# Nessus Report

## Nessus Scan Report

Thu, 07 Dec 2017 19:12:53 EET

# Table Of Contents

# Hosts Summary (Executive)

## 192.168.10.1

### Summary

| Critical | High | Medium | Low | Info | Total | |
|---|---|---|---|---|---|---|
| 0 | 0 | 3 | 0 | 33 | 36 | |

### Details

| Severity | Plugin Id | Name |
|---|---|---|
| Medium (6.4) | 51192 | SSL Certificate Cannot Be Trusted |
| Medium (6.4) | 57582 | SSL Self-Signed Certificate |
| Medium (5.0) | 97861 | Network Time Protocol (NTP) Mode 6 Scanner |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| Info | 10287 | Traceroute Information |
| Info | 10386 | Web Server No 404 Error Code Check |
| Info | 10662 | Web mirroring |
| Info | 10863 | SSL Certificate Information |
| Info | 10884 | Network Time Protocol (NTP) Server Detection |
| Info | 11002 | DNS Server Detection |
| Info | 11032 | Web Server Directory Enumeration |
| Info | 11219 | Nessus SYN scanner |
| Info | 11935 | IPSEC Internet Key Exchange (IKE) Version 1 Detection |
| Info | 11936 | OS Identification |
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 21643 | SSL Cipher Suites Supported |
| Info | 22964 | Service Detection |
| Info | 24260 | HyperText Transfer Protocol (HTTP) Information |
| Info | 25220 | TCP/IP Timestamps Supported |
| Info | 35716 | Ethernet Card Manufacturer Detection |
| Info | 42057 | Web Server Allows Password Auto-Completion |
| Info | 42822 | Strict Transport Security (STS) Detection |
| Info | 45590 | Common Platform Enumeration (CPE) |
| Info | 49704 | External URLs |

| Info | 50344 | Missing or Permissive Content-Security-Policy HTTP Response Header |
|------|-------|-------------------------------------------------------------------|
| Info | 54615 | Device Type |
| Info | 56984 | SSL / TLS Versions Supported |
| Info | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| Info | 62564 | TLS Next Protocols Supported |
| Info | 62695 | IPSEC Internet Key Exchange (IKE) Version 2 Detection |
| Info | 70544 | SSL Cipher Block Chaining Cipher Suites Supported |
| Info | 87242 | TLS NPN Supported Protocol Enumeration |
| Info | 91634 | HyperText Transfer Protocol (HTTP) Redirect Information |
| Info | 91815 | Web Application Sitemap |

## 192.168.10.10

### Summary

| Critical | High | Medium | Low | Info | Total |
|----------|------|--------|-----|------|-------|
| 3 | 0 | 2 | 0 | 31 | 36 |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Critical (10.0) | 53514 | MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check) |
| Critical (10.0) | 72836 | MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check) |
| Critical (10.0) | 97833 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) |
| Medium (6.8) | 90510 | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| Medium (5.0) | 72837 | MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check) |
| Info | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| Info | 10287 | Traceroute Information |
| Info | 10394 | Microsoft Windows SMB Log In Possible |
| Info | 10736 | DCE Services Enumeration |
| Info | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| Info | 10884 | Network Time Protocol (NTP) Server Detection |
| Info | 10919 | Open Port Re-check |
| Info | 11002 | DNS Server Detection |
| Info | 11011 | Microsoft Windows SMB Service Detection |
| Info | 11219 | Nessus SYN scanner |
| Info | 11936 | OS Identification |
| Info | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 20870 | LDAP Server Detection |
| Info | 21745 | Authentication Failure - Local Checks Not Run |
| Info | 22964 | Service Detection |

| Info | 24786 | Nessus Windows Scan Not Performed with Admin Privileges |
|------|-------|---------------------------------------------------------|
| Info | 25220 | TCP/IP Timestamps Supported |
| Info | 25701 | LDAP Crafted Search Request Server Information Disclosure |
| Info | 26917 | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry |
| Info | 35716 | Ethernet Card Manufacturer Detection |
| Info | 43829 | Kerberos Information Disclosure |
| Info | 45590 | Common Platform Enumeration (CPE) |
| Info | 53513 | Link-Local Multicast Name Resolution (LLMNR) Detection |
| Info | 54615 | Device Type |
| Info | 72779 | DNS Server Version Detection |
| Info | 72780 | Microsoft DNS Server Version Detection |
| Info | 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| Info | 100871 | Microsoft Windows SMB Versions Supported (remote check) |
| Info | 104410 | Host Authentication Failure(s) for Provided Credentials |

## 192.168.10.30

### Summary

| Critical | High | Medium | Low | Info | Total | |
|----------|------|--------|-----|------|-------|---|
| 0 | 0 | 0 | 0 | 3 | 3 | |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 35716 | Ethernet Card Manufacturer Detection |

## 192.168.10.51

### Summary

| Critical | High | Medium | Low | Info | Total |
|----------|------|--------|-----|------|-------|
| 0 | 0 | 1 | 0 | 20 | 21 |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Medium (5.0) | 88098 | Apache Server ETag Header Information Disclosure |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| Info | 10287 | Traceroute Information |
| Info | 11032 | Web Server Directory Enumeration |
| Info | 11219 | Nessus SYN scanner |
| Info | 11936 | OS Identification |
| Info | 18261 | Apache Banner Linux Distribution Disclosure |
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 22964 | Service Detection |
| Info | 24260 | HyperText Transfer Protocol (HTTP) Information |
| Info | 25220 | TCP/IP Timestamps Supported |
| Info | 35716 | Ethernet Card Manufacturer Detection |
| Info | 39521 | Backported Security Patch Detection (WWW) |
| Info | 43111 | HTTP Methods Allowed (per directory) |
| Info | 45590 | Common Platform Enumeration (CPE) |
| Info | 50344 | Missing or Permissive Content-Security-Policy HTTP Response Header |
| Info | 50345 | Missing or Permissive X-Frame-Options HTTP Response Header |
| Info | 54615 | Device Type |
| Info | 91815 | Web Application Sitemap |

## 192.168.10.52

### Summary

| Critical | High | Medium | Low | Info | Total |
|----------|------|--------|-----|------|-------|
| 0 | 0 | 1 | 0 | 20 | 21 |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Medium (5.0) | 88098 | Apache Server ETag Header Information Disclosure |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| Info | 10287 | Traceroute Information |
| Info | 11032 | Web Server Directory Enumeration |
| Info | 11219 | Nessus SYN scanner |
| Info | 11936 | OS Identification |
| Info | 18261 | Apache Banner Linux Distribution Disclosure |
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 22964 | Service Detection |
| Info | 24260 | HyperText Transfer Protocol (HTTP) Information |
| Info | 25220 | TCP/IP Timestamps Supported |
| Info | 35716 | Ethernet Card Manufacturer Detection |
| Info | 39521 | Backported Security Patch Detection (WWW) |
| Info | 43111 | HTTP Methods Allowed (per directory) |
| Info | 45590 | Common Platform Enumeration (CPE) |
| Info | 50344 | Missing or Permissive Content-Security-Policy HTTP Response Header |
| Info | 50345 | Missing or Permissive X-Frame-Options HTTP Response Header |
| Info | 54615 | Device Type |
| Info | 91815 | Web Application Sitemap |

## 192.168.10.234

### Summary

| Critical | High | Medium | Low | Info | Total |
|----------|------|--------|-----|------|-------|
| 0 | 0 | 1 | 0 | 38 | 39 |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Medium (6.4) | 51192 | SSL Certificate Cannot Be Trusted |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10147 | Nessus Server Detection |
| Info | 10267 | SSH Server Type and Version Information |
| Info | 10863 | SSL Certificate Information |
| Info | 10881 | SSH Protocol Versions Supported |
| Info | 11032 | Web Server Directory Enumeration |
| Info | 11936 | OS Identification |
| Info | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| Info | 12634 | Authenticated Check : OS Name and Installed Package Enumeration |
| Info | 14272 | Netstat Portscanner (SSH) |
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 21643 | SSL Cipher Suites Supported |
| Info | 21745 | Authentication Failure - Local Checks Not Run |
| Info | 22964 | Service Detection |
| Info | 24260 | HyperText Transfer Protocol (HTTP) Information |
| Info | 25202 | Enumerate IPv6 Interfaces via SSH |
| Info | 25203 | Enumerate IPv4 Interfaces via SSH |
| Info | 25221 | Remote listeners enumeration (Linux / AIX) |
| Info | 33276 | Enumerate MAC Addresses via SSH |
| Info | 34098 | BIOS version (SSH) |
| Info | 35351 | System Information Enumeration (via DMI) |
| Info | 35716 | Ethernet Card Manufacturer Detection |
| Info | 45432 | Processor Information (via DMI) |
| Info | 45433 | Memory Information (via DMI) |

| | | |
|---|---|---|
| **Info** | 45590 | Common Platform Enumeration (CPE) |
| **Info** | 50344 | Missing or Permissive Content-Security-Policy HTTP Response Header |
| **Info** | 54615 | Device Type |
| **Info** | 55472 | Device Hostname |
| **Info** | 56468 | Time of Last System Startup |
| **Info** | 56984 | SSL / TLS Versions Supported |
| **Info** | 58651 | Netstat Active Connections |
| **Info** | 64582 | Netstat Connection Information |
| **Info** | 70544 | SSL Cipher Block Chaining Cipher Suites Supported |
| **Info** | 70657 | SSH Algorithms and Languages Supported |
| **Info** | 84502 | HSTS Missing From HTTPS Server |
| **Info** | 91815 | Web Application Sitemap |
| **Info** | 97993 | OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) |

## 192.168.10.245

### Summary

| Critical | High | Medium | Low | Info | Total | |
|----------|------|--------|-----|------|-------|---|
| 0 | 0 | 0 | 0 | 3 | 3 | |

### Details

| Severity | Plugin Id | Name |
|----------|-----------|------|
| Info | 19506 | Nessus Scan Information |
| Info | 20094 | VMware Virtual Machine Detection |
| Info | 35716 | Ethernet Card Manufacturer Detection |

## 192.168.10.251

### Summary

| Critical | High | Medium | Low | Info | Total | |
|---|---|---|---|---|---|---|
| **0** | **0** | **0** | **0** | **19** | **19** | |

### Details

| Severity | Plugin Id | Name |
|---|---|---|
| **Info** | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| **Info** | 10267 | SSH Server Type and Version Information |
| **Info** | 10287 | Traceroute Information |
| **Info** | 10881 | SSH Protocol Versions Supported |
| **Info** | 11219 | Nessus SYN scanner |
| **Info** | 11819 | TFTP Daemon Detection |
| **Info** | 11936 | OS Identification |
| **Info** | 19506 | Nessus Scan Information |
| **Info** | 20094 | VMware Virtual Machine Detection |
| **Info** | 21745 | Authentication Failure - Local Checks Not Run |
| **Info** | 22964 | Service Detection |
| **Info** | 25220 | TCP/IP Timestamps Supported |
| **Info** | 35716 | Ethernet Card Manufacturer Detection |
| **Info** | 39520 | Backported Security Patch Detection (SSH) |
| **Info** | 45590 | Common Platform Enumeration (CPE) |
| **Info** | 54615 | Device Type |
| **Info** | 66717 | mDNS Detection (Local Network) |
| **Info** | 70657 | SSH Algorithms and Languages Supported |
| **Info** | 104410 | Host Authentication Failure(s) for Provided Credentials |