Trustwave[®]

DATA SHEET

Trustwave Vulnerability Management

STAY AHEAD OF NETWORK VULNERABILITIES

Benefits

- Increase visibility by identifying your IT assets and associated vulnerabilities
- Leverage expertise and intelligence gathered by the SpiderLabs research team
- Save time and resources when remediating vulnerabilities with prioritized results
- Supplement your team with managed scanning and testing services from SpiderLabs

For most organizations today, running applications and databases on their IT network is a big part of running their business. Knowing their IT network is susceptible to vulnerabilities such as software flaws and configuration issues, security professionals need to identify, classify, remediate or mitigate the vulnerabilities that attackers could successfully exploit to access valuable data.

Get the Complete Picture

Trustwave Vulnerability Management provides IT and security professionals with insight into their network vulnerabilities and exposure to attack and/or compromise from outside and inside the corporate firewall. This helps customers meet both IT security objectives – such as protecting confidential data and ensuring the integrity and availability of IT systems – and compliance goals, including auditing security controls to safeguard sensitive information.

External Vulnerability Scanning

Regularly scheduled or ad-hoc in-the-cloud, external scanning offers insight into what vulnerabilities are being exposed through your firewall to the outside world. Regular vulnerability updates are provided by the SpiderLabs Security Research Team.

Internal Vulnerability Scanning

Internal scanning offers the same industry leading vulnerability technology as external scanning, providing you with a hacker's view of vulnerabilities inside the network behind your firewall.

Trustwave Vulnerability Management is available as a self-service application or as a managed scanning service, part of Trustwave Managed Security Testing service.

	Vulner	abilities	ies Asset Inventory		Targets	Live He	ost Disco	(
	Exception R	escan Co	mpare	Generate Report	Columns	Export	2 Refres	,		Q _v All Values	
Status	IP	Vuln	erability Na	ime		Pro	tocol	Port	Severity	CVE	
]	10.70.33.14	Nokia	IPSO Defa	ult Credentials		tcp		23			
]	10.70.33.14	Nokia	Voyager V	Veb Management Int	erface Guessed	tcp		443			
]	10.70.33.14	Gues	able SNMF	Community String		udp		161		CVE-1999-051	7, CVE-
]	10.70.33.14	Unsuj	ported Ve	rsion of Nokia/Check	point IPSO	-		-			
]	10.70.33.14	Unen	rypted Co	mmunication Channe	el Accessibility	tcp		23			
]	10.70.33.14	SSL 0	ertificate B	Expired		tcp		443			
1	10.70.33.14	SSL (ertificate P	Public Key Too Small		tcp		443			
											(a)
Details Evi	dence (1)	Exception			Page 1 of 1						
Guessable S	SNMP Commun										
	High <u>CVE-1999-05</u> <u>CVE-1999-07</u>	17 CVE-1999	0147 CVE	-1999-0254 CVE-195 -2001-0380 CVE-200 -2004-1474 CVE-201	9-0508 CVE-1999						
Guessable S Severity	High CVE-1999-05 CVE-1999-07 CVE-2002-04 SNMP is a pro- The commun Although only (configuration	17 CVE-1999 92 CVE-2000 78 CVE-2002 otocol used for thy string (ess r the "read" (a) string is als a able to mon	-0147 CVE -1229 CVE r remote n entially, th nonitoring) o guessabl tor or reco	-2001-0380 CVE-200	9-0508 CVE-1999 11-0514 CVE-200 0-1574 uration of networ SNMP service w his probably mea	-1210 CVE-2 devices and s easily gues that the "w nity strings fo	servers. sed. rite" r this				
Guessable S Severity CVE	NMP Commun High CVE-1999-05 CVE-1999-02 CVE-2002-04 SNMP is a pri The commun Although only (configuration device will be service to yo a At a minimum	12 CVE-1999 32 CVE-2000 78 CVE-2000 78 CVE-2002 stocol used for thy string (ess able to mon ur system or n, you should s. If SNMP is 1	-0147 CVE -1229 CVE r remote n entially, th monitoring) o guessabl tor or reco network. change yo iot require	-2001-0380 CVE-200 -2004-1474 CVE-201 nonitoring and config e password) for your e string was tested, it le. An attacker who le nfigure the device, p ur read and write co d, you should disable	19-0508 CVE-1999 12-0514 CVE-2003 0-1574 uration of networ SNMP service wa his probably measure nows the commu otentially leading mmunity strings t	-1210 CVE-2 c devices and s easily gues is that the "winity strings fo to a serious c o something t	servers. sed. rite" r this lenial of hat is				

With prioritized scan results and actionable report details, Trustwave Vulnerability Management helps you find and fix vulnerabilities faster.

Comprehensive Scanning Services from the Experts

Managed Security Testing from Trustwave SpiderLabs® allows IT and information security teams to take a programmatic approach to vulnerability management through managed vulnerability scanning across databases, networks and applications, as well as, in-depth manual penetration testing of networks and applications.

With a comprehensive menu of services and multiple levels of testing that get increasingly advanced, Trustwave offers the flexibility for organizations to choose the level of testing that best supports their business. Scans and tests are performed by SpiderLabs experts and a report with validated results is shared with the customer.

Self-Service Support

Users of self-service scanning can schedule, configure and run scans themselves via Trustwave's award-winning secure TrustKeeper web portal. Upon completion of a scan, the user receives a list of raw results from Trustwave Vulnerability Management that they interpret on their own.

The TrustKeeper web portal also gives users access to:

- Summaries Dashboard views of scan results including trending analysis
- Flexibility Support for multiple scan types, including light inventory and full vulnerability scanning
- Visibility Multiple scan profiles for varying visibility needs by network location
- Reporting General vulnerability and compliance-based reporting
- Alerts Customizable notifications including upcoming scans, scan kickoffs and completion

About Trustwave SpiderLabs®

Expertise

Our team consists of many of the top security professionals in the world. With career experience ranging from corporate security executives to security research labs as well as federal and local law enforcement, our team has the expertise and dedication to stay ahead of the issues and threats affecting your organization's security posture.

Experience

We have performed thousands of incident response and forensic investigations as well as application and network security penetration tests for customers around the globe — from startups to Fortune 50 companies.

Facilities

We maintain the most advanced security testing and research labs in the industry — located in every region across the globe to deliver the best quality of service to you.

Confidentiality

We work closely with you to ensure that all our services are performed with strict confidentiality and under rigorous legal oversight.

Sca	nning		Sca	Scan Overview Configuration			on Reports Disputes		Exce	ptions	Notificat	ions	Account	
	no s'	ystem notifications			External Targets	108/	1000 Scans 6	3/500 Licens	e Expires		mer: ⊤	/M_Parer	t Change Customer	Support & Help
+ Nev		Scan Now Delete	edit	Clone	O isable	Columi		Global	Confi	guration D	etails			
۵	Config	uration Name	Status		Scan Type		Schedule	Next Scan						
	Military	TimeViaConfig-AM	Enabled		PCI Scan		Monthly	2015-08-23		Configurati	on Name	BlackO	utPageTesting-1	
	Military	TimeWithBlkOutViaConfi	Enabled		PCI Scan		Monthly	2015-08-23			Scanner		al Scapper	
	Par 4-2	3-2013	Enabled		Vulnerability Scan		Monthly	2015-08-23						
	BlackO	utPageTesting-1	Enabled		PCI Scan		Monthly	2015-08-24	•		can Type	PCI Sci		
	Parent	Full 2	Enabled		Vulnerability Scan		Quarterly	2015-10-24			Schedule		on the 24th at 10:48 fro	
	Config	test	Enabled		Vulnerability Scan		Immediate			8	lackouts	Annual	ly 10-23 to 10-24 M - 10	:00 to 12:00
	config t	est without config expor	Enabled		Vulnerability Scan		Immediate					More		
	config t	est2	Enabled		Vulnerability Scan		Immediate				Targets	10.70.2		
	no conf	ig test	Enabled		Vulnerability Scan		Immediate			Fx	clusions	10.70.3		
	parent-		Enabled		Live Host Discovery		Immediate			Last Comple				
		Inventory	Enabled		Port Service Fingerpi		Immediate		1	caas compie	ico scan	1015-0		
					Displaying 13		1.20							

It's quick and easy to configure scans and view their status through the TrustKeeper web portal



041

ξ