Nessus Report

Nessus Scan Report Thu, 07 Dec 2017 19:12:53 EET

Table Of Contents

Hosts Summary (Executive)	3
•192.168.10.1	
•192.168.10.10	
•192.168.10.30	
•192.168.10.51	
● 192.168.10.52	10
•192.168.10.234	11
•192.168.10.245	13
•192.168.10.251	1

Hosts Summary (Executive)

.168.10.1 mmary					
Critical	High	Medium	Low	Info	Total
)	0	3	0	33	36
ails					
Severity	Plugin				
Medium (6.4)	51192		Certificate Cannot		
Medium (6.4)	57582	SSL S	Self-Signed Certif	icate	
/ledium (5.0)	97861	Netwo	ork Time Protocol	(NTP) Mode 6 Sca	anner
nfo	10107	HTTP	Server Type and	d Version	
nfo	10114	ICMP	Timestamp Requ	uest Remote Date	Disclosure
nfo	10287	Trace	eroute Information		
nfo	10386	Web	Server No 404 Er	ror Code Check	
nfo	10662	Web	mirroring		
nfo	10863	SSL (Certificate Informa	ation	
nfo	10884	Netwo	ork Time Protocol	(NTP) Server Dete	ection
nfo	11002	DNS	Server Detection		
nfo	11032	Web	Server Directory I	Enumeration	
nfo	11219	Ness	us SYN scanner		
nfo	11935	IPSE	C Internet Key Ex	change (IKE) Vers	ion 1 Detection
nfo	11936	OS Id	lentification		
nfo	19506	Nessi	us Scan Informati	on	
nfo	20094	VMwa	are Virtual Machir	ne Detection	
nfo	21643	SSL (Cipher Suites Sup	pported	
nfo	22964	Servi	ce Detection		
nfo	24260	Hype	rText Transfer Pro	otocol (HTTP) Infor	mation
nfo	25220		IP Timestamps S		
nfo	35716		net Card Manufac		
nfo	42057			ssword Auto-Comp	letion
nfo	42822			ty (STS) Detection	
nfo	45590		non Platform Enu		
	40090	Com	non i lauoim Enu	meration (GFE)	

Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62564	TLS Next Protocols Supported
Info	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	87242	TLS NPN Supported Protocol Enumeration
Info	91634	HyperText Transfer Protocol (HTTP) Redirect Information
Info	91815	Web Application Sitemap

	2.168.10.10 ummary									
	Critical	High		Medi	um	Low	Info		Total	
	3	0		2		0	31		36	
De	etails									
	Severity		Plugin Id		Name					
	Critical (10.0)		53514				ry in DNS Resolu remote check)	tion Cou	uld Allow Rem	ote Code
	Critical (10.0)		72836				ies in DNS Serve uncredentialed ch		Allow Remote	e Code
	Critical (10.0)		97833		(ETERNAL	.BLUE) (ETE	odate for Microso ERNALCHAMPIC (WannaCry) (Et	N) (ETI	ERNALROMA	NCE)
	Medium (6.8)		90510				odate for SAM an incredentialed ch		Remote Prot	ocols
	Medium (5.0)		72837			Vulnerabilit (uncredentia	ry in DNS Server aled check)	Could A	Allow Denial of	Service
	Info		10150		Windows N	letBIOS / SI	MB Remote Host	Informa	ation Disclosur	е
	Info		10287		Traceroute	Information				
	Info		10394		Microsoft V	Vindows SM	IB Log In Possibl	е		
	Info		10736		DCE Service	ces Enumer	ation			
	Info		10785		Microsoft V Disclosure	Vindows SM	IB NativeLanMan	ager Re	emote System	Information
	Info		10884		Network Ti	me Protocol	(NTP) Server De	etection		
	Info		10919		Open Port	Re-check				
	Info		11002		DNS Serve	er Detection				
	Info		11011		Microsoft V	Vindows SM	B Service Detec	tion		
	Info		11219		Nessus SY	N scanner				
	Info		11936		OS Identific	cation				
	Info		12053		Host Fully	Qualified Do	omain Name (FQ	DN) Res	solution	
	Info		19506		Nessus Sc	an Informati	on			
	Info		20094		VMware Vi	rtual Machir	ne Detection			
	Info		20870		LDAP Serv	er Detection	n			
	Info		21745		Authenticat	tion Failure	- Local Checks N	lot Run		
	Info		22964		Service De	tection				

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	35716	Ethernet Card Manufacturer Detection
Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
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)
Info	104410	Host Authentication Failure(s) for Provided Credentials

192.168.10.30 Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3
Details					
Severity	Plugin	ld Name			
Info	19506	Nessus	Scan Informati	on	
Info	20094	VMwar	e Virtual Machir	ne Detection	
Info	35716	Etherno	et Card Manufa	cturer Detection	

192.168.10.51						
Summary						
Critical	High	Medium	Low	Info	Total	
0	0	1	0	20	21	
Details						
Severity	Plugin I	d Name	•			
Medium (5.0)	88098	Apach	ne Server ETag H	Header Informatio	n Disclosure	
Info	10107	HTTP	Server Type and	d Version		
Info	10114	ICMP	Timestamp Req	uest Remote Date	e Disclosure	
Info	10287	Trace	route Informatior	n		
Info	11032	Web S	Server Directory	Enumeration		
Info	11219	Nessu	ıs SYN scanner			
Info	11936	OS Ide	entification			
Info	18261	Apach	ne Banner Linux	Distribution Disclo	osure	
Info	19506	Nessu	ıs Scan Informat	ion		
Info	20094	VMwa	re Virtual Machi	ne Detection		
Info	22964	Servic	ce Detection			
Info	24260	Hyper	Text Transfer Pr	otocol (HTTP) Inf	ormation	
Info	25220	TCP/I	P Timestamps S	upported		
Info	35716	Etherr	net Card Manufa	cturer Detection		
Info	39521	Backp	orted Security P	atch Detection (W	/WW)	
Info	43111	HTTP	Methods Allowe	d (per directory)		
Info	45590	Comm	non Platform Enu	umeration (CPE)		
Info	50344	Missir	ng or Permissive	Content-Security	Policy HTTP Response	e Header
Info	50345	Missir	ng or Permissive	X-Frame-Options	HTTP Response Head	der
Info	54615	Device	e Type			

Web Application Sitemap

Info

91815

100 100 10 50									
192.168.10.52 Summary									
Critical	Hig	h	Med	ium	Low	Info		Total	
0	0		1		0	20		21	
Details									
Severity		Plugin Id		Name					
Medium (5.0)		88098		Apache S	erver ETag H	eader Informati	on Discl	osure	
Info		10107		HTTP Ser	ver Type and	Version			
Info		10114		ICMP Tim	estamp Requ	iest Remote Da	ite Disclo	sure	
Info		10287		Tracerout	e Information				
Info		11032		Web Serv	er Directory E	Enumeration			
Info		11219		Nessus S	YN scanner				
Info		11936		OS Identif	fication				
Info		18261		Apache B	anner Linux D	Distribution Disc	losure		
Info		19506		Nessus S	can Information	on			
Info		20094		VMware V	/irtual Machin	e Detection			
Info		22964		Service D	etection				
Info		24260		HyperTex	t Transfer Pro	otocol (HTTP) Ir	nformatio	n	
Info		25220		TCP/IP Ti	mestamps Su	ipported			
Info		35716		Ethernet (Card Manufac	turer Detection			
Info		39521		Backporte	ed Security Pa	atch Detection (WWW)		
Info		43111		HTTP Met	thods Allowed	d (per directory)			
Info		45590		Common	Platform Enui	meration (CPE)			
Info		50344		Missing or	r Permissive (Content-Securit	y-Policy	HTTP Respo	onse Header
Info		50345		Missing or	r Permissive)	X-Frame-Option	ns HTTP	Response H	leader
Info		54615		Device Ty	rpe				
Info		91815		Web Appl	ication Sitema	ар			

92.168.10.234						
Summary Critical	High		Mediur	n Low	Info	Total
0	0		1	0	38	39
Details				•		**
Severity		Plugin Id	N	lame		
Medium (6.4)		51192	S	SL Certificate Canno	t Be Trusted	
Info		10107	F	ITTP Server Type and	d Version	
Info		10147	N	lessus Server Detecti	on	
Info		10267	S	SH Server Type and	Version Information	n
Info		10863	S	SL Certificate Inform	ation	
Info		10881	S	SH Protocol Versions	Supported	
Info		11032	V	Veb Server Directory	Enumeration	
Info		11936	C	S Identification		
Info		12053	H	lost Fully Qualified Do	omain Name (FQDI	N) Resolution
Info		12634	А	uthenticated Check:	OS Name and Inst	alled Package Enumeration
Info		14272	N	letstat Portscanner (S	SSH)	
Info		19506	Ν	lessus Scan Informat	ion	
Info		20094	V	Mware Virtual Machin	ne Detection	
Info		21643	S	SL Cipher Suites Su	pported	
Info		21745	А	uthentication Failure	- Local Checks Not	Run
Info		22964	S	ervice Detection		
Info		24260	H	lyperText Transfer Pr	otocol (HTTP) Infor	mation
Info		25202	E	numerate IPv6 Interfa	aces via SSH	
Info		25203	E	numerate IPv4 Interfa	aces via SSH	
Info		25221	R	temote listeners enun	neration (Linux / Alz	X)
Info		33276	E	numerate MAC Addr	esses via SSH	
Info		34098	В	IOS version (SSH)		
Info		35351	S	ystem Information Er	numeration (via DM	1)
Info		35716	E	thernet Card Manufa	cturer Detection	
Info		45432	Р	rocessor Information	(via DMI)	
Info		45433	N	lemory Information (v	ia DMI)	

Info	45590	Common Platform Enumeration (CPE)
Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
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	91815	Web Application Sitemap
Info	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

192.168.10.245 Summary	5					
Critical	High	Medium	Low	Info	Total	
0	0	0	0	3	3	
Details						
Severity	Plugi	in Id Name				
Info	1950	6 Nessu	ıs Scan Informati	on		
Info	2009	4 VMwa	re Virtual Machir	ne Detection		
Info	3571	6 Etherr	net Card Manufac	cturer Detection		

192.168.10.25 Summary	i1							
Critical	High	Me	edium	Low	Info	Total		
0	0	0		0	19	19		
Details								
Severity	PI	ugin ld	Name					
Info	10)114	ICMP Tir	nestamp Req	uest Remote Date	Disclosure		
Info	10	267	SSH Ser	ver Type and	Version Information	on		
Info	10	287	Tracerou	ite Information	n			
Info	10)881	SSH Pro	tocol Version	s Supported			
Info	11	219	Nessus S	SYN scanner				
Info	11	819	TFTP Da	nemon Detect	ion			
Info	11	936	OS Ident	S Identification				
Info	19	9506	Nessus S	Scan Informat	ion			
Info	20	0094	VMware	Virtual Machi	ne Detection			
Info	21	745	Authentic	cation Failure	- Local Checks No	ot Run		
Info	22	2964	Service [Detection				
Info	25	5220	TCP/IP T	imestamps S	supported			
Info	35	5716	Ethernet	Card Manufa	cturer Detection			
Info	39	9520	Backport	ed Security F	atch Detection (SS	SH)		
Info	45	5590	Common	Platform En	umeration (CPE)			
Info	54	615	Device T	ype				
Info	66	3717	mDNS D	etection (Loc	al Network)			
Info	70	0657	SSH Algo	orithms and L	anguages Support	ed		
Info	10)4410	Host Aut	hentication Fa	ailure(s) for Provide	ed Credentials		