## Nessus Report

Nessus Scan Report Thu, 23 Nov 2017 16:19:05 GMT

## **Table Of Contents**

Hosts Summary (Executive)	3
•192.168.0.1	
•192.168.0.2	
•192.168.0.10	10
●192 168 N 11	12

## Hosts Summary (Executive)

0.141		ac ::			<b>T</b> .4.1
Critical	High	Medium	Low	Info	Total
3	2	5	0	56	66
etails Severity	Plugin	ld Name	<b>1</b>		
Critical (10.0)	72836	MS11	-058: Vulnerabili	ties in DNS Server uncredentialed che	Could Allow Remote Code
Critical (10.0)	97833	(ETE	RNALBLUE) (ET RNALSYNERGY	ERNALCHAMPION	Windows SMB Server (4013389 N) (ETERNALROMANCE) rnalRocks) (Petya) (uncredential
Critical (10.0)	100464	Micro	soft Windows SN	MBv1 Multiple Vulne	erabilities
High (7.6)	103876		soft Windows SN edentialed check		) Multiple Vulnerabilities
High (7.5)	42411	Micro	soft Windows SN	MB Shares Unprivile	eged Access
Medium (6.8)	90510			pdate for SAM and uncredentialed che	LSAD Remote Protocols ck)
Medium (5.8)	42263	Unen	crypted Telnet S	erver	
Medium (5.0)	10704	Apach	ne Multiviews Art	oitrary Directory Lis	ting
Medium (5.0)	11213	HTTP	TRACE / TRAC	K Methods Allowed	i
Medium (5.0)	72837		-017: Vulnerabili 170) (uncredenti		could Allow Denial of Service
Info	10107	HTTP	Server Type an	d Version	
Info	10114	ICMP	Timestamp Req	uest Remote Date	Disclosure
Info	10150	Windo	ows NetBIOS / S	MB Remote Host Ir	nformation Disclosure
Info	10281	Telne	t Server Detection	n	
Info	10287	Trace	route Information	า	
Info	10394	Micro	soft Windows SN	MB Log In Possible	
Info	10395	Micro	soft Windows SN	/IB Shares Enumera	ation
Info	10398		soft Windows SN on Domain SID B		ationPolicy Function NULL
Info	10399	SMB	Use Domain SID	to Enumerate Use	rs
Info	10400	Micro	soft Windows SN	IB Registry Remote	ely Accessible
Info	10413	Micro	soft Windows SN	/IB Registry : Remo	te PDC/BDC Detection
Info	10428	Micro	soft Windows SN	//B Registry Not Ful	lly 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)			

92.168.0.2						
Summary						
Critical	High	Medium	Low	Info	Total	
3	2	3	0	55	63	
Details	Divers I	d Name				
Severity	Plugin le					
Critical (10.0)	72836			ties in DNS Server of the control of	Could Allow Remote Code ck)	
Critical (10.0)	97833	(ETEF	RNALBLUE) (ET RNALSYNERGY	ERNALCHAMPION	Windows SMB Server (4013389) ) (ETERNALROMANCE) nalRocks) (Petya) (uncredentialed	
Critical (10.0)	100464	Micros	soft Windows SN	1Bv1 Multiple Vulne	rabilities	
High (7.6)	103876		soft Windows SNedentialed check		Multiple Vulnerabilities	
High (7.5)	42411	Micros	soft Windows SN	IB Shares Unprivile	ged Access	
Medium (6.8)	90510			pdate for SAM and uncredentialed chec	LSAD Remote Protocols	
Medium (5.8)	42263	Unend	crypted Telnet Se	erver		
Medium (5.0)	72837		-017: Vulnerabili 170) (uncredenti		ould Allow Denial of Service	
Info	10107	HTTP Server Type and Version				
Info	10114	ICMP	Timestamp Req	uest Remote Date [	Disclosure	
Info	10150	Windo	Windows NetBIOS / SMB Remote Host Information Disclosure			
Info	10281	Telnet	Server Detection	n		
Info	10287	Trace	route Information	1		
Info	10394	Micros	soft Windows SN	IB Log In Possible		
Info	10395	Micros	soft Windows SN	1B Shares Enumera	ition	
Info	10398		soft Windows SN on Domain SID B		ationPolicy Function NULL	
Info	10399	SMB (	Jse Domain SID	to Enumerate User	s	
Info	10400	Micros	soft Windows SN	IB Registry Remote	ly Accessible	
Info	10413	Micros	soft Windows SN	IB Registry : Remot	re PDC/BDC Detection	
Info	10428	Micros	soft Windows SN	IB Registry Not Full	y Accessible Detection	
Info	10736	DCE S	Services Enume	ation		
Info	10785	Micros Disclo		1B NativeLanManaoู	ger Remote System Information	

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)

100 100 0 10						
192.168.0.10 Summary						
Critical	High	Medium	Low	Info	Total	
3	3	3	0	37	46	
Details						
Severity	Plugi	n Id Name	•			
Critical (10.0)	16334	4 ArGos	Soft FTP Server	< 1.4.2.8 Multiple .L	NK File Handling Vulne	erabilities
Critical (10.0)	53514		-030: Vulnerabili ution (2509553) (		on Could Allow Remote	Code
Critical (10.0)	97833	(ETER	RNALBLUE) (ET RNALSYNERGY	ERNALCHAMPION	Windows SMB Server ( I) (ETERNALROMANC nalRocks) (Petya) (unc	E)
High (7.6)	1038		soft Windows SN edentialed check	· · · · · · · · · · · · · · · · · · ·	) Multiple Vulnerabilitie:	S
High (7.5)	15623	3 ArGos	Soft FTP Server	Ink Shortcut Upload	d Arbitrary File Manipul	ation
High (7.5)	4241	1 Micros	soft Windows SN	MB Shares Unprivile	ged Access	
Medium (6.8)	90510			pdate for SAM and uncredentialed chec	LSAD Remote Protoco ck)	ls
Medium (6.0)	17303	3 ArGos	Soft FTP Server	DELE Command R	emote Buffer Overrun	
Medium (5.0)	57608	SMB	Signing Disabled	I		
Info	10092	2 FTP S	Server Detection			
Info	10114	4 ICMP	Timestamp Req	uest Remote Date I	Disclosure	
Info	10150	) Windo	ows NetBIOS / S	MB Remote Host In	formation Disclosure	
Info	1028	7 Trace	route Information	ı		
Info	10394	4 Micros	soft Windows SN	MB Log In Possible		
Info	1039	5 Micros	soft Windows SN	MB Shares Enumera	ation	
Info	10398		soft Windows SN on Domain SID E		ationPolicy Function NU	JLL
Info	10399	9 SMB	Use Domain SID	to Enumerate Use	rs	
Info	1073	DCE S	Services Enume	ration		
Info	1078	5 Micros Disclo		/IB NativeLanManaoุ	ger Remote System Info	ormation
Info	10859		soft Windows SN eration	IB LsaQueryInform	ationPolicy Function SI	D
Info	10860	SMB	Use Host SID to	Enumerate Local U	sers	
Info	1089	7 Micros	soft Windows - L	Isers 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)

100 100 0 11								
192.168.0.11 Summary								
Critical	High		Mediu	ım	Low	Info	Tota	I
2	0		2		0	35	39	
Details								
Severity	PI	ugin ld		Name				
Critical (10.0)	53	3514				ty in DNS Resolu remote check)	tion Could Allo	ow Remote Code
Critical (10.0)	97	7833		(ETERNALI	BLUE) (ETI	ERNALCHAMPIC	ON) (ETERNAI	MB Server (4013389) LROMANCE) Petya) (uncredentialed
Medium (6.8)	90	0510				odate for SAM ar incredentialed ch		ote Protocols
Medium (5.0)	57	7608	;	SMB Signin	ng Disabled			
Info	10	)114		ICMP Time	stamp Requ	uest Remote Dat	e Disclosure	
Info	10	)150	,	Windows N	etBIOS / SI	MB Remote Host	Information D	isclosure
Info	10	)287		Traceroute	Information	ı		
Info	10	)394		Microsoft W	/indows SM	IB Log In Possibl	е	
Info	10	395		Microsoft W	/indows SM	IB Shares Enume	eration	
Info	10	)398	Microsoft Windows SMB LsaQueryInformationPolicy Function NU Session Domain SID Enumeration					Function NULL
Info	10	399	;	SMB Use Domain SID to Enumerate Users				
Info	10	736		DCE Services Enumeration				
Info	10	)785		Microsoft W Disclosure	/indows SM	IB NativeLanMar	nager Remote	System Information
Info	10	)859		Microsoft W Enumeratio		IB LsaQueryInfor	mationPolicy F	Function SID
Info	10	0860	;	SMB Use H	lost SID to	Enumerate Local	Users	
Info	10	)897		Microsoft W	/indows - U	sers Information	: Disabled Acc	counts
Info	10	)898		Microsoft W	/indows - U	sers Information	: Never Chang	ged Password
Info	10	)899		Microsoft W	/indows - U	sers Information	: User Has Ne	ever Logged In
Info	10	900		Microsoft W	/indows - U	sers Information	: Passwords N	Never Expire
Info	10	)902		Microsoft W	/indows 'Ad	lministrators' Gro	up User List	
Info	10	)913		Microsoft W	/indows - Lo	ocal Users Inform	nation : Disable	ed Accounts
Info	10	)914		Microsoft W	/indows - Lo	ocal Users Inform	nation : 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)