Network Vulnerability Report

May 25, 2017 at 11:14 AM

This report provides detailed information about all the vulnerabilities that were successfully exploited by Core Impact during this test. Each one of the reported vulnerabilities was actively exploited in order to obtain control, elevate privileges or obtain information about the vulnerable host. None of these results are potential, all of them were practically tested as part of this test.

This information provides a practical approach to determine the key vulnerable points in the tested network, and to assess the risk associated with such vulnerabilities.

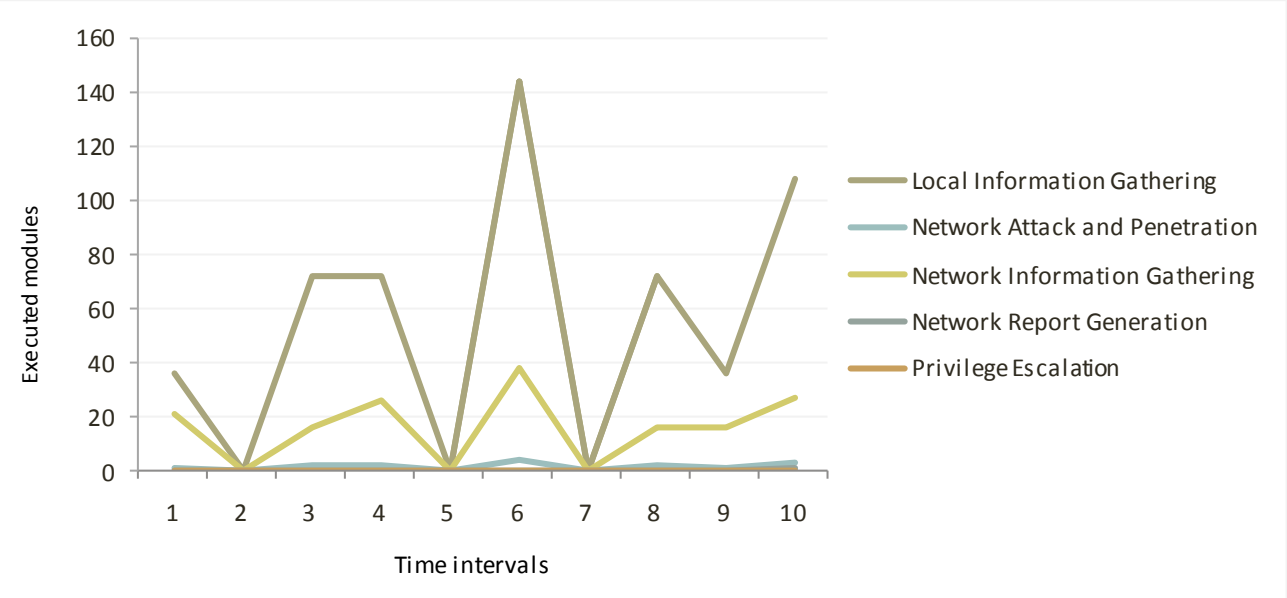
Workspace(s) information

Name	Company/Test Area	Started	Finished	Exact Time	Running Time
Demo		04/24/17 01:06 PM	05/25/17 11:14 AM	30d 22h 8m 3s	21h 0m 54s

Effort chart

The chart report lifespan was divided into 10 time intervals, time interval 1 begins when the first task started, and time interval 10 ends when the last task finished running.

Distribution of modules in time



Summary

Risks

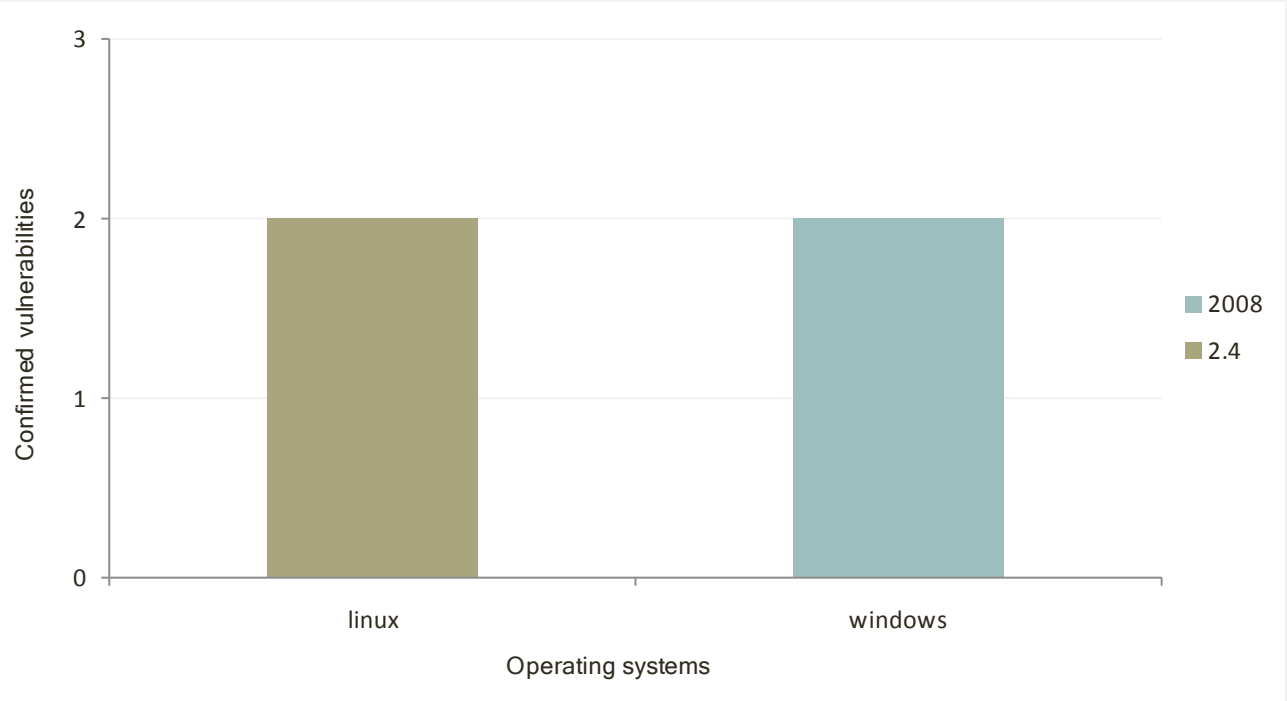
Vulnerabilities	Total
Successfully exploited	4
Total agents installed	5
Unique vulnerabilities successfully exploited	4

General

Effort	Total
Modules run	85

Confirmed vulnerabilities

Confirmed vulnerabilities per operating system version

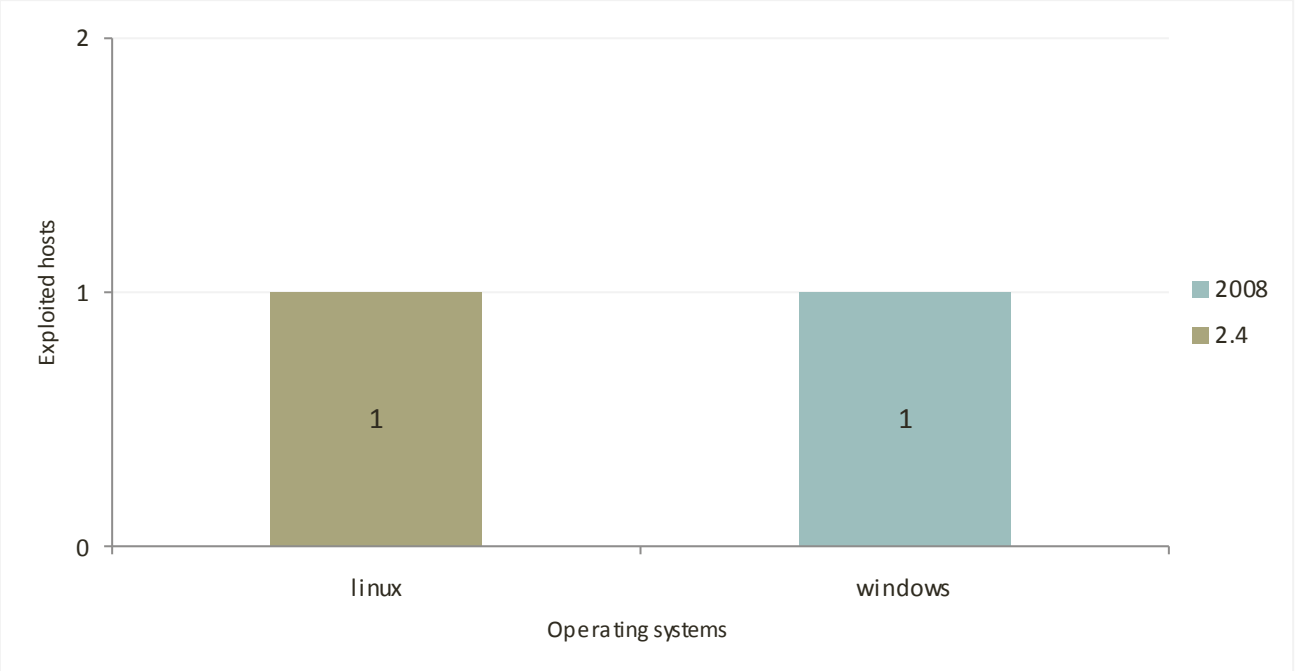


At most ten vulnerabilities are shown, and ties with the last shown vulnerability are not included.

Vulnerability	Module Name	CVSS Score	Affected
CVE-2003-0545	Apache - OpenSSL ASN.1 deallocation exploit	10	1
CVE-1999-0518	SMB Identity Verifier	7.5	1
CVE-1999-0503	SMB Identity Verifier	7.2	1
CVE-2003-0961	Linux kernel do_brk() exploit	7.2	1

Exploited hosts

Compromised hosts per operating system version



At most ten host are shown, and ties with the last shown hosts are not included.

Workspace	Visibility Path	Host Name	CVSS Score	Vulnerabilities
Demo	/192.168.123.11	192.168.123.11	10	1
Demo	/192.168.123.77	win12377	7.5	1
Demo	/192.168.123.11	192.168.123.11	7.2	1
Demo	/192.168.123.77	win12377	7.2	1

Critical vulnerabilities

At most ten vulnerabilities are shown, and ties with the last shown vulnerability are not included.

Vulnerability	Module Name	CVSS Score
CVE-2003-0545	Apache - OpenSSL ASN.1 deallocation exploit	10
CVE-1999-0518	SMB Identity Verifier	7.5
CVE-1999-0503	SMB Identity Verifier	7.2
CVE-2003-0961	Linux kernel do_brk() exploit	7.2

Vulnerabilities

Workspace	Visibility Path	Host Name	Vulnerability Identifier	CVSS	Vector Description	Vulnerability Description	Affected Port	Module Name	Remediation URL
Demo	/192.168.123.11	192.168.123.11	CVE-2003-0545	10	Access Vector: Network exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Complete), Integrity Impact: Allows unauthorized modification (Complete), Availability Impact: Allows disruption of service (Complete)	Double free vulnerability in OpenSSL 0.9.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding.	443	Apache - OpenSSL ASN.1 deallocation exploit	http://www.securityfocus.com/bid/8732/solution
Demo	/192.168.123.11	192.168.123.11	CVE-2003-0961	7.2	Access Vector: Locally exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Complete), Integrity Impact: Allows unauthorized modification (Complete), Availability Impact: Allows disruption of service (Complete)	Integer overflow in the do_brk function for the brk system call in Linux kernel 2.4.22 and earlier allows local users to gain root privileges.	Unknown	Linux kernel do_brk() exploit	
Demo	/192.168.123.77	win12377	CVE-1999-0503	7.2	Access Vector: Locally exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Complete), Integrity Impact: Allows unauthorized modification (Complete), Availability Impact: Allows disruption of service (Complete)	A Windows NT local user or administrator account has a guessable password.	445	SMB Identity Verifier	

Demo	/192.168.123.77	win12377	CVE-1999-0518	7.5	Access Vector: Network exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Partial), Integrity Impact: Allows unauthorized modification (Partial), Availability Impact: Allows disruption of service (Partial)	A NETBIOS/SMB share password is guessable.	445	SMB Identity Verifier

Vulnerabilities container details

Workspace Name	Visibility Path	CVE	Container	1st Key	1st Value	2nd Key	2nd Value	3rd Key	3rd Value	4th Key	4th Value
Demo	/192.168.123.77	CVE-1999-0503	Identities	0		Password	AitbISP4eCiG				
Demo	/192.168.123.77	CVE-1999-0503	Identities	0		Username	admin				
Demo	/192.168.123.77	CVE-1999-0503	Identities	17		NTLM hash	aad3b435b5140 4eeaad3b435b5 1404ee:906a58 a75fb3012bcc6 41ff7feac582b				
Demo	/192.168.123.77	CVE-1999-0503	Identities	17		Username	admin				
Demo	/192.168.123.77	CVE-1999-0503	Identities	18		NTLM hash	aad3b435b5140 4eeaad3b435b5 1404ee:40aceb ee455d4a49e6e ad6bd4c47da06				
Demo	/192.168.123.77	CVE-1999-0503	Identities	18		Username	Backdoor				
Demo	/192.168.123.77	CVE-1999-0518	Identities	0		Password	AitbISP4eCiG				
Demo	/192.168.123.77	CVE-1999-0518	Identities	0		Username	admin				
Demo	/192.168.123.77	CVE-1999-0518	Identities	17		NTLM hash	aad3b435b5140 4eeaad3b435b5 1404ee:906a58 a75fb3012bcc6 41ff7feac582b				
Demo	/192.168.123.77	CVE-1999-0518	Identities	17		Username	admin				
Demo	/192.168.123.77	CVE-1999-0518	Identities	18		NTLM hash	aad3b435b5140 4eeaad3b435b5 1404ee:40aceb ee455d4a49e6e ad6bd4c47da06				
Demo	/192.168.123.77	CVE-1999-0518	Identities	18		Username	Backdoor				

Vulnerabilities extra links

Workspace Name	CVE	URL
Demo	CVE-1999-0503	http://xforce.iss.net/static/1328.php
Demo	CVE-1999-0503	http://xforce.iss.net/static/282.php
Demo	CVE-1999-0518	http://xforce.iss.net/static/182.php
Demo	CVE-2003-0545	http://oval.mitre.org/oval/definitions/data/oval2590.html
Demo	CVE-2003-0545	http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2590
Demo	CVE-2003-0545	http://secunia.com/advisories/22249
Demo	CVE-2003-0545	http://www.cert.org/advisories/CA-2003-26.html
Demo	CVE-2003-0545	http://www.debian.org/security/2003/dsa-394
Demo	CVE-2003-0545	http://www.frsirt.com/english/advisories/2006/3900
Demo	CVE-2003-0545	http://www.kb.cert.org/vuls/id/935264
Demo	CVE-2003-0545	http://www.redhat.com/support/errata/RHSA-2003-292.html
Demo	CVE-2003-0545	http://www.securityfocus.com/bid/8732
Demo	CVE-2003-0545	http://www.securityfocus.com/bid/8732/solution
Demo	CVE-2003-0545	http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm
Demo	CVE-2003-0545	http://www.vupen.com/english/advisories/2006/3900
Demo	CVE-2003-0545	http://www-1.ibm.com/support/docview.wss?uid=swg21247112
Demo	CVE-2003-0961	http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000796
Demo	CVE-2003-0961	http://isec.pl/papers/linux_kernel_do_brk.pdf
Demo	CVE-2003-0961	http://marc.theaimsgroup.com/?l=bugtraq&m=107064798706473&w=2
Demo	CVE-2003-0961	http://marc.theaimsgroup.com/?l=bugtraq&m=107064830206816&w=2
Demo	CVE-2003-0961	http://marc.theaimsgroup.com/?l=bugtraq&m=107394143105081&w=2
Demo	CVE-2003-0961	http://secunia.com/advisories/10328
Demo	CVE-2003-0961	http://secunia.com/advisories/10329
Demo	CVE-2003-0961	http://secunia.com/advisories/10330
Demo	CVE-2003-0961	http://secunia.com/advisories/10333
Demo	CVE-2003-0961	http://secunia.com/advisories/10338
Demo	CVE-2003-0961	http://www.debian.org/security/2003/dsa-403
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-417
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-423
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-433
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-439
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-440
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-442
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-450
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-470
Demo	CVE-2003-0961	http://www.debian.org/security/2004/dsa-475
Demo	CVE-2003-0961	http://www.kb.cert.org/vuls/id/301156
Demo	CVE-2003-0961	http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:110
Demo	CVE-2003-0961	http://www.mandriva.com/security/advisories?name=MDKSA-2003:110
Demo	CVE-2003-0961	http://www.novell.com/linux/security/advisories/2003_049_kernel.html
Demo	CVE-2003-0961	http://www.redhat.com/support/errata/RHSA-2003-368.html
Demo	CVE-2003-0961	http://www.redhat.com/support/errata/RHSA-2003-389.html