windows

Report generated by Nessus™ Mon, 01 Jul 2019 08:45:15 EDT

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.0.128

Vulnerabilities Total: 31

SEVERITY	CVSS	PLUGIN	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)
HIGH	7.5	11580	Firewall UDP Packet Source Port 53 Ruleset Bypass
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	42799	Broken Web Servers
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.153

Vulnerabilities Total: 36

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
CRITICAL	10.0	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
CRITICAL	10.0	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (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	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version

INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure