intruders can potentially flood the device with constant large ICMP packets. ICMP flooding has the potential to cause a DOS (Denial of Service) attack. Internet devices running ICMP can also provide intruders with the knowledge of the OS (Operating System) that the remote device is running. This process is known as ICMP-fingerprinting. Since ICMP may allow for a DOS attack or OS determination it receives a medium security violation status.</td>
</tr>
</tbody>
</table>

**Host - 192.168.36.28**

| Visibility Path: | /192.168.36.28 |
| Operating System: | ![Solaris 8 (SPARC_v8)](image) |
TCP Ports in state listen
21, 23, 7100, 32772

Services Found
- font-service (7100-tcp)
- ftp (21-tcp)
- sometimes-rpc7 (32772-tcp)
- telnet (23-tcp)

Exposures

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>FTP Active on Internet Device</td>
</tr>
<tr>
<td>Severity</td>
<td>LOW</td>
</tr>
<tr>
<td>Service</td>
<td>ftp</td>
</tr>
<tr>
<td>Exptype</td>
<td>service</td>
</tr>
<tr>
<td>Description</td>
<td>FTP (File Transfer Protocol) is the Internet language responsible for transferring or uploading/downloading of files to and from Internet sites. Internet sites often host such services even when they do not appear to have FTP links on their website. FTP services should be protected with access-lists to protect them from any Internet client connecting to them. If the FTP service is meant to be accessible to every Internet client, then this warning can be ignored. If this is undesirable, then this service should be protected. Since this does not lead to any direct system compromise or theft of data, it is classified as information gathering and receives a low threat rating.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Telnet Active on Internet Device</td>
</tr>
<tr>
<td>Severity</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Service</td>
<td>telnet</td>
</tr>
<tr>
<td>Exptype</td>
<td>service</td>
</tr>
<tr>
<td>Description</td>
<td>TELNET services provide a method to remotely configure network devices over an IP network. On an internal IP network, administrators often use telnet to remotely configure routers, switches, and firewalls. Telnet should never be accessible to Internet clients. If telnet is accessible over the Internet, an intruder can begin to brute force passwords on the device to gain system access. Some telnet DOS (Denial of Service) attacks are easily exploited to effectively shut down communications to the networked device. Since this could potentially lead to system compromise it is classified as penetration setup and receives a medium threat rating.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visibility</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Internet Device Responded to ICMP</td>
</tr>
<tr>
<td>Severity</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Service</td>
<td>n/a</td>
</tr>
<tr>
<td>Exptype</td>
<td>icmp-responded</td>
</tr>
<tr>
<td>Description</td>
<td>ICMP is a protocol that network professionals utilize to troubleshoot Internet connectivity problems. ICMP Echo requests (or PING) send network traffic toward a specific IP host. The IP host then responds to the request with a reply. This proves that network connectivity between two network hosts is functional. On the Internet, devices should never have ICMP enabled or should be protected behind a firewall. When ICMP is accessible from the Internet, intruders can potentially flood the device with constant large ICMP packets. ICMP flooding has the potential to cause a DOS (Denial of Service) attack. Internet devices running ICMP can also provide intruders with the knowledge of the OS (Operating System) that the remote device is running. This process is known as ICMP-fingerprinting. Since ICMP may allow for a DOS attack or OS determination it receives a medium security violation status.</td>
</tr>
</tbody>
</table>
Host - 192.168.36.30

Visibility Path: /192.168.36.30

Operating System: Windows 2003 SP 2 (i386)

TCP Ports in state listen
25, 110

UDP Ports in state listen
53, 135

Services Found
- domain (53-udp)
- loc-srv (135-udp)
- pop-3 (110-tcp)
- smtp (25-tcp)

Exposures

Visibility External

Title SMTP Active on Internet Device

Severity LOW

Service smtp

Exptype service

Description SMTP (Simple Mail Transfer Protocol) is the network protocol typically responsible for relaying and delivering e-mail to and from network hosts and Internet domains. SMTP however, due to its simple format, is easily exploited to perform an array of network attacks. Spamming or UCE (Unsolicited Commercial E-mail), is a popular term referenced in the networking community that refers to the SMTP service when it allows any machine to submit mail destined for anyone for delivery without the need to authenticate. This gives intruders the ability to send network viruses and malicious content to the entire networked organization, anonymously. This along with other vulnerabilities makes SMTP a quick target for attackers.

Visibility External

Title SVRLOC Active on Internet Device

Severity HIGH

Service loc-srv

Exptype service

Description The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks. It has been defined in RFC 2608 and RFC 3224 as Standards Track document.

Visibility External

Title DNS Active on Internet Device

Severity LOW

Service domain

Exptype service

Description DNS (Domain Name Services) are services responsible for resolving Internet and internal host names to IP addresses. Internet clients, along with internal IP clients, use DNS to essentially find computers on the network by computer host name, rather than using IP addresses. Intruders find DNS services of particular interest as they can often aid in finding other network targets. Hackers employ special methods to obtain host computer names from the DNS even when they are not authorized.
**Title**
MS-RPC Active on Internet Device

**Severity**
HIGH

**Description**
MS-RPC (Microsoft Remote Procedure Call) is a protocol utilized in Microsoft networks. MS-RPC provides a remote interface that allows process execution. This service is commonly found on internal networks and is designed for workgroup and/or domain structures. MS-RPC has many known vulnerabilities associated with it and should never be found in legitimate Internet traffic. Most MS-RPC vulnerabilities lead directly to system compromise through brute forcing of passwords and buffer overflow attacks. This vulnerability receives a high security threat violation status.

**Title**
POP3 Service Discovered

**Severity**
MEDIUM

**Description**
POP3 (Post office Protocol version 3) is the protocol responsible for allowing IP hosts to download e-mail from a mail server hosting these services. POP3 allows for many concurrent connections from a single host, as well as multiple attempts to guess a password for a user account. This makes POP3 services a prime target for brute force password attacks. An intruder will use these services to derive valid user identities on the network. If no password lockout policies are set, this could become a serious threat. Most POP3 services lack integration to select which users can and cannot access the service remotely. Most internal mail services, such as Microsoft's Exchange Server and Novell's GroupWise Server, offer proprietary protocols for obtaining mail on the mail server. If this is the case POP3 can safely be removed from the affected server.

**Title**
Internet Device Responded to ICMP

**Severity**
MEDIUM

**Description**
ICMP is a protocol that network professionals utilize to troubleshoot Internet connectivity problems. ICMP Echo requests (or PING) send network traffic toward a specific IP host. The IP host then responds to the request with a reply. This proves that network connectivity between two network hosts is functional. On the Internet, devices should never have ICMP enabled or should be protected behind a firewall. When ICMP is accessible from the Internet, intruders can potentially flood the device with constant large ICMP packets. ICMP flooding has the potential to cause a DOS (Denial of Service) attack. Internet devices running ICMP can also provide intruders with the knowledge of the OS (Operating System) that the remote device is running. This process is known as ICMP-fingerprinting. Since ICMP may allow for a DOS attack or OS determination it receives a medium security violation status.

**Title**
Version Disclosure on a Service

**Severity**
MEDIUM

**Description**
A service is providing a banner that might be revealing too much information. Services: pop-3
<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Workspace Summary</td>
<td>1</td>
</tr>
<tr>
<td>/192.168.36.22 - 2K3622 - (3 vuln)</td>
<td>6</td>
</tr>
<tr>
<td>/192.168.36.23 - (1 vuln)</td>
<td>8</td>
</tr>
<tr>
<td>/192.168.36.26 - 2K3626 - (2 vuln)</td>
<td>10</td>
</tr>
<tr>
<td>/192.168.36.28</td>
<td>11</td>
</tr>
<tr>
<td>/192.168.36.30</td>
<td>12</td>
</tr>
</tbody>
</table>