Full VAPT Scan Report

Scan Name: Firewall

Audited on 2026-06-29 18:14:05

Confidential

Table of Contents

Introduction 3
Severity Levels 4
Scan Profile Information 5
Executive Summary 6
Traceroute 8
Operating Systems 9
Identified Ports and Services 10
Version Banner Identified 11
Summary of Vulnerabilities 12
Vulnerabilities 14
Target: 192.168.10.1 14

Introduction

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

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 categorized 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 risk 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 **CVSS score(*)**, a **CVE(**)** and/or a **USN(***)** are present, for further details.

Every system vulnerability discovered is supplied with a possible remedy.

(*) CVSS is the NIST (National Institute of Standards and Technology) severity scoring system.
(**) 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.

Scan Profile Information

Best Scan - Popular Ports

This scan targets the most commonly used network ports to quickly identify potential vulnerabilities in widely used services and protocols.

Scans **8000** among the **most common ports**.
Web application vulnerability scanner WAS
Automatic Service Identification
SQL Injection
XSS Cross Site Scripting
Command Execution
Web Crawler
Google Hack DB
Joomla Security Scan
Google Safe Browsing
50+ Blacklist Checks
Wordpress Security Scan
Firewall, DNS, FTP, Web, SSL, SSH, SQL, Netbios and much more.
Scans Windows, Mac OS X, Linux, Nix and other operating systems.
Lethal Attack Crawler - SQL Injection, Blind SQL Injection, XSS, XSS Attack String Reflection, RCE, Remote File Inclusion, Directory Traversal.
Duration can be several hours depending on how many services are found during the scan.
It is designed to be **non harmful and not flood the services** by simulating the human behavior.
Performs Penetration Testing-level checks using automated, safe technique.
APT Group Fingerprinting Module added for enhanced threat detection.

Executive Summary

This report represents a security scan performed by **admin**. 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	Firewall	**Scan Profile**	Best Scan
Started at	2026-06-29 18:14:05		
Scan Engine	9.9.33.2934	**Firmware Version**	68.0.3
Audited Targets	192.168.10.1		

Overall Risk Level

High (Critical Level)

The scan performed by **admin** 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 Targets

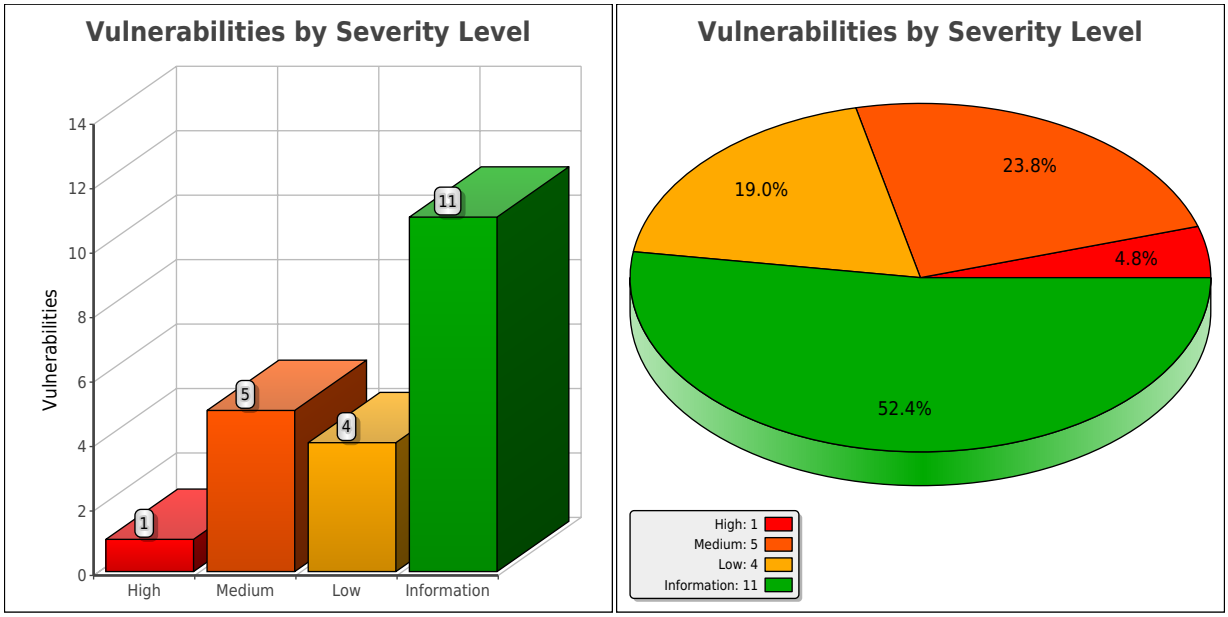
All the targets were online at the time of scan.

Offline Targets

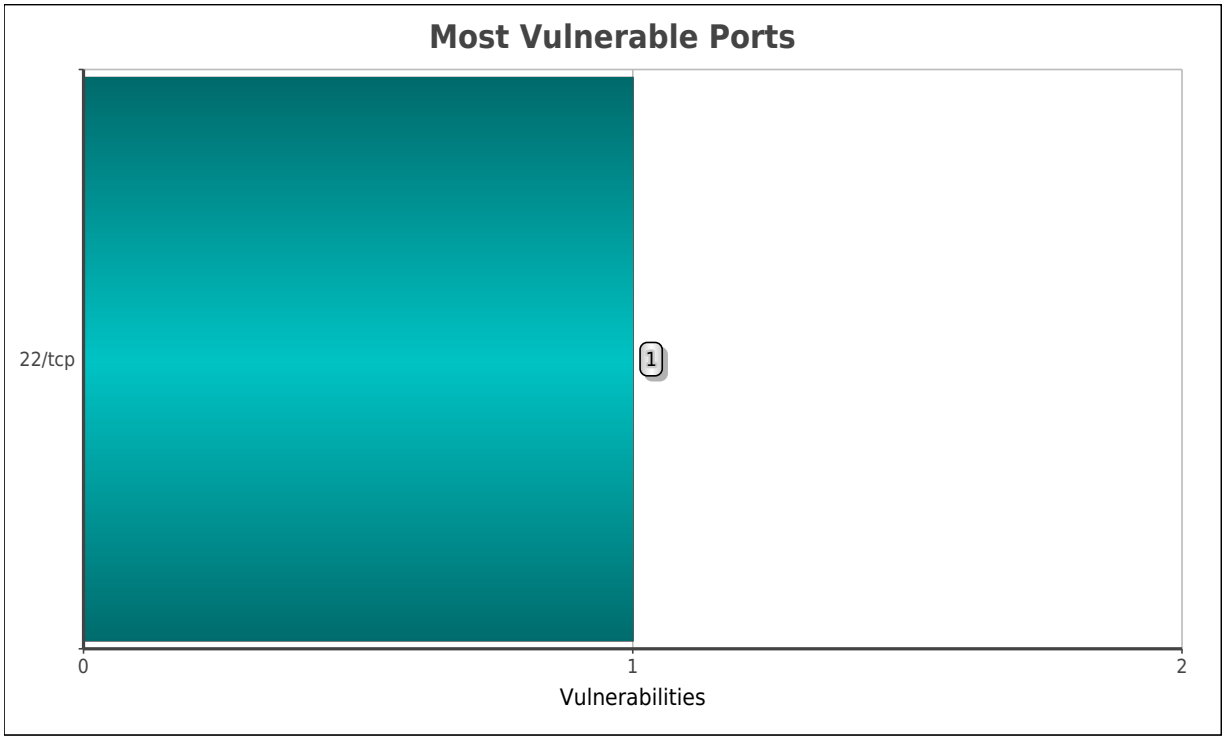
The scan has not detected any offline target.

Analysis of Results

A total number of **21** potential vulnerabilities were identified on the target systems, with a ratio of **4.8%** of high level vulnerabilities.



Overall number of Vulnerabilities



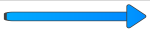
List of the most Vulnerable ports, based on the number of Vulnerabilities found on that port

Traceroute

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

A packet filtering device was found protecting the target system typically a firewall system or a router system with ACL (Access Control Lists) set. Even though a filtering device has been found it can still be mis configured and leaving the system vulnerable.

traceroute to 192.168.10.1 (192.168.10.1), 15 hops max, 60 byte packets

Hop	Name	IP	Location	Avg(ms)	Graph
1	192.168.10.1	192.168.10.1		0.414	

Operating Systems

The following Operating Systems were identified:

Target: 192.168.10.1

Fortinet Firewall

Identified Ports and Services

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

Ports and Services for Target: 192.168.10.1

Port	Protocol	Status	Service
22	tcp	open	The Secure Shell (SSH) Protocol
443	tcp	open	http protocol over TLS/SSL

Version Banner Identified

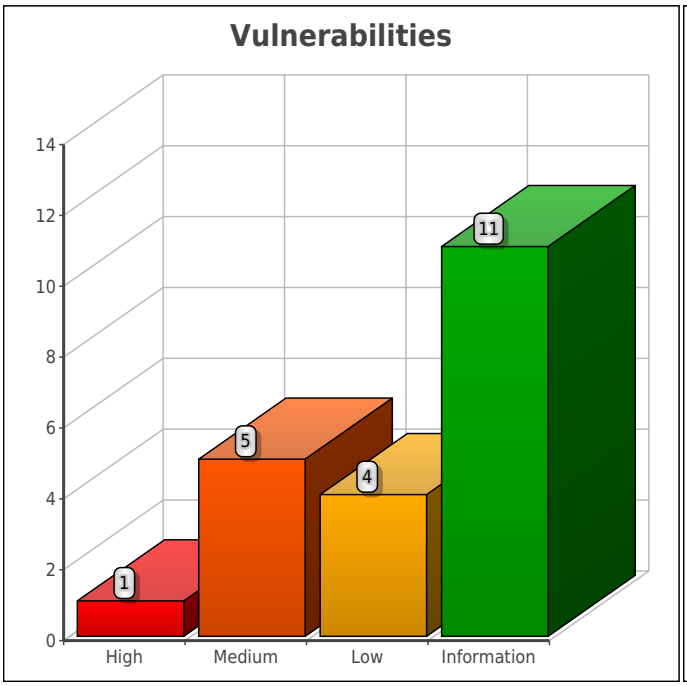
The following Service Version Banner outputs were readable on the target systems.
It is highly recommended to reconfigure these banners with bogus or no information at all.

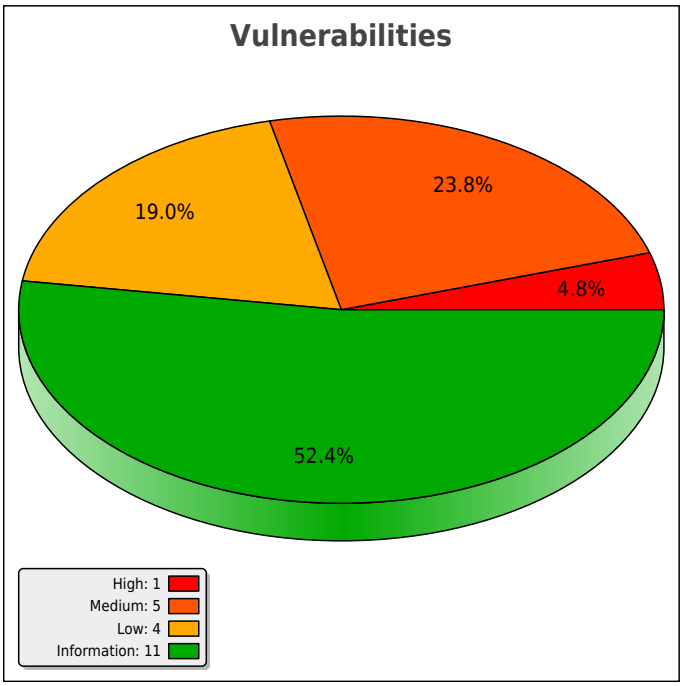
Service Version Banners for Target: 192.168.10.1

Banner name	SSHd Version Banner
Port	22
Details	SSH-2.0-D6kWA
Mitigation	To safeguard your system against attackers who might use information about your operating system and service versions to launch further attacks, it is highly recommended to configure your service version output to return false or no information. If you have already implemented this security measure, please disregard this warning.

Summary of Vulnerabilities

Target: 192.168.10.1





Risk Level	Vulnerability
	SSH Service Accessible
	File /logout Information Disclosure Vulnerability
	Missing Web Security Header Tag Permissions-Policy SSL
	SSL Certificate Cannot Be Trusted (Missing Extended Key Usage) on 192.168.10.1:443
	TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_256_CBC_SHA256
	SSL Certificate - Invalid Maximum Validity Date on 192.168.10.1:443
	Self-Signed Certificate on 192.168.10.1:443
	TLS CBC Cipher Suite Accepted - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS CBC Cipher Suite Accepted - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	All Protocols Tested on the Target System
	Direct HTTP 26586 & HTTPS 218209 Connections
	Exposure through PING Response
	HTTP2 Protocol Identified Port 443
	Identified Operating System Check #2 Fortinet Firewall
	MAC Address 18-66-da-2a-57-93 Dell Inc.
	Operating System Identification via Packet Analysis Linux 2.2.x-3.x Check #3
	SSL Client Information
	System SSL Certificate information
	System Time Exposure through ICMP Timestamp Requests

Risk Level	Vulnerability
	System Time Revealed ICMP TimeStamp

Vulnerabilities

Target: 192.168.10.1

Vulnerability	SSH Service Accessible
Risk Level	High
Port	22/tcp
SecPoint ID	2733
Impact	The SSH (Secure Shell) service, as currently configured, permits unrestricted access to any user trying to connect, which is a significant security risk. This open access increases the likelihood of brute force attacks, where attackers try various username and password combinations to gain unauthorized entry. Considering SSHs essential role in system management, such a breach could severely compromise both system integrity and data confidentiality. Additionally, the SSH service has a history of documented vulnerabilities, including some severe ones that could be exploited if not regularly updated. This history adds an additional risk layer, as attackers might use known vulnerabilities against systems that are not updated. This could also enable attackers to deduce the operating system in use, forming the basis for further attacks.
Mitigation	To mitigate this vulnerability, a two-pronged approach is recommended: Firewall Configuration: Implement strict firewall rules that restrict SSH access to only a set of predefined IP addresses or IP ranges. This measure will significantly reduce the attack surface by ensuring that only machines from trusted networks can attempt to connect to the SSH service. User Access Control: Modify the SSH configuration to limit access to a specific list of trusted users. Implementing robust user authentication methods, such as key-based authentication and two-factor authentication, can further strengthen security. Service Management: If the SSH service is not essential for daily operations, consider disabling it entirely. This approach follows the principle of least functionality, reducing potential entry points for attackers. However, if the service is necessary, ensure that it is regularly updated to patch any known vulnerabilities and employ strong password policies to guard against brute force attacks. These measures, when combined, provide a comprehensive approach to securing the SSH service against unauthorized access and exploitation. Regular monitoring and auditing of SSH access logs are also advised to detect and respond to any anomalous activities promptly.
Vulnerability Output / Evidences	
	`AttackOutput: SSH-2.0-D6kWA`

Vulnerability	File /logout Information Disclosure Vulnerability
Risk Level	Medium
Port	443/tcp
SecPoint ID	68292
Impact	A file on the remote web server has been identified as vulnerable to information disclosure. Unauthorized access to this file could provide attackers with critical data, forming the basis for further attacks. If attackers obtain confidential information, such as passwords, database details, or other sensitive data, they could exploit it for malicious activities like identity theft, fraud, corporate espionage, or to launch additional attacks.
Mitigation	To mitigate this vulnerability, please consider the following actions: Upgrade to the most recent version of the software associated with the identified file. If the file contains sensitive data, ensure that it is inaccessible to unauthorized users. Before deleting any files, always ensure you have a reliable backup in place. If the check consistently identifies the file, and you have determined that it is not a risk, you can ignore this check. Or if the file is sensitive make it unavailable.
Vulnerability Output / Evidences	
	AttackString: cgi100ssl2 HTTPS GET /logout HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	X-Frame-Options: SAMEORIGIN
	Content-Security-Policy: frame-ancestors self
	Strict-Transport-Security: max-age=63072000
	date: Mon, 29 Jun 2026 13:04:46 GMT
	content-length: 64
	content-type: text/html
	Connection: close
	<script language="javascript">
	top.location="/login"
	</script>

Vulnerability	Missing Web Security Header Tag Permissions-Policy SSL
Risk Level	Medium
Port	443/tcp
SecPoint ID	58860
Impact	The 'Permissions-Policy' header is a critical security measure in safeguarding websites against Cross-Site Scripting (XSS) attacks. By specifying a whitelist of approved content sources, it helps prevent browsers from loading potentially malicious content. This security header empowers web security administrators to precisely control which resources a user agent is permitted to load on a webpage, offering a robust defense against XSS attacks.
Mitigation	To fortify your website's security, it is advised to implement the following 'Permissions-Policy' header: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)") This configuration will restrict access to sensitive features on your site unless specifically allowed, thereby significantly enhancing your sites security posture.
Vulnerability Output / Evidences	

Vulnerability	SSL Certificate Cannot Be Trusted (Missing Extended Key Usage) on 192.168.10.1:443
Risk Level	Medium
Port	443/tcp
SecPoint ID	131441
CVE	CVE-2020-1971
USN	4662-1
Impact	Certificate is missing the Extended Key Usage (EKU) field, which can allow misuse in contexts it wasn't intended for, such as authentication or encryption.
Mitigation	Re-issue the certificate with a proper EKU extension (e.g., serverAuth).
Vulnerability Output / Evidences	
	`Extended Key Usage extension is missing`

Vulnerability	TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_128_CBC_SHA256
Risk Level	Medium
Port	443/tcp
SecPoint ID	134376
Impact	The server accepts a TLS 1.2 cipher suite that combines CBC-mode encryption with static RSA key exchange. CBC-mode cipher suites are legacy and are discouraged by modern TLS hardening guidance. Static RSA key exchange does not provide Perfect Forward Secrecy, meaning previously captured traffic could be at greater risk if the server private key is compromised later. This is a valid TLS hardening finding, but it should not be described as BEAST unless TLS 1.0 CBC negotiation is also confirmed by the separate BEAST check.
Mitigation	Disable TLS_RSA_* cipher suites. Prefer TLS 1.3 and modern TLS 1.2 ECDHE AEAD cipher suites such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
Vulnerability Output / Evidences	
	`Server 192.168.10.1:443 accepted TLS 1.2 cipher TLS_RSA_WITH_AES_128_CBC_SHA256`
	`OpenSSL cipher AES128-SHA256`
	`negotiated protocol TLSv1.2`
	`negotiated cipher AES128-SHA256`

Vulnerability	SSL Certificate - Invalid Maximum Validity Date on 192.168.10.1:443
Risk Level	Low
Port	443/tcp
SecPoint ID	132143
Impact	Certificate exceeds industry-standard maximum validity of 398 days, potentially reducing trust and revocation effectiveness.:It's a compliance issue introduced by the CA/Browser Forum, enforced by major browsers and systems (since Sept 2020)
Mitigation	Re-issue certificate with validity under 398 days to comply with best practices.
Vulnerability Output / Evidences	
	`Validity period is 11567 days (Sep 24 09:37:48 2024 GMT to May 26 20:48:33 2056 GMT)`

Vulnerability	Self-Signed Certificate on 192.168.10.1:443
Risk Level	Low
Port	443/tcp
SecPoint ID	56214
CVE	CVE-2004-2761
CVSS	CVE-2004-2761 - CVSS Score V2: **5**
USN	740-1
Impact	Identity of the service cannot be verified Self-signed certificates pose a risk because they lack third-party validation, allowing attackers to impersonate services and performman-in-the-middle attacks.
Mitigation	Replace with cert from trusted CA
Vulnerability Output / Evidences	
	`Subject CN=FG121GTK24007744` `Issuer CN=fortinet-subca2001`

Vulnerability	TLS CBC Cipher Suite Accepted - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Risk Level	Low
Port	443/tcp
SecPoint ID	134376
Impact	The server accepts a TLS 1.2 CBC-mode cipher suite. CBC-mode cipher suites are legacy and are discouraged by modern TLS hardening guidance because AEAD cipher suites such as AES-GCM or ChaCha20-Poly1305 provide stronger and simpler protection. This cipher uses ephemeral ECDHE or DHE key exchange and is intended to provide Perfect Forward Secrecy when negotiated with adequate parameters. This finding should normally be treated as a TLS hardening finding unless a specific exploitable CBC condition is also confirmed. BEAST is reported separately only when TLS 1.0 CBC negotiation is confirmed.
Mitigation	Prefer TLS 1.3 and modern TLS 1.2 AEAD cipher suites using ECDHE, such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. Disable CBC-mode TLS 1.2 cipher suites where compatibility requirements allow it.
Vulnerability Output / Evidences	
	`Server 192.168.10.1:443 accepted TLS 1.2 cipher TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
	`OpenSSL cipher ECDHE-RSA-AES128-SHA256`
	`negotiated protocol TLSv1.2`
	`negotiated cipher ECDHE-RSA-AES128-SHA256`

	All Protocols Tested on the Target System
Risk Level	Information
SecPoint ID	8311
Impact	This check examines all ports to verify their actual protocols. If everything matches as expected, please disregard this check.
Mitigation	If known services are discovered on unexpected ports, it is recommended to thoroughly test these ports.
Vulnerability Output / Evidences	
	`Protocol on 192.168.10.1:22/tcp matches ssh`
	`Protocol on 192.168.10.1:443/tcp matches ssl`

	Direct HTTP 26586 & HTTPS 218209 Connections
Risk Level	Information
SecPoint ID	6175
Impact	The Vulnerability Scanner, employing a variety of techniques during scan assessments, lists all Direct HTTP and HTTPS Connections. This list excludes connections from crawlers and external tools, focusing solely on direct interactions. This detailed enumeration is crucial for users to verify that the Vulnerability Scanner is performing all intended checks comprehensively. It also assists in identifying any potential obstructions, such as firewall interference or session shunning, which might hinder the scanners effectiveness. By providing a clear view of the direct connections made, users can ensure that their security systems are not inadvertently blocking crucial vulnerability assessment processes, thereby maintaining the integrity and thoroughness of the security audit.
Mitigation	If the number of connections is notably lower than expected, it is advisable to first investigate any potential firewall configurations that might be obstructing the scanners access. This includes verifying firewall rules and checking for any IP-based restrictions that might be in place. If, upon review, the connection count appears normal and there are no indications of firewall interference, this particular check can be considered a false alarm and safely ignored. However, it is important to regularly review these connection logs to ensure ongoing accuracy and security effectiveness, as changes in network configuration or security policies might alter the scanners access and effectiveness.

	Exposure through PING Response
Risk Level	Information
SecPoint ID	2853
Impact	The remote system is currently configured to respond to PING commands. The PING command is a diagnostic utility primarily used to check the availability of a networked device. If a system responds to this command, it signifies its presence on the network. This seemingly benign response can be exploited by attackers, as it gives them an initial indication that the system is active. With this information, malicious actors can further probe for vulnerabilities or include the system in a broader network scan. It is a starting point that potentially facilitates subsequent, more sophisticated attacks.
Mitigation	To enhance the systems security posture, it is advised to configure the firewall to prevent the system from responding to PING queries. By cloaking the system from such basic network reconnaissance, novice attackers might presume there is no active system associated with the IP address and subsequently move on to another target. Specifically, you should block incoming ICMP type 13 messages and block outgoing ICMP type 14 messages.
Vulnerability Output / Evidences	
	`64 octets from 192.168.10.1: icmp_seq=0 ttl=255 time=0.6 ms`