Network Executive Report

January 13, 2017 at 3:59 PM

This report produces an overall summary of the tests performed and results found for the Network Security Risk Assessment carried out by Core Impact. It contains the summary of risks that were identified in targeted hosts and identities that were tested.

Workspace(s) information

Name	Company/Test Area	Started	Finished	Exact Time	Running Time
Demo		01/13/17 12:08 PM	01/13/17 03:59 PM	3h 50m 50s	23m 51s

Summary

Risks

Vulnerabilities	Total
Successfully exploited	4
Agents installed	4
Unique vulnerabilities successfully exploited	4

Exposures	Total
Found	0

Assets

Hosts	Total
Found	18
At Risk (confirmed vulnerabilities or exposures)	2
Compromised (at least one agent installed)	2

Cameras	Total
Found	0
At Risk (confirmed vulnerabilities)	0

Mobiles	Total
Found	0
Android mobiles found	0
BlackBerry mobiles found	0
iOS mobiles found	0

Wireless	Total
Access Point found	0
Stations found	0

Identities

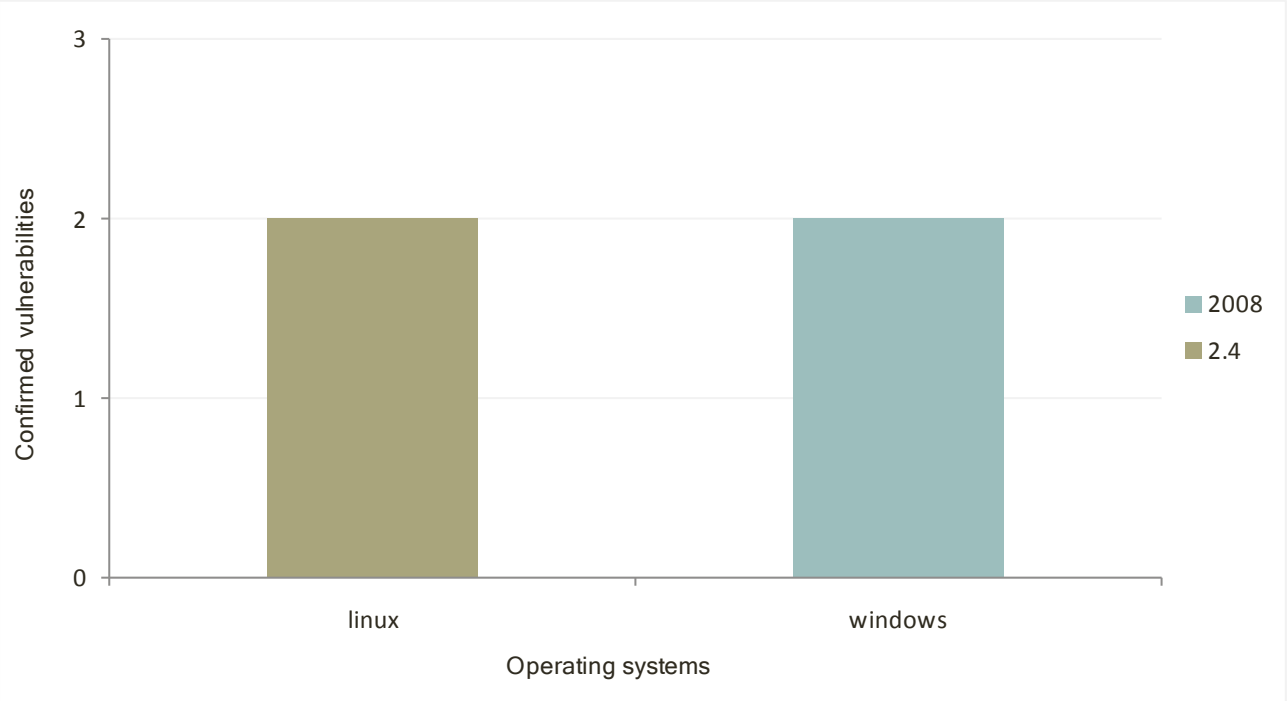
Identities	Total
Tested	206
Validated	22
Agents installed	1

General

Effort	Total
Modules run (vulnerabilities)	8
Modules run (exposures)	0

Confirmed vulnerabilities

Confirmed vulnerabilities per operating system version

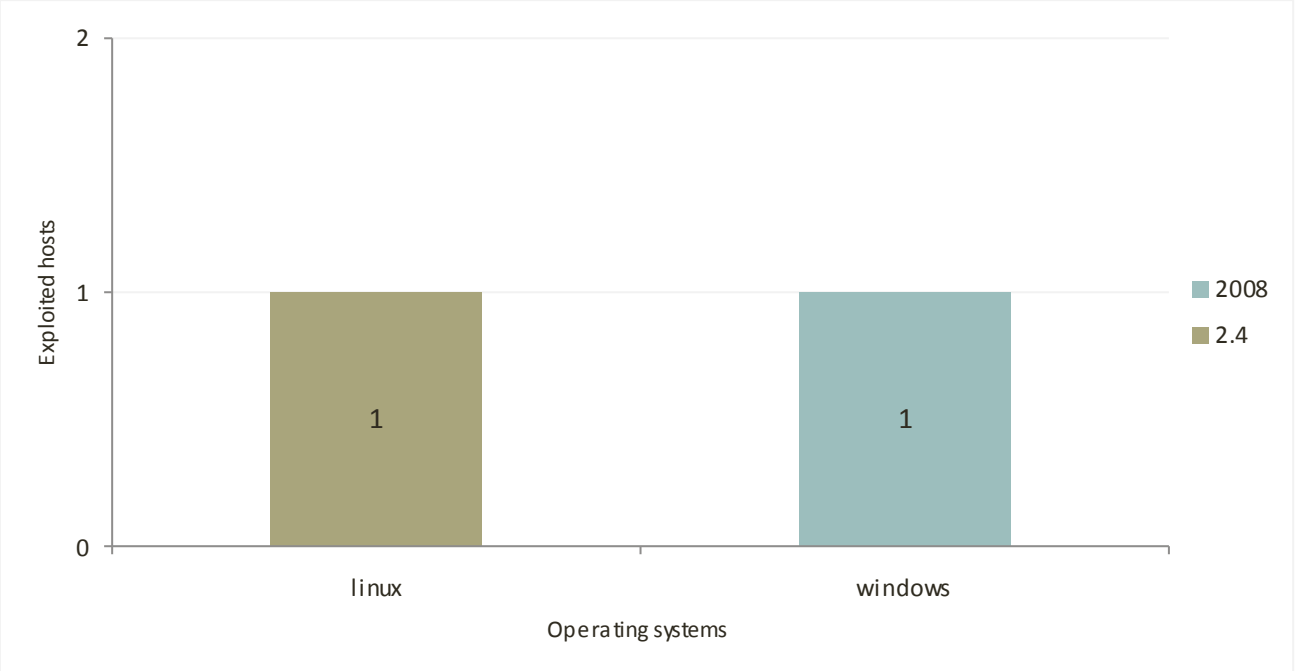


At most ten vulnerabilities are shown, and ties with the last shown vulnerability are not included.

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

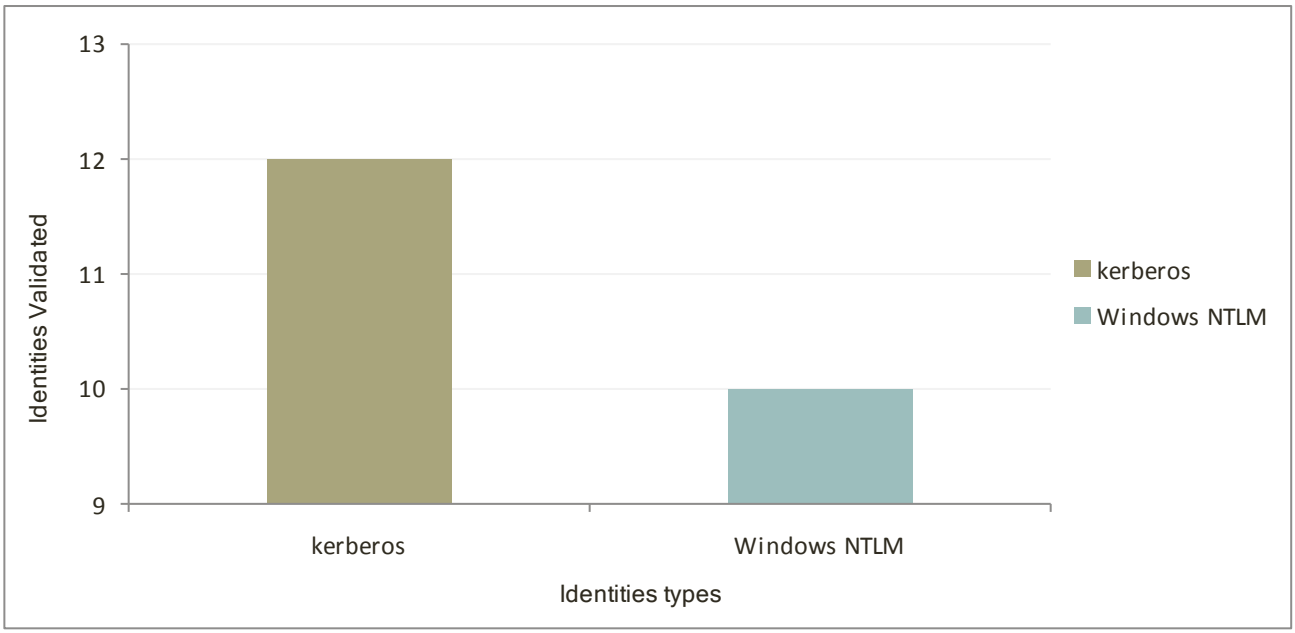
Critical vulnerabilities

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

Identities types

Identities validated categorized by type



At most ten types of validated identities are shown

Type	Identities
kerberos	12
Windows NTLM	10

Most validated identities

At most ten identities grouped by user name are shown

Username	Hosts in
jim	8
WIN12377$	5
admin	2
win12377$	2
Administrator	1
Backdoor	1
Guest	1
IUSR_WIN-JFACNQKQSUS	1
joe@FREEFLY.NET	1

Most gathered identities

At most ten identities gathered grouped by user name are shown

Username	Hosts in
jim	8
WIN12377$	5
admin	2
Administrator	2
Backdoor	2
Guest	2
IUSR_WIN-JFACNQKQSUS	2
win12377$	2
joe@FREEFLY.NET	1

Hosts with more amount of validated identities

At most ten hosts with validated identities

Workspace	Visibility Path	Host Name	Identities
Demo	/192.168.123.77	win12377	22