Nessus Report

Nessus Scan Report

Thu, 23 Nov 2017 16:19:05 GMT

Table Of Contents

Hosts Summary (Executive)

192.168.0.1

Summary

Critical	High	Medium	Low	Info	Total
3	2	5	0	56	66

Details

Severity	Plugin Id	Name
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)
Critical (10.0)	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (5.0)	10704	Apache Multiviews Arbitrary Directory Listing
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
Info	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection

Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10897	Microsoft Windows - Users Information : Disabled Accounts
Info	10898	Microsoft Windows - Users Information : Never Changed Password
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In
Info	10900	Microsoft Windows - Users Information : Passwords Never Expire
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10908	Microsoft Windows 'Domain Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
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	13855	Microsoft Windows Installed Hotfixes
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
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	24260	HyperText Transfer Protocol (HTTP) Information
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	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	66334	Patch Report
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)

192.168.0.2

Summary

Critical	High	Medium	Low	Info	Total
3	2	3	0	55	63

Details

Severity	Plugin Id	Name
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)
Critical (10.0)	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (5.0)	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
Info	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10897	Microsoft Windows - Users Information : Disabled Accounts
Info	10898	Microsoft Windows - Users Information : Never Changed Password
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In
Info	10900	Microsoft Windows - Users Information : Passwords Never Expire
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10908	Microsoft Windows 'Domain Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
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	13855	Microsoft Windows Installed Hotfixes
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
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	24260	HyperText Transfer Protocol (HTTP) Information
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	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)

Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
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)

192.168.0.10

Summary

Critical	High	Medium	Low	Info	Total
3	3	3	0	37	46

Details

Severity	Plugin Id	Name
Critical (10.0)	16334	ArGoSoft FTP Server < 1.4.2.8 Multiple .LNK File Handling Vulnerabilities
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	15623	ArGoSoft FTP Server .lnk Shortcut Upload Arbitrary File Manipulation
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (6.0)	17303	ArGoSoft FTP Server DELE Command Remote Buffer Overrun
Medium (5.0)	57608	SMB Signing Disabled
Info	10092	FTP Server Detection
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10897	Microsoft Windows - Users Information : Disabled Accounts

Info	10898	Microsoft Windows - Users Information : Never Changed Password
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In
Info	10900	Microsoft Windows - Users Information : Passwords Never Expire
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
Info	100871	Microsoft Windows SMB Versions Supported (remote check)

192.168.0.11

Summary

Critical	High	Medium	Low	Info	Total
2	0	2	0	35	39

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)	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)	57608	SMB Signing Disabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10897	Microsoft Windows - Users Information : Disabled Accounts
Info	10898	Microsoft Windows - Users Information : Never Changed Password
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In
Info	10900	Microsoft Windows - Users Information : Passwords Never Expire
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10914	Microsoft Windows - Local Users Information : Never Changed Passwords

Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
Info	100871	Microsoft Windows SMB Versions Supported (remote check)