Nessus Report

Nessus Scan Report Thu, 07 Dec 2017 18:25:33 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	10
•10.0.100.91	11
•10.0.100.234	
•10.0.100.251	12

Hosts Summary (Executive)

10.0.100.1								
Summary Critical	Hig	h	Med	ium	Low	Info	Total	
Critical	nig	"	Wed	iuiii	LOW	IIIIO	Total	
0	0		1		0	4	5	
Details								
Severity		Plugin Id		Name				
Medium (5.8)		50686		IP Forward	ding Enabled			
Info		10114		ICMP Time	estamp Requ	est Remote Date	Disclosure	
Info		19506		Nessus So	can Informatio	on		
Info		20094		VMware V	irtual Machin	e Detection		
Info		35716		Ethernet C	ard Manufac	turer Detection		

ummary					
Critical	High	Medium	Low	Info	Total
4	0	9	0	40	53
etails					
Severity	Plugin l	d Name			
Critical (10.0)	53514		-030: Vulnerabilit tion (2509553) (r		on Could Allow Remote Code
Critical (10.0)	72836			ies in DNS Server incredentialed che	Could Allow Remote Code ck)
Critical (10.0)	79638		-066: Vulnerabilit 611) (uncredentia		ld Allow Remote Code Executio
Critical (10.0)	97833	(ETEF	RNALBLUE) (ETE RNALSYNERGY)	RNALCHAMPION	Windows SMB Server (4013389 I) (ETERNALROMANCE) nalRocks) (Petya) (uncredential
Medium (6.8)	90510			date for SAM and ncredentialed che	LSAD Remote Protocols ck)
Medium (6.4)	51192	SSL C	Certificate Cannot	Be Trusted	
Medium (6.4)	57582	SSL S	Self-Signed Certifi	cate	
Medium (5.8)	50686	IP For	warding Enabled		
Medium (5.0)	42873	SSL M	Medium Strength	Cipher Suites Sup	ported
Medium (5.0)	72837		-017: Vulnerability 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 In	formation Disclosu	re Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL C	Certificate Signed	Using Weak Hash	ing Algorithm
Info	10150	Windo	ows NetBIOS / SN	/IB Remote Host Ir	nformation Disclosure
Info	10287	Trace	route Information		
Info	10394	Micros	soft 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	Certificate Informa	tion	
Info	10884	Netwo	ork Time Protocol	(NTP) Server Dete	ection
Info	10940	Windo	ows Terminal Serv	vices Enabled	
Info	11002	DNS S	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	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	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)
Info	100871	Microsoft Windows SMB Versions Supported (remote check)

10.0.100.20						
Summary						
Critical	High	Medium	Low	Info	Total	
2	0	0	0	19	21	
Details						
Severity	Plugin I	d Name				
Critical (10.0)	53514		-030: Vulnerabili ition (2509553) (n Could Allow Remote	Code
Critical (10.0)	97833	(ETER	RNALBLUE) (ET RNALSYNERGY	ERNALCHAMPION	Windows SMB Server) (ETERNALROMANC nalRocks) (Petya) (unc	E)
Info	10150	Windo	ows NetBIOS / S	MB Remote Host In	formation Disclosure	
Info	10287	Tracei	route Information	า		
Info	10394	Micros	soft Windows SN	MB Log In Possible		
Info	10736	DCE S	Services Enume	ration		
Info	10785	Micros Disclo		/IB NativeLanManag	ger Remote System Inf	ormation
Info	11011	Micros	soft Windows SN	MB Service Detectio	n	
Info	11219	Nessu	ıs SYN scanner			
Info	11936	OS Ide	entification			
Info	19506	Nessu	ıs Scan Informat	ion		
Info	20094	VMwa	re Virtual Machi	ne Detection		
Info	24786	Nessu	ıs Windows Sca	n Not Performed wit	h Admin Privileges	
Info	25220	TCP/II	P Timestamps S	supported		
Info	26917	Micros Regist		/IB Registry : Nessu	s Cannot Access the V	Vindows
Info	35716	Etherr	net Card Manufa	cturer Detection		
Info	45590	Comm	non Platform Enu	umeration (CPE)		
Info	53513	Link-L	ocal Multicast N	ame Resolution (LL	MNR) Detection	
Info	54615	Device	е Туре			
Info	96982	Serve check)		(SMB) Protocol Ve	rsion 1 Enabled (uncre	edentialed
Info	100871	Micros	soft Windows SN	MB Versions Suppor	ted (remote check)	

0.0.100.30 ummary					
Critical	High	Medium	Low	Info	Total
0	0	12	4	32	48
etails					
Severity	Plugin	ld Name	:		
Medium (6.4)	51192	SSL C	Certificate Canno	t Be Trusted	
Medium (6.4)	57582	SSL S	Self-Signed Certi	ficate	
Medium (5.0)	11213	HTTP	TRACE / TRAC	K Methods Allowed	
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 Supp	ported
Medium (5.0)	94437	SSL 6	34-bit Block Size	Cipher Suites Supp	orted (SWEET32)
Medium (4.3)	26928	SSL V	Veak Cipher Sui	tes Supported	
Medium (4.3)	62565	Trans	port Layer Secu	rity (TLS) Protocol C	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	SSLC	Certificate Signed	d Using Weak Hash	ing Algorithm
Low (2.6)	65821	SSL F	RC4 Cipher Suite	es Supported (Bar M	litzvah)
Low (2.6)	70658	SSHS	Server CBC Mod	e Ciphers Enabled	
Low (2.6)	71049	SSH \	Weak MAC Algo	rithms Enabled	
Low	69551	SSL C	Certificate Chain	Contains RSA Keys	Less Than 2048 bits
Info	10107	HTTP	Server Type an	d Version	
Info	10114	ICMP	Timestamp Req	uest Remote Date [Disclosure
Info	10267	SSH S	Server Type and	Version Information	1
Info	10287	Trace	route Information	า	
Info	10386	Web S	Server No 404 E	rror Code Check	
Info	10863	SSL C	Certificate Inform	ation	
Info	10881	SSH F	Protocol Version	s Supported	
Info	11219	Nessu	us SYN scanner		
Info	11936	OS Id	entification		
Info	18261			Distribution Disclos	ure

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	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	22	26		
tails							
Severity	Plugin	ld Name	9				
Medium (5.0)	11213	HTTF	PTRACE / TRAC	K Methods Allowed			
Medium (4.3)	90317	SSH	Weak Algorithms	Supported			
_ow (2.6)	70658	SSH	Server CBC Mod	e Ciphers Enabled			
_ow (2.6)	71049	SSH	Weak MAC Algor	rithms Enabled			
nfo	10107	HTTF	Server Type and	d Version			
nfo	10114	ICMP	Timestamp Req	uest Remote Date [Disclosure		
nfo	10267	SSH	Server Type and	Version Information	l		
nfo	10287	Trace	eroute Information	1			
nfo	10719	MySC	QL Server Detect	ion			
nfo	10881	SSH	SH Protocol Versions Supported				
nfo	11153	Servi	vice Detection (HELP Request)				
nfo	11219	Ness	us SYN scanner				
nfo	11936	OS Id	lentification				
nfo	18261	Apacl	he Banner Linux	Distribution Disclosi	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	35716	Ether	net Card Manufa	cturer Detection			
nfo	39520	Backı	ported Security P	atch Detection (SSI	H)		
nfo	39521	Backı	ported Security P	atch Detection (WW	/W)		
nfo	43111	HTTF	Methods Allowe	d (per directory)			
nfo	45590	Comr	mon Platform Enu	umeration (CPE)			
nfo	54615	Devic	е Туре				
nfo	70657	SSH	Algorithms and L	anguages Supporte	d		

10.0.100.91 Summary						
•	High	Medium	Low	Info	Total	
	0	1	0	16	17	
Details Severity	Plugin Id	Name				
	_					
Medium (5.0)	88098	Apache	e Server ETag H	leader Information	Disclosure	
Info	10107	HTTP	Server Type and	l Version		
Info	10114	10114 ICMP Timestamp Request Remote Date Disclosure				
Info	10287	Tracero	oute Information			
Info	11219	Nessus	s SYN scanner			
Info	11936	OS Ide	ntification			
Info	18261	Apache	e Banner Linux [Distribution Disclo	sure	
Info	19506	Nessus	s Scan Informati	on		
Info	20094	VMwar	e Virtual Machin	e Detection		
Info	22964	Service	e Detection			
Info	24260	HvnerT	ext Transfer Pro	otocol (HTTP) Info	rmation	
				, ,	····duoi	
Info	25220		Timestamps Su			
Info	35716	Etherno	et Card Manufac	cturer Detection		
Info	39521	Backpo	orted Security Pa	atch Detection (W	WW)	
Info	43111	HTTP I	Methods Allowed	d (per directory)		
Info	45590	Commo	on Platform Enu	meration (CPE)		
Info	54615	Device	Type			

.0.100.234 Immary					
Critical	High	Medium	Low	Info	Total
0	0	1	0	35	36
etails					
Severity	Plugir				
Medium (6.4)	51192		Certificate Canno		
Info	10107	HTTF	P Server Type and	d Version	
Info	10147	Ness	us Server Detecti	on	
Info	10267	SSH	Server Type and	Version Information	n
Info	10863	SSL	Certificate Informa	ation	
Info	10881	SSH	Protocol Versions	Supported	
Info	11936	OS Id	lentification		
Info	12053	Host	Fully Qualified Do	omain Name (FQDI	N) Resolution
Info	12634	Authe	enticated Check:	OS Name and Inst	alled Package Enumeration
Info	14272	Netst	at Portscanner (S	SSH)	
Info	19506	Ness	us Scan Informati	ion	
Info	20094	VMwa	are Virtual Machir	ne Detection	
Info	21643	SSL	Cipher Suites Sup	ported	
Info	21745	Authe	entication Failure	- Local Checks Not	Run
Info	22964	Servi	ce Detection		
Info	24260	Нуре	rText Transfer Pr	otocol (HTTP) Infor	rmation
Info	25202	Enum	nerate IPv6 Interfa	aces via SSH	
Info	25203	Enum	nerate IPv4 Interfa	aces via SSH	
Info	25221	Remo	ote listeners enun	neration (Linux / Al)	×)
Info	33276	Enum	nerate MAC Addre	esses via SSH	
Info	34098	BIOS	version (SSH)		
Info	35351			numeration (via DM	I)
Info	35716	•	net Card Manufa	·	•
Info	45432		essor Information		
Info	45433		ory Information (v		
Info	45433			imeration (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	17	17
Details					
Severity	Plugir 	ı Id Name			
Info	10114	ICMP '	Timestamp Requ	uest Remote Date	Disclosure
Info	10267	SSH S	Server Type and	Version Information	on
Info	10287	Tracer	oute Information		
Info	10881	SSH P	Protocol Versions	Supported	
Info	11219	11219 Nessus SYN scanner			
Info	11819	11819 TFTP Daemon Detection			
Info	11936	OS Ide	entification		
Info	19506	Nessu	s Scan Informati	on	
Info	20094	VMwa	re Virtual Machir	e Detection	
Info	22964	Service	e Detection		
Info	25220	TCP/IF	P Timestamps Su	upported	
Info	35716	Ethern	et Card Manufac	cturer Detection	
Info	39520	Backp	orted Security Pa	atch Detection (SS	SH)
Info	45590	Comm	on Platform Enu	meration (CPE)	
Info	54615	Device	е Туре		
Info	66717	mDNS	Detection (Loca	l Network)	
Info	70657	SSH A	Algorithms and La	anguages Support	ed