



SecPoint - Full Scan Report

Scan Name: credential

Audited on 2016-10-02 13:23:33

Confidential

© SecPoint ® 1999-2017

Table of Contents

Introduction	3
Severity Levels	4
Executive Summary	5
Traceroute	7
Identified Ports and Services	8
Version Banner Identified	9
Summary of Vulnerabilities	11
Vulnerabilities	15
IP: 192.168.1.1	15
IP: 192.168.1.6	24
IP: 192.168.1.139	32
IP: 192.168.1.170	33
IP: 192.168.1.234	36
Gap analysis	37
IP: 192.168.1.1	37
IP: 192.168.1.6	38
IP: 192.168.1.139	39
IP: 192.168.1.170	40
IP: 192.168.1.234	41
Offline Nodes	42

Introduction

This report is the result of an "online vulnerability assessment scan", performed by **SecPoint**.

This document has been compiled and arranged to provide a quick and easy-to-understand report to simplify the task of securing computer systems and IT equipment connected to the Internet.

System vulnerabilities are categorised under one of four headings: **High risk, Medium risk, Low risk or Information**. A detailed explanation of each category of vulnerability can be found under the heading of **Severity Levels**.

An **Executive Summary** has been compiled specifically for a management level review. This summary contains both written and graphic details based upon the results of the scanner. These results include such information as "when the scan was performed", "who performed the scan", and the amount of system vulnerabilities found in each category.

The **Executive Summary** also includes a conclusion reporting the "overall security level" of the tested system.

Details and names of vulnerabilities discovered are found under the heading of **Summary of vulnerabilities**. This is followed by individual descriptions for fixing each found vulnerability.

Where possible, a **Bugtraq ID(*)**, a **CVE(**)** and/or a **USN(***)** are present, for further details.

Every system vulnerability discovered is supplied with a possible remedy.



(*) Bugtraq ID is the official Securityfocus.com ID; Also known as bugtraq.

(**) CVE is the official CVE Mitre list.

(***) USN is the official Ubuntu Security Notice list.

Severity Levels

High Risk Vulnerabilities

When a high risk vulnerability is identified, it means that it is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive system information. This in turn could lead to theft or loss of private and sensitive data.

Medium Risk Vulnerabilities

When a medium Risk vulnerability is identified, it means that an intruder can gain access to system information that could lead to more specific attacks and possibly a full system compromise. This in turn could lead to theft or loss of private and sensitive data.

Low Risk Vulnerabilities

When a low risk vulnerability is identified, it generally means that an intruder can gain access to system information that can aid and lead to more specific attacks resulting in the theft or loss of private and sensitive data.

Information

All entries at this level simply provide additional information to that already available about the tested system. It doesn't imply that the system is vulnerable or not.

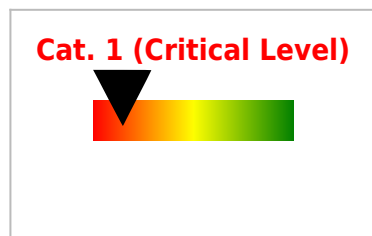
Executive Summary

This report represents a security scan performed by **SecPoint**. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network security.

Scan Name	credential	Scan Profile	Best Scan
Started at	2016-10-02 13:23:33	Ended at	2016-10-02 14:28:23
Duration	01:04:50 (1 hour, 4 minutes, 50 seconds)		
Scan Engine	9.8.1.136		
List of audited IPs	192.168.1.0, 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14, 192.168.1.15, 192.168.1.16, 192.168.1.17, ... ,192.168.1.255		

This scan was performed with SecPoint® Penetrator by user **admin**.

Overall Security Level



The scan performed by **SecPoint** has determined that your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data. It is recommended that you take immediate action to improve the security level.

Online Nodes

The following nodes were online at the time of scan:

192.168.1.1, 192.168.1.6, 192.168.1.139, 192.168.1.170, 192.168.1.234

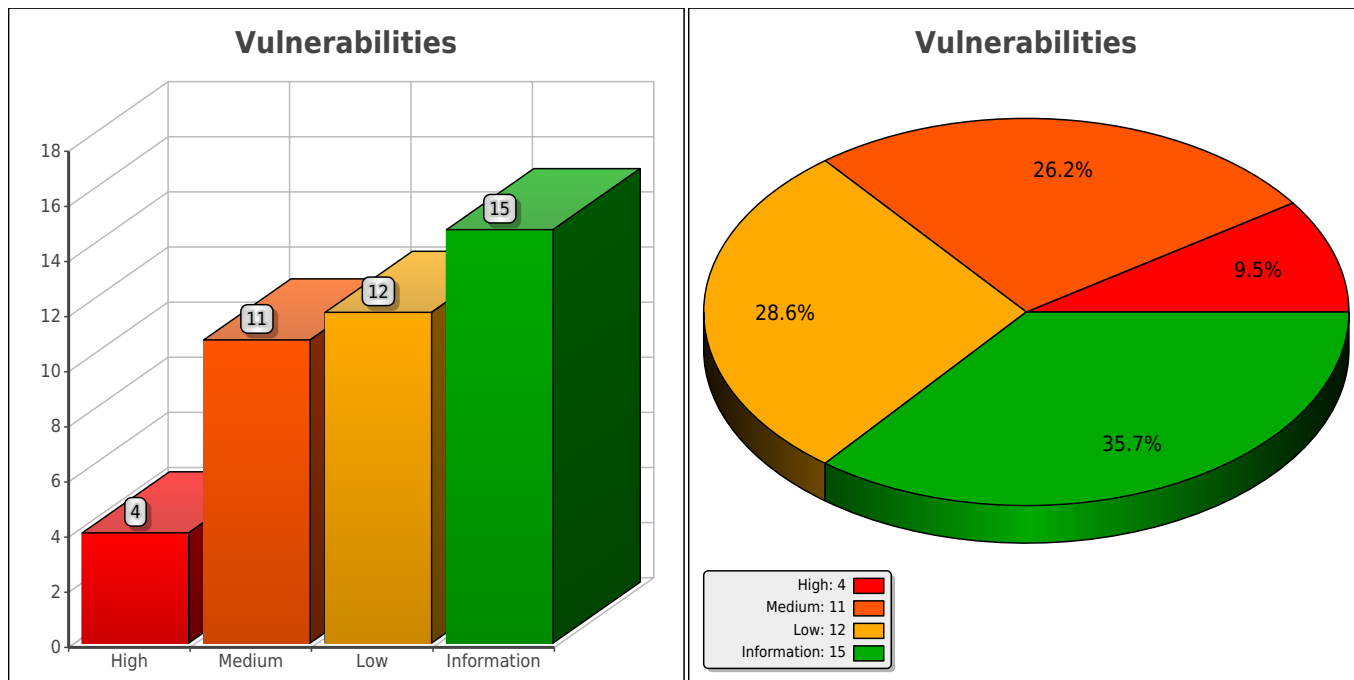
Offline Nodes

Some Nodes were offline at the time of scan, so they were excluded from the results above.

Offline Nodes: 192.168.1.0, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14, 192.168.1.15, 192.168.1.16, 192.168.1.17, 192.168.1.18, 192.168.1.19, ... ,192.168.1.255

Vulnerabilities

42 potential vulnerabilities identified, with the following risk levels:



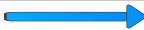
Comments

This is a user-added comment to the report

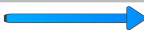
Traceroute

This is the result of a traceroute from SecPoint to the target systems:

traceroute to 192.168.1.1 (192.168.1.1), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	192.168.1.1	192.168.1.1		2.108	

traceroute to 192.168.1.6 (192.168.1.6), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	penetrator.nfrpiero.com	192.168.1.6		0.005	

traceroute to 192.168.1.139 (192.168.1.139), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	192.168.1.139	192.168.1.139		6.970	

traceroute to 192.168.1.170 (192.168.1.170), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	192.168.1.170	192.168.1.170		5.944	

traceroute to 192.168.1.234 (192.168.1.234), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	192.168.1.234	192.168.1.234		6.820	

Identified Ports and Services

The following Ports and Services were identified on the target systems:

Ports and Services for IP: 192.168.1.1

Port	Protocol	Status	Service
23	tcp	open	Telnet
80	tcp	open	World Wide Web HTTP
139	tcp	open	NETBIOS Session Service
443	tcp	open	http protocol over TLS/SSL
445	tcp	open	Microsoft-DS

Ports and Services for IP: 192.168.1.6

Port	Protocol	Status	Service
25	tcp	open	Simple Mail Transfer
37	tcp	open	Time
80	tcp	open	World Wide Web HTTP
113	tcp	open	
443	tcp	open	http protocol over TLS/SSL
587	tcp	open	Submission
3790	tcp	open	QuickBooks RDS
5432	tcp	open	PostgreSQL Database
6001	tcp	open	Administration Server Connector

Ports and Services for IP: 192.168.1.139

Port	Protocol	Status	Service
41800	tcp	open	

Ports and Services for IP: 192.168.1.170

Port	Protocol	Status	Service
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service
445	tcp	open	Microsoft-DS

Ports and Services for IP: 192.168.1.234

No Ports or Services could be identified for this IP.

Version Banner Identified

The following Service Version Banner outputs were readable on the target systems. It is highly recommended to reconfigure these banners with bogus or no information at all.

Service Version Banners for IP: 192.168.1.1

Banner name	BIND/NAMED Version Banner
Port	53/udp
Details	TelecomItaliaDNS
Solution	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "" . If you have already made it return bogus information please ignore this check.

Service Version Banners for IP: 192.168.1.6

Banner name	Smtplib Version Banner
Port	25/tcp
Details	220 penetrator.nfrpiero.com ESMTP protector
Solution	<p>It is highly advisable to configure this output to return bogus or no information at all.</p> <p>UNIX: Sendmail 1:Open up the sendmail.cf file 2:Find the line saying O SmtplibGreetingMessage= PARAMETERS (Where the parameters can be several \$ codes) 3:Change the line to O SmtplibGreetingMessage=\$j (And nothing more).</p> <p>WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level.</p> <p>If you have already removed the version please ignore this warning.</p>

Banner name	Smtplib Version Banner
Port	587/tcp
Details	220 penetrator.nfrpiero.com ESMTP protector
Solution	<p>It is highly advisable to configure this output to return bogus or no information at all.</p> <p>UNIX: Sendmail 1:Open up the sendmail.cf file 2:Find the line saying O SmtplibGreetingMessage= PARAMETERS (Where the parameters can be several \$ codes) 3:Change the line to O SmtplibGreetingMessage=\$j (And nothing more).</p> <p>WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level.</p> <p>If you have already removed the version please ignore this warning.</p>

Banner name	HTTPS Version Banner
Port	3790/tcp
Details	nginx
Solution	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning.

Service Version Banners for IP: 192.168.1.139

None

Service Version Banners for IP: 192.168.1.170

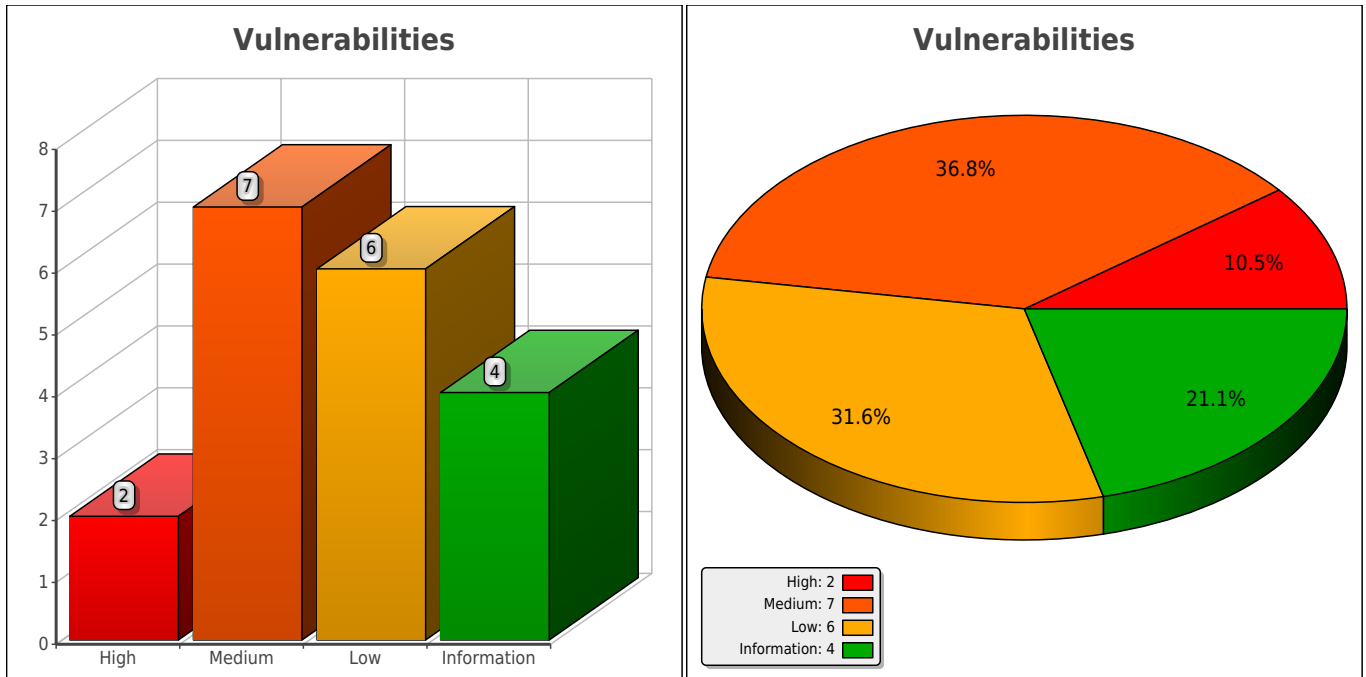
None

Service Version Banners for IP: 192.168.1.234

None

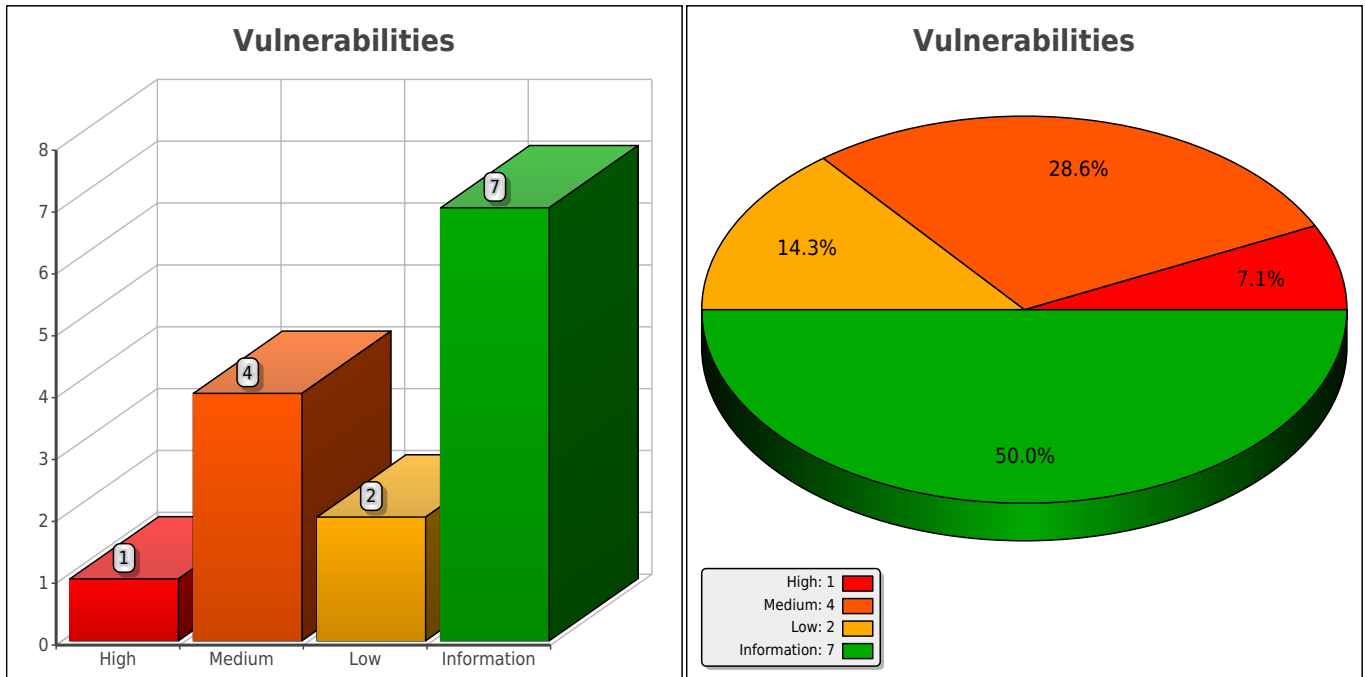
Summary of Vulnerabilities

IP: 192.168.1.1



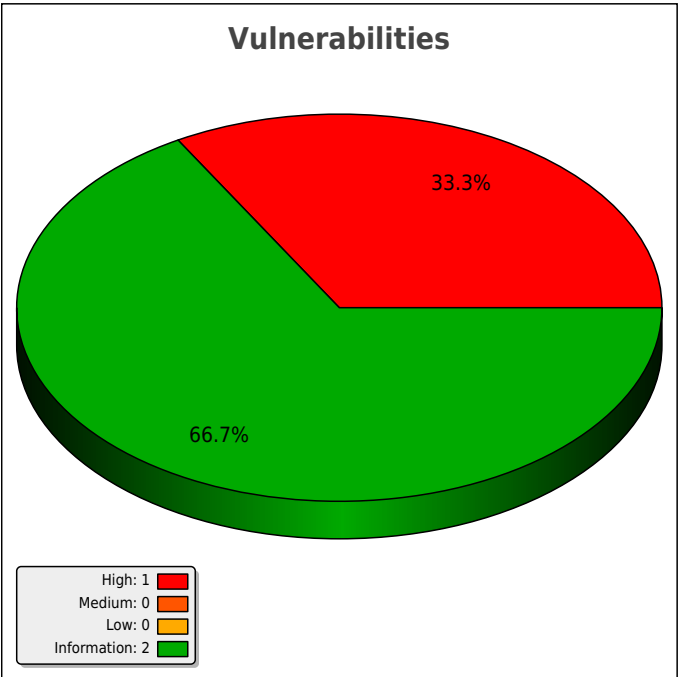
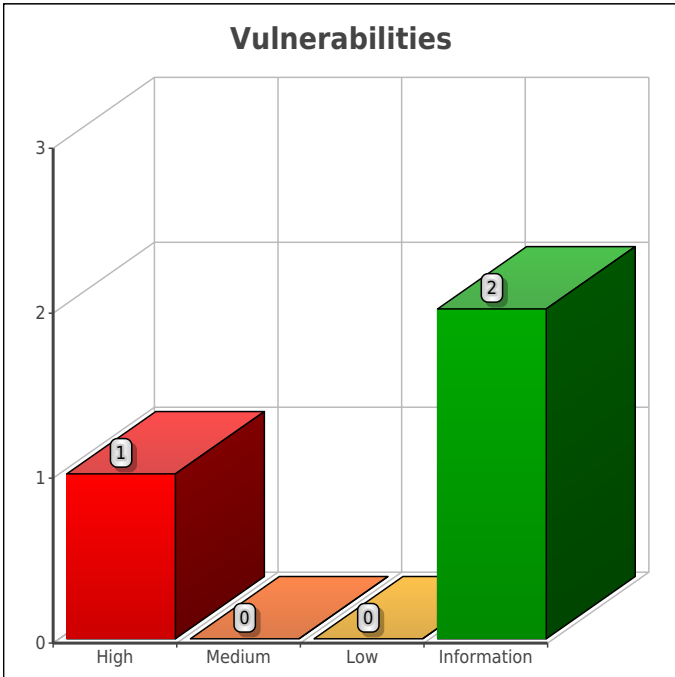
Risk Level	Vulnerability
High	Target SSL Web Server has SSLv2 Vulnerability
High	Telnet Service Default Password
Medium	SSL Web Server has SSLv3 Enabled Poodle Vulnerability
Medium	Shoutcast Long Backslash Admin.cgi Vulnerability
Medium	Target OpenSSL Man in Middle CCS Vulnerability
Medium	Telnet Service
Medium	NetBIOS User Name Retrieval #1
Medium	Web Server: Cross Site Scripting
Medium	DNS Recursion Allowed
Low	NetBIOS service listening 139 TCP
Low	NetBIOS service listening 445 UDP
Low	List of Netbios service lists installed
Low	It is possible to obtain remote NetBIOS name table.
Low	MAC address obtained via NetBIOS
Low	Apple Mac Identified on the remote System
Information	System Time Revealed via. ICMP TimeStamp
Information	System time via remote Web Server
Information	All Protocols Tested
Information	SSL Certificate information

IP: 192.168.1.6



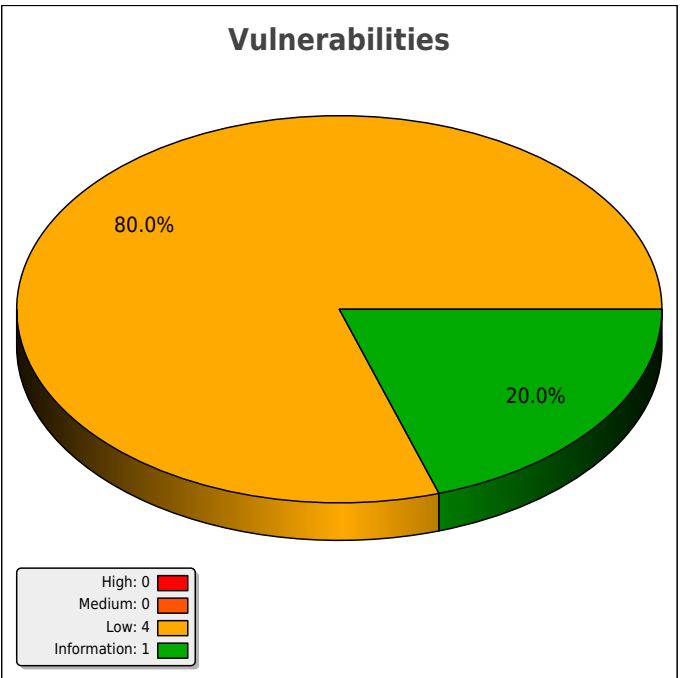
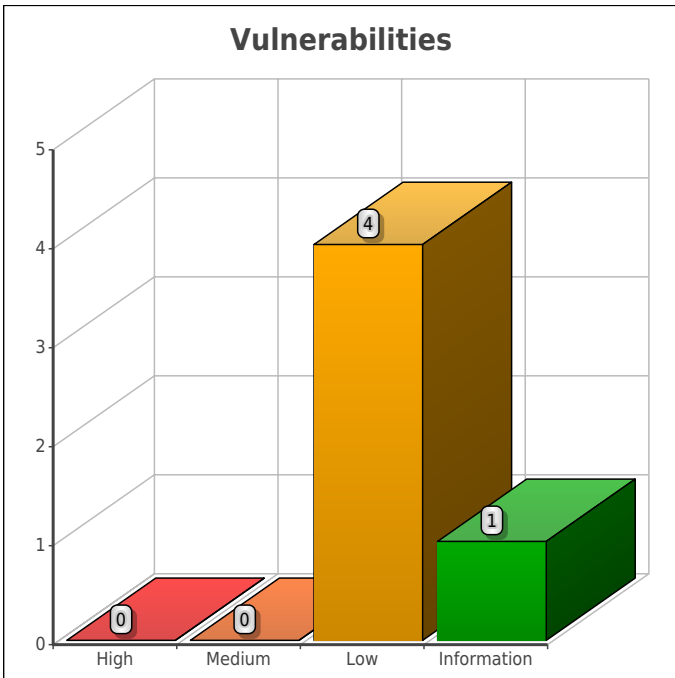
Risk Level	Vulnerability
High	PostgreSQL Service vulnerability
Medium	SSL Web Server has SSLv3 Enabled Poodle Vulnerability
Medium	Target OpenSSL Man in Middle CCS Vulnerability
Medium	web server /test/ directory world readable
Medium	X11 Server / Microsoft Windows RPC over HTTP
Low	RCPT TO: SMTP Service Username Guessing
Low	Ident service has been identified Check #2
Information	SMTP Ehlo Command
Information	SSL Certificate information
Information	System Time Revealed via. ICMP TimeStamp
Information	PHP Identified
Information	Identified directory /login/ Identified
Information	World read able access to /robots.txt
Information	All Protocols Tested

IP: 192.168.1.139



Risk Level	Vulnerability
■	Libgtop_service vulnerability
■	System Time Revealed via. ICMP TimeStamp
■	All Protocols Tested

IP: 192.168.1.170



Risk Level	Vulnerability
	NetBIOS service listening 445 UDP
	NetBIOS service listening 139 TCP
	MAC address obtained via NetBIOS
	It is possible to obtain remote NetBIOS name table.
	All Protocols Tested


IP: 192.168.1.234





Risk Level	Vulnerability
	System Time Revealed via. ICMP TimeStamp

Vulnerabilities

IP: 192.168.1.1

Vulnerability	Target SSL Web Server has SSLv2 Vulnerability
Risk Level	 High
Port	443/tcp
SecPoint ID	3647
BugtraqID	8746
Impact	The target web server system running with SSL (Secure Socket Layer) for https encrypted communication has the SSLv2 protocol enabled. The SSLv2 protocol is known to be vulnerable to several techniqs including man in the middle where it is possible for an attacker to break the encryption.
Solution	It is recommended that you set your web server software to only support SSLv3 and TLSv1. If using the mod_ssl adding the following lines in httpd.conf or ssl.conf will force the webservice to only use SSLv3 and TLSv1 SSLProtocol -all +SSLv3 +TLSv1 SSLCipherSuite: ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA+HIGH+MEDIUM
Vulnerability output / Evidences	
	-----BEGIN CERTIFICATE-----

Vulnerability	Telnet Service Default Password
Risk Level	 High
Port	23/tcp
SecPoint ID	1705
Impact	It is possible on the remote telnet device to log in with the default login "root" and default password "root". An attacker can log into the target and change the settings or log you out of the device.
Solution	Change the password on the telnet device from its configuration utility and or please block incoming TCP traffic to port 23.
Vulnerability output / Evidences	
	AttackString: pass
	AttackOutput: root
	Password:

Vulnerability	SSL Web Server has SSLv3 Enabled Poodle Vulnerability
Risk Level	 Medium
Port	443/tcp
SecPoint ID	6608
CVE	CVE-2014-3566
USN	2487-1
USN	2486-1
Impact	CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the POODLE issue. The target web server has the SSL v3 enabled.

Solution	It is recommended to disable SSLv3 by opening httpd.conf and adding: SSLProtocol All -SSLv2 -SSLv3
Vulnerability output / Evidences	
	Protocol : SSLv3

Vulnerability	Shoutcast Long Backslash Admin.cgi Vulnerability
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
Port	80/tcp
SecPoint ID	2308
BugtraqID	3934
Impact	The identified file /admin.cgi is subject to a Denial of Service when an overly long request is proceeded. This can crash the service.
Solution	Please make sure you are running the latest version of shoutcast from http://www.shoutcast.com/download/files.phtml If you are already running the latest version please ignore this check.
Vulnerability output / Evidences	
	<pre> AttackString: GET /admin.cgi HTTP/1.0 AttackOutput: HTTP/1.0 200 OK Content-Type: text/html Set-Cookie: rg_cookie_session_id=1163338342 path=/ Cache-Control: no-cache,no-store Pragma: no-cache Expires: Sun, 02 Oct 2016 11:48:09 GMT Date: Sun, 02 Oct 2016 11:48:09 GMT Accept-Ranges: bytes Connection: close <!-- Page(9154)=[Alice - Info] ---><HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html charset=UTF-8"><link rel="StyleSheet" type="text/css" href="images/ta- belle.css"><script language="javascript" type="text/javascript" src="im- ages/script.js"></script><TITLE>Alice Gate VoIP - Alice - Info</TITLE></HEAD><- BODY onload=javascript: loaded() ><SCRIPT language="Javascript"><!-- top.document.title = document.title // --> </SCRIPT><DIV style="position:absolute left:30px top:5px width:670px height:690px z-index:1 overflow: auto "><FORM name="form_contents" method=POST action="admin.cgi" enctype="applica- tion/x-www-form-urlencoded" onSubmit="if (window.is_submit && is_submit==1) re- turn false is_submit=1 </pre>


```

return true
"><INPUT type=HIDDEN name="active_page" value="9154"><INPUT type=HIDDEN name="-
page_title" value="Alice - Info"><INPUT type=HIDDEN name="mimic_button_field"
value=""><INPUT type=HIDDEN name="button_value" value=""><INPUT type=HIDDEN
name="strip_page_top" value="0"><SCRIPT language="Javascript"><!--
top.location = index.html
var is_button_in_focus=false
var is_textarea_in_focus=false
var is_submit=0
var is_loaded=0
function loaded()
var inp
is_loaded=1
function mimic_button(button_name,use_default_cgi)
if (is_submit)
return
f=document.form_contents
f.mimic_button_field.value = button_name
is_submit=1
setTimeout("is_submit=0", 1000)
if (use_default_cgi)
{
if (f.encoding)
f.encoding = "application/x-www-form-urlencoded"
else
f.enctype = "application/x-www-form-urlencoded"
f.action = "admin.cgi"
}
f.submit()
function set_cgi(action,encoding)
f=document.form_contents
if (f.encoding)
f.encoding=encoding
else
f.enctype=encoding
f.action

```

Vulnerability	Target OpenSSL Man in Middle CCS Vulnerability
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
Port	443/tcp
SecPoint ID	57021
CVE	CVE-2014-0224
USN	2232-1

Impact	Due to a vulnerability in the TLS and DTLS implementation in OpenSSL 1.0.1 and before 1.0.1g in the way of handling of extension packets. OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability. This can allow remote attackers to obtain sensitive information from the memory and base other attacks on.
Solution	It is recommended to update your operating system to the latest packages or upgrade to the latest openssl from http://www.openssl.org/
Vulnerability output / Evidences	
	[TLsv1] 192.168.1.1:443 allows early CCS [SSLv3] 192.168.1.1:443 allows early CCS

Vulnerability	Telnet Service
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
Port	23/tcp
SecPoint ID	29
CVE	CVE-1999-0619
Impact	The telnet service has been found on TCP port 23. This service is used for remote administration. Telnet sends all usernames, passwords and data unencrypted.
Solution	UNIX: Disable the Telnet service by uncommenting the telnet line in /etc/inetd.conf on UNIX systems. WINDOWS: Systems enter Control-Panel->Administrative Tools->Services and put the telnet service on Disable. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Vulnerability output / Evidences	
	Please note in this check we only relied on the presence of the found port.

Vulnerability	NetBIOS User Name Retrieval #1
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
SecPoint ID	1772
Impact	It is possible to query NetBIOS Windows file sharing services running on The identified TCP port to gain a list of and other NetBIOS information. Determined attackers can use this information to launch effective brute-force attacks against shared resources.
Solution	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via the identified TCP port. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Vulnerability output / Evidences	

AttackOutput: admin
AgC7nf1g3xpd4t4s

Vulnerability	Web Server: Cross Site Scripting
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
SecPoint ID	5244
Impact	The identified file found in the VULNOUTPUT section are subject to a remote Cross Site Scripting vulnerability. This can allow an attacker to steal cookie based authentication credentials from the target system. The service is also running on 80/tcp.
Solution	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it.
Vulnerability output / Evidences	
Possible Cross Site Scripting: (http://192.168.1.1/admin.cgi?button%5fvalue=`/bin/echo+w00t`&strip%5fpage%5ftop=0&mimic%5fbutton%5ffieldd=1&req%5fmode=0&active%5fpage=9103)	

Vulnerability	DNS Recursion Allowed
Risk Level	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Medium
SecPoint ID	56963
Impact	The target DNS service is subject to a remote DNS Recursion vulnerability. Attackers can exploit this in DDoS Attacks. Recursion is used to process a DNS request where the DNS server performs the request for the client. Recursion should only be allowed for trusted clients. RECOMMENEDED SOLUTION: Set permissions so only trusted clients can do recursion requests or disable recursion. On Unix* You can edit /etc/bind/named.conf. allow-transfer {"none";}; allow-recursion {"none";}; recursion no; On Windows please see: http://technet.microsoft.com/en-us/library/cc771738.aspx
Vulnerability output / Evidences	
yahoo.com mail is handled by 1 mta7.am0.yahoodns.net.	

Vulnerability	NetBIOS service listening 139 TCP
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	139/tcp
SecPoint ID	1990
Impact	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Solution	<p>WINDOWS:</p> <p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.</p>
Vulnerability output / Evidences	
Please note in this check we only relied on the presence of the found port.	

Vulnerability	NetBIOS service listening 445 UDP
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	445/tcp
SecPoint ID	1990
Impact	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Solution	<p>WINDOWS:</p> <p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto:</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.</p>
Vulnerability output / Evidences	
Please note in this check we only relied on the presence of the found port.	

Vulnerability	List of Netbios service lists installed
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	2616
Impact	It is possible on the remote system via the NetBIOS service to retrieve a list of installed servicelist patches on the system. An attacker can use this information to base other attacks on.
Solution	It is recommended to block incoming traffic to the NetBIOS service running on the UDP ports 135,136,137,139,445 TCP ports 135,136,137,139,445
Vulnerability output / Evidences	
<pre> servicelist List: Server: \\192.168.1.1: User: Domain: Connection: OK Services ----- Spooler: Print Spooler NETLOGON: Net Logon RemoteRegistry: Remote Registry Service WINS: Windows Internet Name Service (WINS) Exit Status: SUCCESS </pre>	

Vulnerability	It is possible to obtain remote NetBIOS name table.
---------------	---

Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	1770
Impact	Attackers can use this information to base other attacks on.
Solution	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Vulnerability output / Evidences	
	<pre>Name Service Type ----- ALICEGATE Workstation Service ALICEGATE Messenger Service ALICEGATE File Server Service ALICEGATE Workstation Service ALICEGATE Messenger Service ALICEGATE File Server Service []_MSBROWSE_[] Master Browser WORKGROUP Browser Service Elections WORKGROUP Domain Name WORKGROUP Browser Service Elections WORKGROUP Master Browser</pre>

Vulnerability	MAC address obtained via NetBIOS
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	1771
Impact	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.
Solution	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Vulnerability output / Evidences	
	MAC Address: 00-00-00-00-00-00

Vulnerability	Apple Mac Identified on the remote System
----------------------	--

Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	3234
Impact	It is possible to identified the remote system via the NetBIOS services. An attacker can use this information to base other attacks on.
Solution	It is recommended to block incoming traffic to the NetBIOS service running on the UDP ports 135,136,137,139,445 TCP ports 135,136,137,139,445
Vulnerability output / Evidences	
	CurrentVersion: REG_SZ: 4.9

Vulnerability	System Time Revealed via. ICMP TimeStamp
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
SecPoint ID	1746
CVE	CVE-1999-0524
Impact	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 12:32:42. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Solution	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.


Vulnerability	System time via remote Web Server
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	80/tcp
SecPoint ID	1745
Impact	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Solution	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.

Vulnerability output / Evidences	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Sun, 02 Oct 2016 11:32:48 GMT

Vulnerability	All Protocols Tested
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
SecPoint ID	8311
Impact	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Solution	If there is found known services on unknown ports it is recommended to properly test those ports.
Vulnerability output / Evidences	
	Protocol on 192.168.1.1:23/tcp matches telnet-t-rex-proxy
	Protocol on 192.168.1.1:23/tcp matches oracle-tns-listener
	Protocol on 192.168.1.1:80/tcp matches http
	Protocol on 192.168.1.1:80/tcp matches http-net.commerce
	Protocol on 192.168.1.1:80/tcp matches http-proxy


Vulnerability	SSL Certificate information
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	443/tcp
SecPoint ID	3702
Impact	It is possible to retrieve the SSL certificate owner information from the target web server running. In this check please review the vulnerability information provided from the ssl certificate.
Solution	If all the information in the certificate output is the correct information and matches what it is supposed to please ignore this check.
Vulnerability output / Evidences	
	subject=/C=IT/ST=ITALY/L=ROMA/O=TELECOM ITALIA SPA/OU=IT TELECOM/CN=homenet.telecomitalia.it/emailAddress=or.ap3@telecomitalia.it
	issuer=/C=IT/O=I.T. Telecom/OU=Servizi di certificazione/CN=I.T. Telecom Private CA


IP: 192.168.1.6

Vulnerability PostgreSQL Service vulnerability	
Risk Level	 High
Port	5432/tcp
SecPoint ID	3609
BugtraqID	6610
BugtraqID	6611
BugtraqID	6612
BugtraqID	6613
BugtraqID	6614
BugtraqID	5527
BugtraqID	5497
BugtraqID	6615
BugtraqID	10470
CVE	CVE-2004-0547
CVE	CVE-2002-1402
CVE	CVE-2002-1401
CVE	CVE-2002-1400
CVE	CVE-2002-1397
CVE	CVE-2012-0866
CVE	CVE-2012-0867
CVE	CVE-2012-0868
CVE	CVE-2012-2143
CVE	CVE-2012-2655
USN	1378-1
USN	1481-1
USN	1461-1
Impact	The identified port found running is known to house the PostgreSQL service. The PostgreSQL is known to run with a default password and if it is possible for an attacker to gain access the service the attacker can obtain shell access on the remote system.
Solution	It is recommended to block all incoming traffic to the identified port. And or please upgrade to the latest version of this software from http://www.postgresql.org and there click on Download. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Vulnerability output / Evidences	
	Please note in this check we only relied on the presence of the found port.

Vulnerability SSL Web Server has SSLv3 Enabled Poodle Vulnerability	
Risk Level	 Medium
Port	3790/tcp

SecPoint ID	6608
CVE	CVE-2014-3566
USN	2487-1
USN	2486-1
Impact	CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the POODLE issue. The target web server has the SSL v3 enabled.
Solution	It is recommended to disable SSLv3 by opening httpd.conf and adding: SSLProtocol All -SSLv2 -SSLv3
Vulnerability output / Evidences	
	Protocol : SSLv3

Vulnerability	Target OpenSSL Man in Middle CCS Vulnerability
Risk Level	 Medium
Port	3790/tcp
SecPoint ID	57021
CVE	CVE-2014-0224
USN	2232-1
Impact	Due to a vulnerability in the TLS and DTLS implementation in OpenSSL 1.0.1 and before 1.0.1g in the way of handling of extension packets. OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability. This can allow remote attackers to obtain sensitive information from the memory and base other attacks on.
Solution	It is recommended to update your operating system to the latest packages or upgrade to the latest openssl from http://www.openssl.org/
Vulnerability output / Evidences	
	[TLSv1] 192.168.1.6:3790 allows early CCS [SSLv3] 192.168.1.6:3790 allows early CCS

Vulnerability	web server /test/ directory world readable
Risk Level	 Medium
Port	80/tcp
SecPoint ID	6038
Impact	The identified directory on the remote web server. This directory can contain valuable information that an attacker can use for further attacks.
Solution	Please set the permissions on the web server software you are running block incoming access to the identified directory. WINDOWS: On a windows system 1: Start ->Control-Panel ->Administrative Tools 2:Enter IIS Admin tool 3:Find the found directory 4: Change permissions so that guest user do not have access to it. UNIX: On Unix system enter the found directory CWD /directory chmod 700 . chmod 755 *

Vulnerability output / Evidences

AttackString: GET /test/ HTTP/1.0
AttackOutput: HTTP/1.1 200 OK
Cache-Control: max-age=86400
Expires: Mon, 03 Oct 2016 11:41:53 GMT
Connection: close
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
<HEAD>
<TITLE>Index of /test</TITLE>
</HEAD>
<BODY>
<H1>Index of /test</H1>
<PRE> Name Last modified Size Description
<HR>
 Parent Directory 20-Sep-2016 18:58 -
 Drag-Portlets.html 26-Mar-2014 21:30 8k
 Drag-Portlets_files/ 27-Mar-2014 19:35 -
 GeoLiteCity_20130305/ 18-Apr-2013 19:20 -
 aircrackload.php 13-Mar-2013 21:53 1k
 butta.php 22-Jan-2014 19:52 1k
 drag/ 27-Mar-2014 19:42 -
 dragbox.htm 18-Apr-2014 11:47 4k
 dragbox_files/ 18-Apr-2014 14:11 -
 dump.csv 13-Mar-2013 15:18 1k
 emule.php 12-Oct-2013 15:52 41k
 emule1.php 12-Oct-2013 18:16 5k
 esempio1.html 23-Mar-2014 15:57 5k
<IMG SRC="/icons/unknown.gif"

Vulnerability X11 Server / Microsoft Windows RPC over HTTP

Risk Level  Medium

Port	6001/tcp
SecPoint ID	2106
Impact	The identified port running is known to contain the X11 windows-system service running. When an attacker has access to this port the attacker can "sniff" keystrokes from the session running or do more specific attacks.
Solution	It is highly recommended to block incoming access to the identified port by applying filters at firewall level. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Vulnerability output / Evidences	
	Please note in this check we only relied on the presence of the found port.

Vulnerability	RCPT TO: SMTP Service Username Guessing
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	25/tcp
SecPoint ID	1766
Impact	It is possible on the remote mail server software SMTP to guess user-names. This is accomplished by sending a RCPT TO: user-name and my this the software replied if the user existed. The service is also running on 587/tcp.
Solution	Please upgrade to the latest version of your mail server software.
Vulnerability output / Evidences	
	AttackString: RCPT TO: nonex1sting
	AttackOutput: 250 2.1.0 nonex1sting@hotmail.com... Sender ok
	550 5.1.1 nonex1sting... User unknown

Vulnerability	Ident service has been identified Check #2
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	113/tcp
SecPoint ID	1688
CVE	CVE-1999-0629
Impact	The Ident service has been identified on the identified TCP port. This service provide sensitive information to an intruder. It will give such info as which accounts, services are running on the target. This information can be used by the attacker to focus on the vulnerable services.
Solution	Disable the service. UNIX: Comment out the Ident line in /etc/inetd.conf WINDOWS: Please goto Control-Panel->Administrative Tools->Services-> and there you can disable the service.
Vulnerability output / Evidences	
	AttackString: 0,0
	AttackOutput: 0 , 0 : ERROR : INVALID-PORT

Vulnerability	SMTP Ehlo Command
----------------------	--------------------------

Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	25/tcp
SecPoint ID	1765
CVE	CVE-1999-0531
Impact	It is possible on the target SMTP mail server software to retrieve information by using the EHLO command instead of the normal HELO. Attackers can use this information to perform more specific attacks. The service is also running on 587/tcp.
Solution	<p>Disable the EHLO command on your mail service software if allowed.</p> <p>WINDOWS:</p> <p>Microsoft(R) Exchange</p> <p>1:Open up regedit.exe</p> <p>2:Goto following registry key HKEY_LOCAL_MACHINE\SystemCurrentControlSet\Services\MSExchange\IMCParameters</p> <p>3:In regedit Choose Edit and then choose New DWORD Value.</p> <p>4:Add the type AdvertiseSMTPExtensions under Value data type 0 for more information please see http://www.microsoft.com/Exchange/</p> <p>UNIX:</p> <p>Please upgrade to the latest version of your mail service software running. The latest sendmail can be obtained from http://www.sendmail.org and there click on mail server.</p>
Vulnerability output / Evidences	
	<pre> AttackString: EHLO hotmail.com AttackOutput: 220 penetrator.nfrpiero.com ESMTP protector 250-penetrator.nfrpiero.com Hello penetrator.nfrpiero.com [192.168.1.6], pleased to meet you 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-8BITMIME 250-SIZE 250-DSN 250-ETRN 250-AUTH DIGEST-MD5 CRAM-MD5 LOGIN PLAIN 250-DELIVERBY 250 HELP </pre>

Vulnerability	SSL Certificate information
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	443/tcp
SecPoint ID	3702
Impact	It is possible to retrieve the SSL certificate owner information from the target web server running. In this check please review the vulnerability information provided from the ssl certificate. The service is also running on 3790/tcp.
Solution	If all the information in the certificate output is the correct information and matches what it is supposed to please ignore this check.
Vulnerability output / Evidences	
	<pre> subject=/C=DK/ST=DK/L=Copenhagen K/0=SecPoint/OU=SecPoint/CN=SecPoint/emailAd- dress=support@secpoint.com issuer=/C=DK/ST=DK/L=Copenhagen K/0=SecPoint/OU=SecPoint/CN=SecPoint/emailAd- dress=support@secpoint.com </pre>

Vulnerability System Time Revealed via. ICMP TimeStamp	
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
SecPoint ID	1746
CVE	CVE-1999-0524
Impact	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 12:33:17. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Solution	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.

Vulnerability PHP Identified	
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	443/tcp
SecPoint ID	500
Impact	It is possible via the banner from the web server software to detect some presence of PHP. PHP has a known history of several security vulnerabilities. Attackers can use this information to do PHP specified attacks. The service is also running on 80/tcp.
Solution	To reconfigure the PHP version banner edit /php-4.0/main/php_version.h and in /php-4.0/sapi/apache/mod_php4.c and look for PHP/ and remove that. Now recompile PHP. Immediately upgrade to the latest version of php from http://www.php.net
Vulnerability output / Evidences	
Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0	
AttackOutput: HTTP/1.1 301 Moved Permanently	
Cache-Control: max-age=86400	
Expires: Mon, 03 Oct 2016 11:39:50 GMT	
Location: https:///login.php	
Connection: close	
Content-Type: text/html	

Vulnerability Identified directory /login/ Identified	
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	80/tcp
SecPoint ID	56003
Impact	The identified directory has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.


Solution	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Vulnerability output / Evidences	
	AttackString: GET /login/ HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Cache-Control: no-cache, must-revalidate
	Expires: Mon, 26 Jul 1997 05:00:00 GMT
	Last-Modified: Sun, 02 Oct 2016 11:41:52 GMT
	Pragma: no-cache
	location: https:///login/
	Connection: close
	Content-Type: text/html


Vulnerability	World read able access to /robots.txt
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
Port	80/tcp
SecPoint ID	1464
Impact	The found file /robots.txt is a file used for web search engines to get a list of directories on the target web server system. This file can disclosure directories not ment to be known to the public. If this file is not disclosing any important information please ignore this check.
Solution	Please modify the robots.txt so that it is not disclosureing any sensitive information.
Vulnerability output / Evidences	
	AttackString: GET /robots.txt HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	Cache-Control: max-age=604800
	Expires: Sun, 09 Oct 2016 11:43:10 GMT
	Last-Modified: Wed, 07 Sep 2016 17:20:26 GMT
	ETag: "2013cb-1b-57d04c5a"
	Accept-Ranges: bytes
	Content-Length: 27
	Connection: close
	Content-Type: text/plain
	User-agent: *
	Disallow: /


Vulnerability	All Protocols Tested
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
SecPoint ID	8311
Impact	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Solution	If there is found known services on unknown ports it is recommended to properly test those ports.
Vulnerability output / Evidences	
	Protocol on 192.168.1.6:25/tcp matches smtp
	Protocol on 192.168.1.6:80/tcp matches http

Protocol on 192.168.1.6:80/tcp matches http-apache-2
Protocol on 192.168.1.6:113/tcp matches auth
Protocol on 192.168.1.6:443/tcp matches http
Protocol on 192.168.1.6:443/tcp matches http-apache-2
Protocol on 192.168.1.6:443/tcp matches ntp
Protocol on 192.168.1.6:443/tcp matches ssl
Protocol on 192.168.1.6:587/tcp matches smtp
Protocol on 192.168.1.6:3790/tcp matches http
Protocol on 192.168.1.6:3790/tcp matches ntp
Protocol on 192.168.1.6:3790/tcp matches ssl
Protocol on 192.168.1.6:5432/tcp matches mysql
Protocol on 192.168.1.6:6001/tcp matches x-windows

IP: 192.168.1.139

Vulnerability	Libgtop_service vulnerability
Risk Level	 High
Port	41800/tcp
SecPoint ID	2135
BugtraqID	3586
BugtraqID	3594
Impact	The libgtop service service that has been found is known to contain a format string vulnerability where it is possible for a remote attacker to gain shell access with the privileges of the nobody user.
Solution	Either block incoming traffic to the identified port and or please upgrade to the latest version of this software from http://www.home-of-linux.org/ NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Vulnerability output / Evidences	
Please note in this check we only relied on the presence of the found port.	

Vulnerability	System Time Revealed via. ICMP TimeStamp
Risk Level	 Information
SecPoint ID	1746
CVE	CVE-1999-0524
Impact	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 12:28:23. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Solution	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.

Vulnerability	All Protocols Tested
Risk Level	 Information
SecPoint ID	8311
Impact	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Solution	If there is found known services on unknown ports it is recommended to properly test those ports.
Vulnerability output / Evidences	
Protocol on 192.168.1.139:41800/tcp matches http	

IP: 192.168.1.170

Vulnerability	NetBIOS service listening 445 UDP
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	445/tcp
SecPoint ID	1990
Impact	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Solution	<p>WINDOWS:</p> <p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto:</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.</p>
Vulnerability output / Evidences	
	Please note in this check we only relied on the presence of the found port.

Vulnerability	NetBIOS service listening 139 TCP
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
Port	139/tcp
SecPoint ID	1990
Impact	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.

Solution	<p>WINDOWS:</p> <p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.</p>
Vulnerability output / Evidences	
	Please note in this check we only relied on the presence of the found port.

Vulnerability	MAC address obtained via NetBIOS
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	1771
Impact	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.
Solution	<p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.</p>
Vulnerability output / Evidences	
	MAC Address: 00-26-c7-df-37-a0


Vulnerability	It is possible to obtain remote NetBIOS name table.
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Low
SecPoint ID	1770
Impact	Attackers can use this information to base other attacks on.
Solution	<p>Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -</p> <p>Click through Start-> Settings-> Network and Dial-up Connection</p> <p>Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.</p>

Vulnerability output / Evidences	
	Name Service Type

	ALESSANDRO-VAIO Workstation Service
	WORKGROUP Domain Name
	ALESSANDRO-VAIO File Server Service
	WORKGROUP Browser Service Elections

Vulnerability	All Protocols Tested
Risk Level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Information
SecPoint ID	8311
Impact	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Solution	If there is found known services on unknown ports it is recommended to properly test those ports.
Vulnerability output / Evidences	
	Protocol on 192.168.1.170:135/tcp matches netbios-session
	Protocol on 192.168.1.170:139/tcp matches netbios-session
	Protocol on 192.168.1.170:445/tcp matches ms-ds

IP: 192.168.1.234

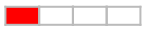
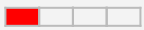

















Vulnerability	System Time Revealed via. ICMP TimeStamp
Risk Level	 Information
SecPoint ID	1746
CVE	CVE-1999-0524
Impact	<p>By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 12:27:26. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.</p>
Solution	<p>At network-level this traffic should be rejected both inbound and outbound.</p> <p>UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly.</p> <p>WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.</p>

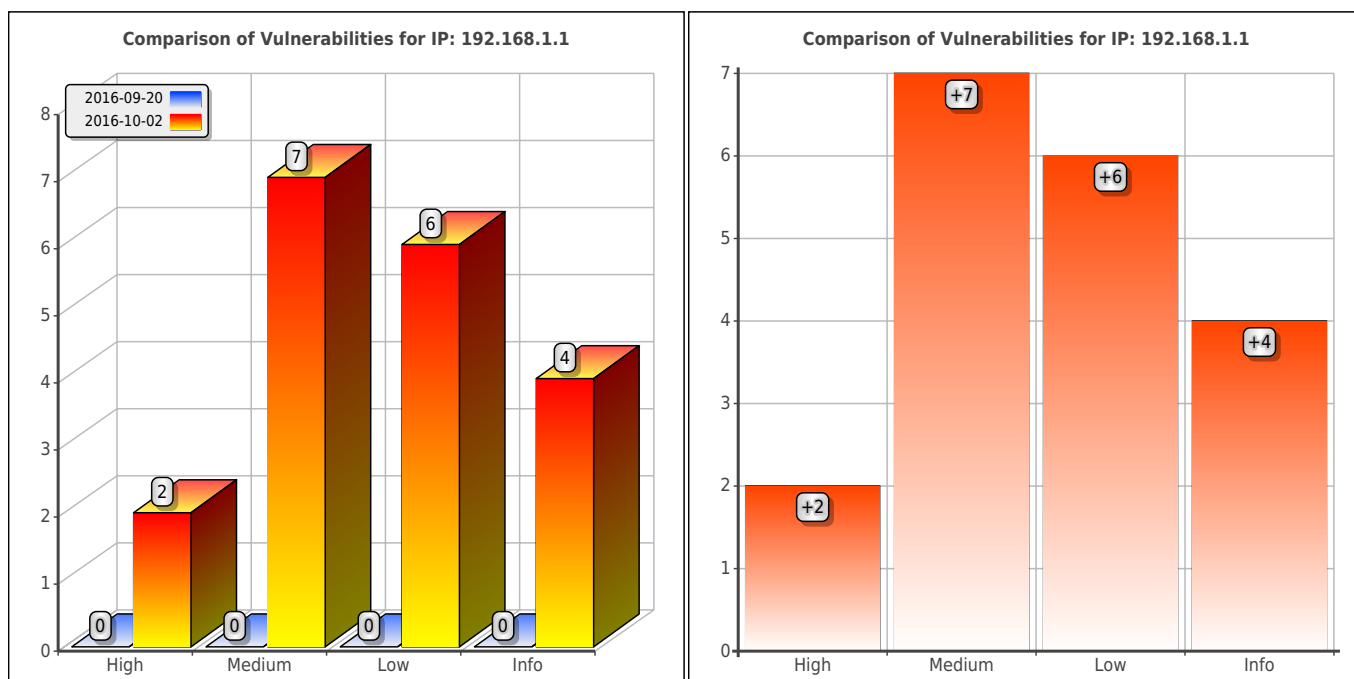
Gap analysis

IP: 192.168.1.1

This is the analysis of the difference between the current scan and the previous one performed on the same IP address, on 2016-09-20 18:54:56

The following new vulnerabilities have been detected:

Risk Level	Vulnerability	SecPoint ID
	Target SSL Web Server has SSLv2 Vulnerability	3647
	Telnet Service Default Password	1705
	DNS Recursion Allowed	56963
	NetBIOS User Name Retrieval #1	1772
	Web Server: Cross Site Scripting	5244
	Shoutcast Long Backslash Admin.cgi Vulnerability	2308
	SSL Web Server has SSLv3 Enabled Poodle Vulnerability	6608
	Target OpenSSL Man in Middle CCS Vulnerability	57021
	Telnet Service	29
	It is possible to obtain remote NetBIOS name table.	1770
	MAC address obtained via NetBIOS	1771
	Apple Mac Identified on the remote System	3234
	List of Netbios service lists installed	2616
	NetBIOS service listening 139 TCP	1990
	NetBIOS service listening 445 UDP	1990
	All Protocols Tested	8311
	System Time Revealed via. ICMP TimeStamp	1746
	System time via remote Web Server	1745
	SSL Certificate information	3702

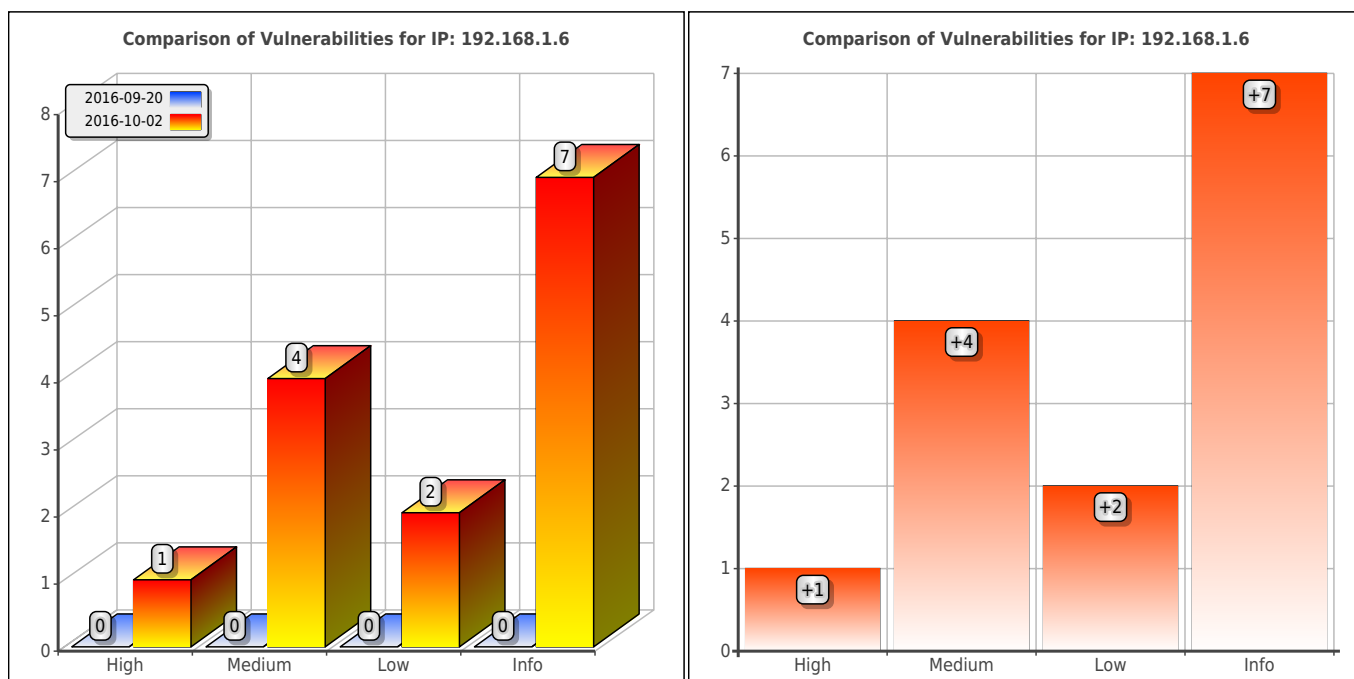


IP: 192.168.1.6

This is the analysis of the difference between the current scan and the previous one performed on the same IP address, on 2016-09-20 18:54:56

The following new vulnerabilities have been detected:

Risk Level	Vulnerability	SecPoint ID
■ ■ ■ ■	PostgreSQL Service vulnerability	3609
■ ■ ■	web server /test/ directory world readable	6038
■ ■ ■	SSL Web Server has SSLv3 Enabled Poodle Vulnerability	6608
■ ■ ■	Target OpenSSL Man in Middle CCS Vulnerability	57021
■ ■ ■	Open SMTP Mail Relay Vulnerability #2	1751
■ ■ ■	X11 Server / Microsoft Windows RPC over HTTP	2106
■ ■	RCPT TO: SMTP Service Username Guessing	1766
■ ■	Ident service has been identified Check #2	1688
■	All Protocols Tested	8311
■	System Time Revealed via. ICMP TimeStamp	1746
■	PHP Identified	500
■	Identified directory /login/ Identified	56003
■	World read able access to /robots.txt	1464
■	SSL Certificate information	3702
■	SMTP Ehlo Command	1765

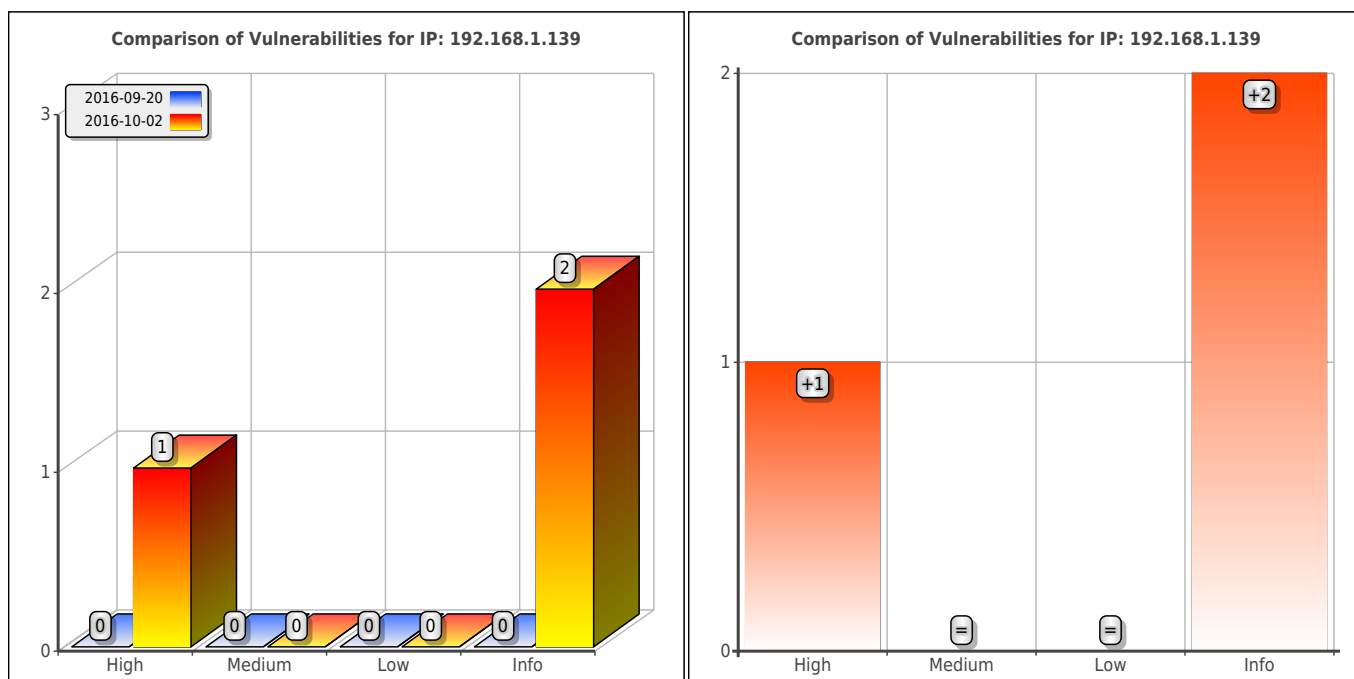


IP: 192.168.1.139

This is the analysis of the difference between the current scan and the previous one performed on the same IP address, on 2016-09-20 18:54:46

The following new vulnerabilities have been detected:

Risk Level	Vulnerability	SecPoint ID
█ 	Libgtop_service vulnerability	2135
 	All Protocols Tested	8311
 	System Time Revealed via. ICMP TimeStamp	1746

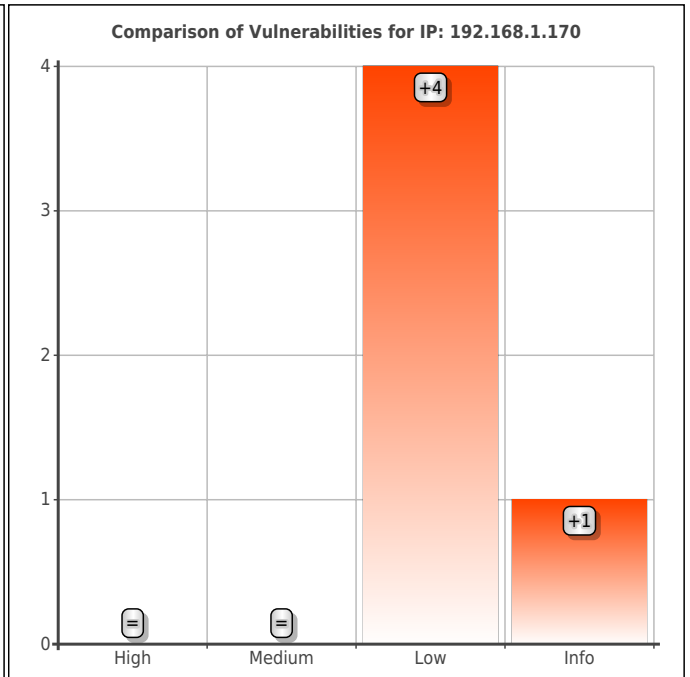
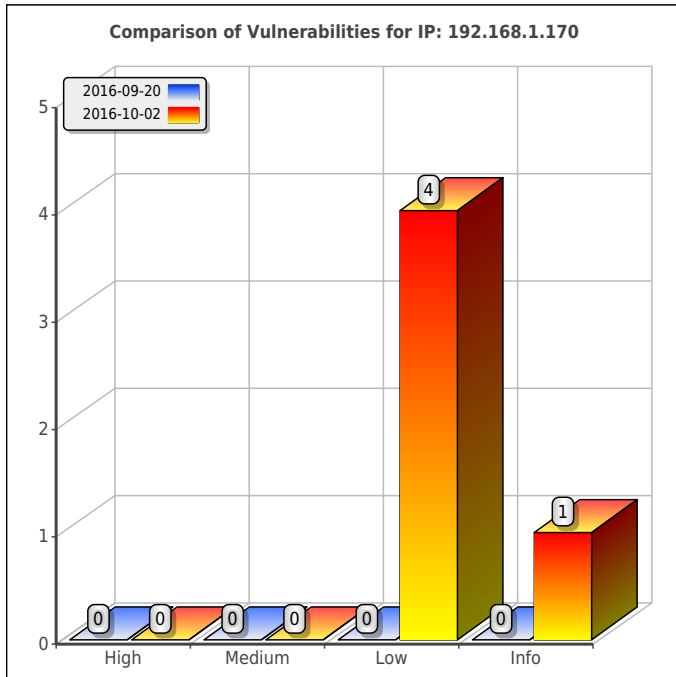


IP: 192.168.1.170

This is the analysis of the difference between the current scan and the previous one performed on the same IP address, on 2016-09-20 18:54:43

The following new vulnerabilities have been detected:

Risk Level	Vulnerability	SecPoint ID
	It is possible to obtain remote NetBIOS name table.	1770
	MAC address obtained via NetBIOS	1771
	NetBIOS service listening 139 TCP	1990
	NetBIOS service listening 445 UDP	1990
	All Protocols Tested	8311

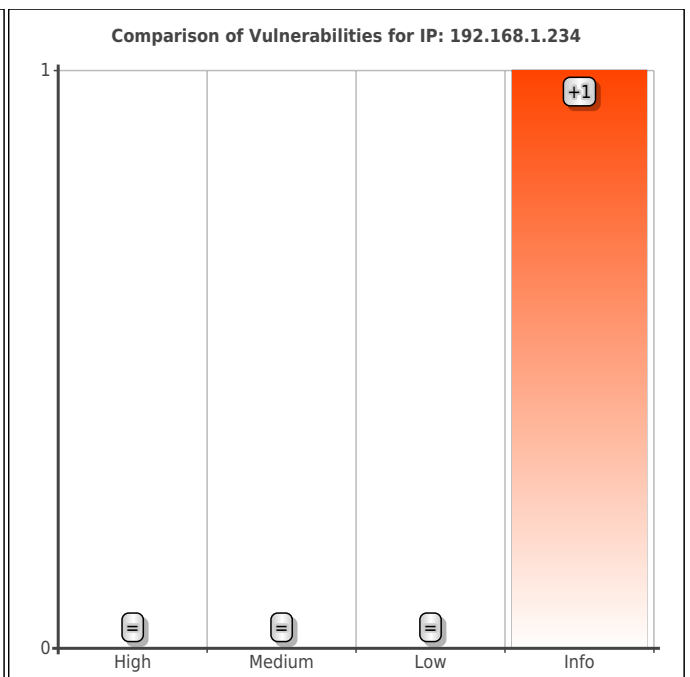
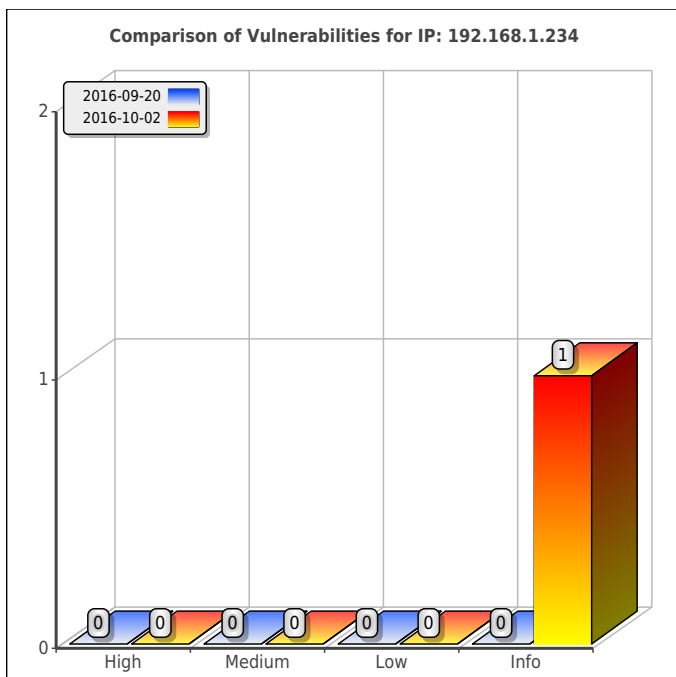


IP: 192.168.1.234

This is the analysis of the difference between the current scan and the previous one performed on the same IP address, on 2016-09-20 18:54:59

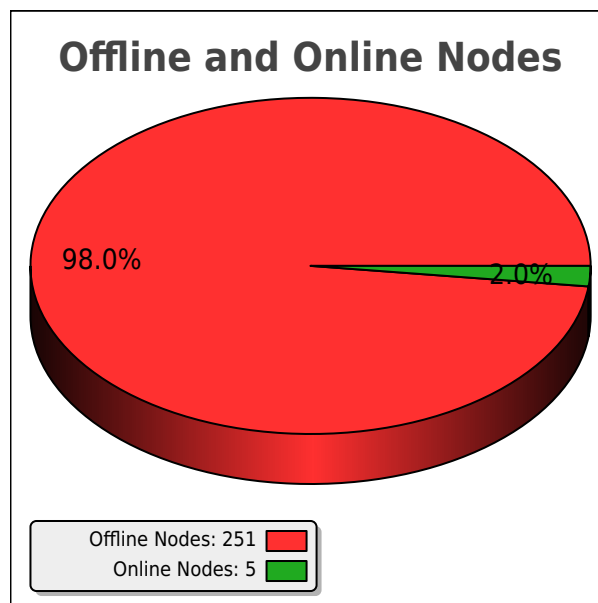
The following new vulnerabilities have been detected:

Risk Level	Vulnerability	SecPoint ID
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	System Time Revealed via. ICMP TimeStamp	1746



Offline Nodes

Scan Name	credential
Scan Profile	Best Scan
Started at	2016-10-02 13:23:33
Ended at	2016-10-02 14:28:23



The scan of the following IPs has been cancelled because the nodes seem down at time of scan.

A total number of 251 nodes were offline at time of scan.

IP	IP	IP	IP
192.168.1.0	192.168.1.2	192.168.1.3	192.168.1.4
192.168.1.5	192.168.1.7	192.168.1.8	192.168.1.9
192.168.1.10	192.168.1.11	192.168.1.12	192.168.1.13
192.168.1.14	192.168.1.15	192.168.1.16	192.168.1.17
192.168.1.18	192.168.1.19	192.168.1.20	192.168.1.21
192.168.1.22	192.168.1.23	192.168.1.24	192.168.1.25
192.168.1.26	192.168.1.27	192.168.1.28	192.168.1.29
192.168.1.30	192.168.1.31	192.168.1.32	192.168.1.33
192.168.1.34	192.168.1.35	192.168.1.36	192.168.1.37
192.168.1.38	192.168.1.39	192.168.1.40	192.168.1.41
192.168.1.42	192.168.1.43	192.168.1.44	192.168.1.45
192.168.1.46	192.168.1.47	192.168.1.48	192.168.1.49
192.168.1.50	192.168.1.51	192.168.1.52	192.168.1.53
192.168.1.54	192.168.1.55	192.168.1.56	192.168.1.57
192.168.1.58	192.168.1.59	192.168.1.60	192.168.1.61
192.168.1.62	192.168.1.63	192.168.1.64	192.168.1.65
192.168.1.66	192.168.1.67	192.168.1.68	192.168.1.69
192.168.1.70	192.168.1.71	192.168.1.72	192.168.1.73
192.168.1.74	192.168.1.75	192.168.1.76	192.168.1.77
192.168.1.78	192.168.1.79	192.168.1.80	192.168.1.81
192.168.1.82	192.168.1.83	192.168.1.84	192.168.1.85

IP	IP	IP	IP
192.168.1.86	192.168.1.87	192.168.1.88	192.168.1.89
192.168.1.90	192.168.1.91	192.168.1.92	192.168.1.93
192.168.1.94	192.168.1.95	192.168.1.96	192.168.1.97
192.168.1.98	192.168.1.99	192.168.1.100	192.168.1.101
192.168.1.102	192.168.1.103	192.168.1.104	192.168.1.105
192.168.1.106	192.168.1.107	192.168.1.108	192.168.1.109
192.168.1.110	192.168.1.111	192.168.1.112	192.168.1.113
192.168.1.114	192.168.1.115	192.168.1.116	192.168.1.117
192.168.1.118	192.168.1.119	192.168.1.120	192.168.1.121
192.168.1.122	192.168.1.123	192.168.1.124	192.168.1.125
192.168.1.126	192.168.1.127	192.168.1.128	192.168.1.129
192.168.1.130	192.168.1.131	192.168.1.132	192.168.1.133
192.168.1.134	192.168.1.135	192.168.1.136	192.168.1.137
192.168.1.138	192.168.1.140	192.168.1.141	192.168.1.142
192.168.1.143	192.168.1.144	192.168.1.145	192.168.1.146
192.168.1.147	192.168.1.148	192.168.1.149	192.168.1.150
192.168.1.151	192.168.1.152	192.168.1.153	192.168.1.154
192.168.1.155	192.168.1.156	192.168.1.157	192.168.1.158
192.168.1.159	192.168.1.160	192.168.1.161	192.168.1.162
192.168.1.163	192.168.1.164	192.168.1.165	192.168.1.166
192.168.1.167	192.168.1.168	192.168.1.169	192.168.1.171
192.168.1.172	192.168.1.173	192.168.1.174	192.168.1.175
192.168.1.176	192.168.1.177	192.168.1.178	192.168.1.179
192.168.1.180	192.168.1.181	192.168.1.182	192.168.1.183
192.168.1.184	192.168.1.185	192.168.1.186	192.168.1.187
192.168.1.188	192.168.1.189	192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193	192.168.1.194	192.168.1.195
192.168.1.196	192.168.1.197	192.168.1.198	192.168.1.199
192.168.1.200	192.168.1.201	192.168.1.202	192.168.1.203
192.168.1.204	192.168.1.205	192.168.1.206	192.168.1.207
192.168.1.208	192.168.1.209	192.168.1.210	192.168.1.211
192.168.1.212	192.168.1.213	192.168.1.214	192.168.1.215
192.168.1.216	192.168.1.217	192.168.1.218	192.168.1.219
192.168.1.220	192.168.1.221	192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225	192.168.1.226	192.168.1.227
192.168.1.228	192.168.1.229	192.168.1.230	192.168.1.231
192.168.1.232	192.168.1.233	192.168.1.235	192.168.1.236
192.168.1.237	192.168.1.238	192.168.1.239	192.168.1.240
192.168.1.241	192.168.1.242	192.168.1.243	192.168.1.244
192.168.1.245	192.168.1.246	192.168.1.247	192.168.1.248
192.168.1.249	192.168.1.250	192.168.1.251	192.168.1.252
192.168.1.253	192.168.1.254	192.168.1.255	