Nessus Report

Nessus Scan Report Fri, 08 Dec 2017 18:00:36 EET

Table Of Contents

Hosts Summary (Executive)	3
•10.0.100.1	
•10.0.100.10	
•10.0.100.20	
•10.0.100.30	
•10.0.100.50	11
•10.0.100.91	13
•10.0.100.234	
•10.0.100.251	

Hosts Summary (Executive)

10.0.100.1 Summary								
Critical	High	1	Medi	um	Low	Info	Total	
0	0		1		0	5	6	
Details								
Severity		Plugin Id		Name				
Medium (5.8)		50686		IP Forwar	ding Enable	d		
Info		10114 ICMP Timestamp Request Remote Date Disclosure						
Info		19506		Nessus Scan Information				
Info		20094		VMware Virtual Machine Detection				
Info		34277		Nessus U	DP Scanner			
Info		35716		Ethernet (Card Manufa	cturer Detection		

0.0.100.10 ummary							
Critical	High	Medium	Low	Info	Total		
4	0	9	0	41	54		
etails							
Severity	Plugin lo	l Name					
Critical (10.0)	53514		-030: Vulnerability tion (2509553) (r		on Could Allow Remote Code		
Critical (10.0)	72836			es in DNS Server incredentialed che	Could Allow Remote Code		
Critical (10.0)	79638		-066: Vulnerability 611) (uncredentia		ld Allow Remote Code Executio		
Critical (10.0)	97833	(ETER (ETER	MS17-010: Security Update for Microsoft Windows SMB Server (4013389 (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredential check)				
Medium (6.8)	90510			date for SAM and ncredentialed che	LSAD Remote Protocols ck)		
Medium (6.4)	51192	SSL C	ertificate Cannot	Be Trusted			
Medium (6.4)	57582	SSL S	SSL Self-Signed Certificate				
Medium (5.8)	50686	IP For	IP Forwarding Enabled				
Medium (5.0)	42873	SSL M	ledium Strength (Cipher Suites Sup	ported		
Medium (5.0)	72837		-017: Vulnerabilit 170) (uncredentia		ould Allow Denial of Service		
Medium (5.0)	94437	SSL 6	4-bit Block Size (Cipher Suites Supp	ported (SWEET32)		
Medium (4.3)	80035	TLS P	adding Oracle Inf	formation Disclosu	re Vulnerability (TLS POODLE)		
Medium (4.0)	35291	SSL C	ertificate Signed	Using Weak Hash	ing Algorithm		
Info	10150	Windo	ws NetBIOS / SN	/IB Remote Host Ir	nformation Disclosure		
Info	10287	Tracer	oute Information				
Info	10335	Nessu	s TCP scanner				
Info	10394	Micros	oft Windows SM	B Log In Possible			
Info	10736	DCE S	Services Enumera	ation			
Info	10785	Micros Disclo		B NativeLanMana	ger Remote System Information		
Info	10863	SSL C	ertificate Informa	tion			
Info	10884	Netwo	rk Time Protocol	(NTP) Server Det	ection		
Info	10940	Windo	ws Terminal Serv	vices Enabled			

Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
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	21643	SSL Cipher Suites Supported
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	34277	Nessus UDP Scanner
Info	35297	SSL Service Requests Client Certificate
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	72779	DNS Server Version Detection
Info	72780	Microsoft DNS Server Version Detection
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

10.0.100.20 Summary						
Critical	High	Medium	Low	Info	Total	
2	0	0	0	20	22	
Details						
Severity	Plugir	n Id Name				
Critical (10.0)	53514	_	-030: Vulnerabilit tion (2509553) (ı		on Could Allow Remote C	ode
Critical (10.0)	97833	(ETER	RNALBLUE) (ETE RNALSYNERGY)	ERNALCHAMPION	Windows SMB Server (4 I) (ETERNALROMANCE nalRocks) (Petya) (uncre	. (
Info	10150	Windo	ws NetBIOS / SI	MB Remote Host Ir	formation Disclosure	
Info	10287	Tracer	oute Information	1		
Info	10335	Nessu	s TCP scanner			
Info	10394	Micros	soft Windows SM	IB Log In Possible		
Info	10736	DCE S	Services Enumer	ation		
Info	10785	Micros Disclo		IB NativeLanMana	ger Remote System Infor	mation
Info	11011	Micros	soft Windows SM	1B Service Detection	n	
Info	11936	OS Ide	entification			
Info	19506	Nessu	s Scan Informati	ion		
Info	20094	VMwa	re Virtual Machir	ne Detection		
Info	24786	Nessu	s Windows Scar	n Not Performed wi	th Admin Privileges	
Info	25220	TCP/II	P Timestamps S	upported		
Info	26917	Micros Regist		1B Registry : Nessu	s Cannot Access the Wi	ndows
Info	34277	Nessu	s UDP Scanner			
Info	35716	Ethern	net Card Manufac	cturer Detection		
Info	45590	Comm	non Platform Enu	imeration (CPE)		
Info	53513	Link-L	ocal Multicast Na	ame Resolution (LL	MNR) Detection	
Info	54615	Device	е Туре			
Info	96982	Server check)		(SMB) Protocol Ve	ersion 1 Enabled (uncred	entialed
Info	10087	1 Micros	soft Windows SM	IB Versions Suppo	rted (remote check)	

ummary					
Critical	High	Medium	Low	Info	Total
0	0	12	4	33	49
etails					
Severity	Plugin				
Medium (6.4)	51192	SSL C	Certificate Canno	t Be Trusted	
Medium (6.4)	57582	SSL S	Self-Signed Certif	ficate	
Medium (5.0)	11213	HTTP	TRACE / TRAC	K Methods Allowed	i
Medium (5.0)	15901	SSL C	Certificate Expiry		
Medium (5.0)	20007	SSL V	ersion 2 and 3 F	Protocol Detection	
Medium (5.0)	42873	SSL N	Medium Strength	Cipher Suites Sup	ported
Medium (5.0)	94437	SSL 6	34-bit Block Size	Cipher Suites Supp	ported (SWEET32)
Medium (4.3)	26928	SSL V	Veak Cipher Suit	es Supported	
Medium (4.3)	62565	Trans	port Layer Secur	ity (TLS) Protocol (CRIME Vulnerability
Medium (4.3)	78479	SSLv3 (POO		e On Downgraded L	egacy Encryption Vulnerability
Medium (4.3)	90317	SSH	Weak Algorithms	Supported	
Medium (4.0)	35291	SSL C	Certificate Signed	I Using Weak Hash	ing Algorithm
Low (2.6)	65821	SSL R	RC4 Cipher Suite	s Supported (Bar N	/litzvah)
Low (2.6)	70658	SSH S	Server CBC Mod	e Ciphers Enabled	
Low (2.6)	71049	SSHV	Weak MAC Algor	rithms Enabled	
Low	69551	SSL C	Certificate Chain	Contains RSA Keys	s Less Than 2048 bits
Info	10107	HTTP	Server Type and	d Version	
Info	10114	ICMP	Timestamp Req	uest Remote Date	Disclosure
Info	10267	SSH S	Server Type and	Version Information	n
Info	10287	Trace	route Information)	
Info	10335	Nessu	us TCP scanner		
Info	10386	Web S	Server No 404 E	ror Code Check	
Info	10863	SSL C	Certificate Information	ation	
Info	10881	SSH F	Protocol Versions	s Supported	
Info	11936	OS Id	entification		

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	34277	Nessus UDP Scanner
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version Detection
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	84502	HSTS Missing From HTTPS Server
Info	84574	Backported Security Patch Detection (PHP)
Info	94761	SSL Root Certification Authority Certificate Information

0.100.50 mmary						
Critical	High	Medium	Low	Info	Total	
)	0	2	2	23	27	
tails	Plugin	ld Name				
Severity	Plugin			IZ NASALS SISS A HERVES		
Medium (5.0)	11213			K Methods Allowed		
Medium (4.3)	90317		Weak Algorithms			
_ow (2.6)	70658			e Ciphers Enabled		
_ow (2.6)	71049		Weak MAC Algor			
nfo ————	10107	HTTF	Server Type and	d Version		
nfo	10114	ICMP	Timestamp Req	uest Remote Date I	Disclosure	
nfo	10267	SSH	Server Type and	Version Information	n	
nfo	10287	Trace	eroute Information	1		
nfo	10335	Ness	us TCP scanner			
nfo	10719	MySC	L Server Detect	on		
nfo	10881	SSH	SSH Protocol Versions Supported			
nfo	11153	Servi	Service Detection (HELP Request)			
nfo	11936	OS Id	lentification			
nfo	18261	Apacl	he Banner Linux	Distribution Disclos	ure	
nfo	19506	Ness	us Scan Informat	ion		
nfo	20094	VMwa	are Virtual Machi	ne Detection		
nfo	22964	Servi	ce Detection			
nfo	24260	Нуре	rText Transfer Pr	otocol (HTTP) Infor	mation	
nfo	25220	TCP/	IP Timestamps S	upported		
nfo	34277	Ness	us UDP Scanner			
nfo	35716	Ether	net Card Manufa	cturer Detection		
nfo	39520	Back	ported Security P	atch Detection (SS	H)	
nfo	39521		-	atch Detection (WV		
nfo	43111		Methods Allowe	·		
nfo	45590		non Platform Enu			
nfo	54615		e Type	, ,		

0.0.100.91							
Summary							
Critical	High		Medi	ium	Low	Info	Total
0	0		1		0	17	18
Details							
Severity		Plugin Id		Name			
Medium (5.0)		88098		Apache Se	erver ETag F	leader Informatio	n Disclosure
Info		10107		HTTP Serv	ver Type and	d Version	
Info		10114		ICMP Time	estamp Req	uest Remote Date	e Disclosure
Info		10287		Traceroute	Information	ı	
Info		10335		Nessus TC	CP scanner		
Info		11936		OS Identifi	cation		
Info		18261		Apache Ba	anner Linux	Distribution Disclo	osure
Info		19506		Nessus Sc	an Informati	on	
Info		20094		VMware V	irtual Machir	ne Detection	
Info		22964		Service De	etection		
Info		24260		HyperText	Transfer Pr	otocol (HTTP) Infe	ormation
Info		25220		TCP/IP Tir	nestamps S	upported	
Info		34277		Nessus UE	OP Scanner		
Info		35716		Ethernet C	ard Manufa	cturer Detection	
Info		39521		Backported	d Security P	atch Detection (W	/WW)
Info		43111		HTTP Met	hods Allowe	d (per directory)	
Info		45590		Common F	Platform Enu	meration (CPE)	
Info		54615		Device Typ	oe		

10.0.100.234						
Summary	Himb		BA a alicena	Law	lufo	Tatal
Critical	High		Medium	Low	Info	Total
0 Details	0		1	0	35	36
Severity		Plugin Id	Nan	ne		
Medium (6.4)		51192	SSL	Certificate Canno	t Be Trusted	
Info		10107	НТТ	P Server Type and	d Version	
Info		10147	Nes	sus Server Detecti	on	
Info		10267	SSH	H Server Type and	Version Information	1
Info		10863	SSL	Certificate Informa	ation	
Info		10881	SSF	H Protocol Versions	Supported	
Info		11936	os	Identification		
Info		12053	Hos	t Fully Qualified Do	omain Name (FQDN	N) Resolution
Info		12634	Auth	nenticated Check:	OS Name and Insta	alled Package Enumeration
Info		14272	Nets	stat Portscanner (S	SH)	
Info		19506	Nes	sus Scan Informat	on	
Info		20094	VMv	ware Virtual Machi	ne Detection	
Info		21643	SSL	. Cipher Suites Sup	pported	
Info		21745	Auth	nentication Failure	- Local Checks Not	Run
Info		22964	Ser	vice Detection		
Info		24260	Нур	erText Transfer Pr	otocol (HTTP) Infor	mation
Info		25202	Enu	merate IPv6 Interfa	aces via SSH	
Info		25203	Enu	merate IPv4 Interfa	aces via SSH	
Info		25221	Ren	note listeners enun	neration (Linux / AI)	()
Info		33276	Enu	merate MAC Addr	esses via SSH	
Info		34098	BIO	S version (SSH)		
Info		35351	Sys	tem Information Er	umeration (via DMI)
Info	_	35716	Ethe	ernet Card Manufa	cturer Detection	
Info		45432	Pro	cessor Information	(via DMI)	
Info		45433	Mer	mory Information (v	ia DMI)	
Info		45590	Con	nmon Platform Enu	meration (CPE)	

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	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

10.0.100.251								
Summary								
Critical	High	Medium	Low	Info	Total			
0	0	0	0	18	18			
Details								
Severity	Plugin lo	l Name						
Info	10114	ICMP 7	Γimestamp Requ	uest Remote Date	Disclosure			
Info	10267	SSH S	erver Type and '	Version Information	n			
Info	10287	Tracero	oute Information					
Info	10335	Nessus	s TCP scanner					
Info	10881	10881 SSH Protocol Versions Supported						
Info	11819	TFTP [Daemon Detection	on				
Info	11936	OS Ide	OS Identification					
Info	19506	Nessus	Nessus Scan Information					
Info	20094	VMwar	e Virtual Machin	rtual Machine Detection				
Info	22964	Service	e Detection					
Info	25220	TCP/IP	Timestamps Su	upported				
Info	34277	Nessus	s UDP Scanner					
Info	35716	Etherno	et Card Manufac	cturer Detection				
Info	39520	Backpo	orted Security Pa	atch Detection (SS	SH)			
Info	45590	Commo	on Platform Enu	meration (CPE)				
Info	54615	Device	Туре					
Info	66717	mDNS	Detection (Loca	l Network)				
Info	70657	SSH A	Igorithms and La	anguages Support	ed			