Network Report

January 13, 2017 at 4:00 PM

This report provides detailed information about network assets and risks found. This information provides a practical approach to determine the key vulnerable points in the tested network, and to assess the risk associated with them.

Vulnerabilities found that were successfully exploited are summarized and detailed along with any exposures or identities found during this test, if exposure or identity testing checks were enabled.

This report also provides detailed information about network assets found like hosts, cameras, mobiles, access points and stations.

Each one of the reported vulnerabilities was actively exploited in order to obtain control, elevate privileges or obtain information about the vulnerable assets. None of these results are potential; all of them were practically tested as part of this test.
Exposures are system configuration issues that allow access to information that can be used as a stepping-stone towards gaining access to the systems themselves.
Identities that were guessable or using default passwords may also have been identified. These represent an additional avenue by which data can be lost or a foothold gained in the target network.

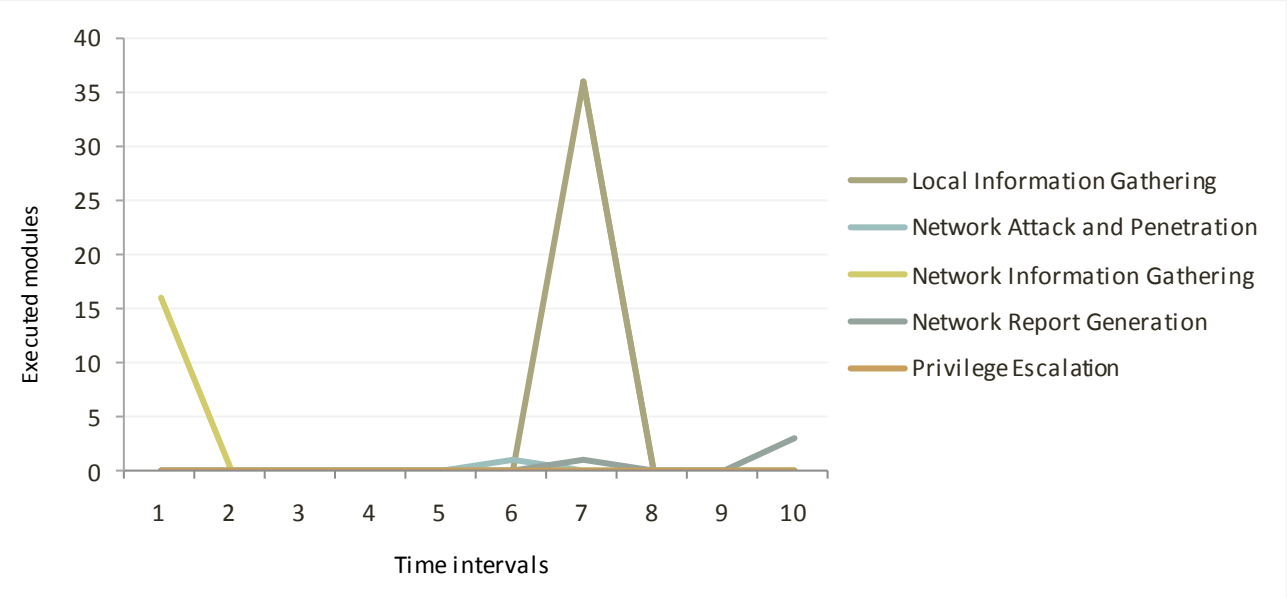
Workspace(s) information

Name	Company/Test Area	Started	Finished	Exact Time	Running Time
Demo		01/13/17 12:08 PM	01/13/17 03:59 PM	3h 51m 28s	23m 52s

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
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

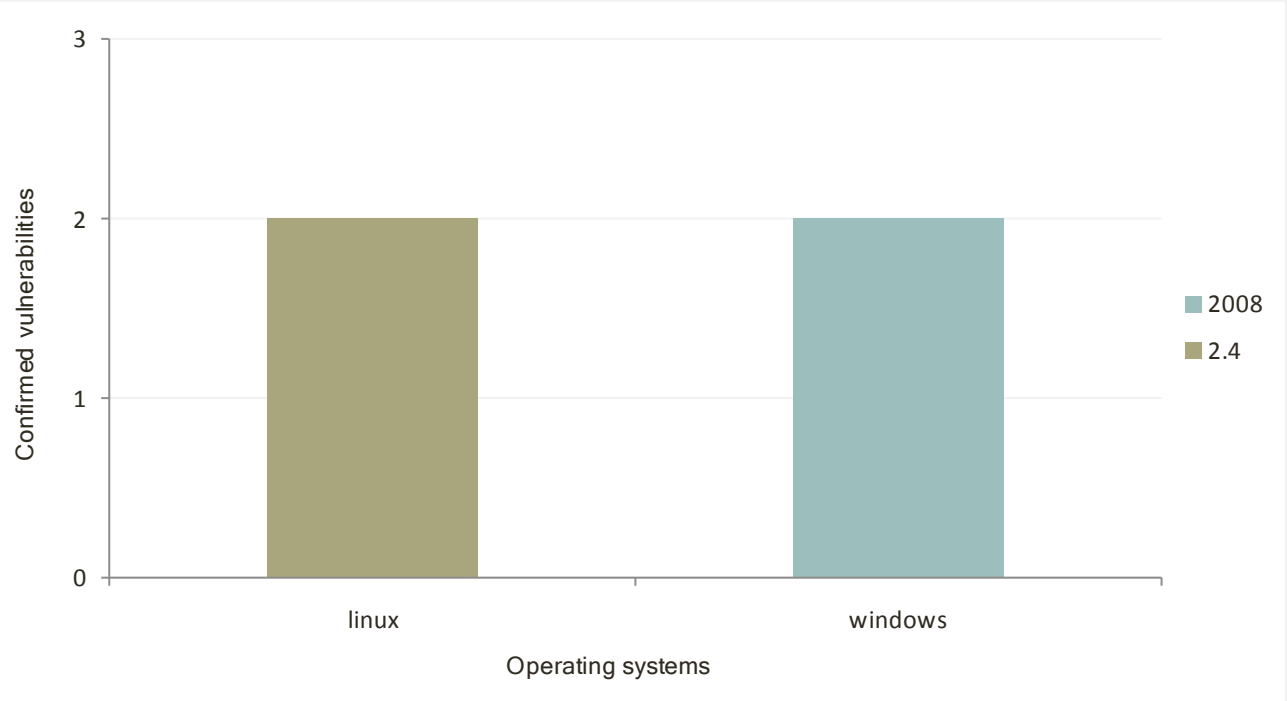
Identities	Total
Tested	206
Validated	22
Agents installed	1

General

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

Confirmed vulnerabilities

Confirmed vulnerabilities per operating system version

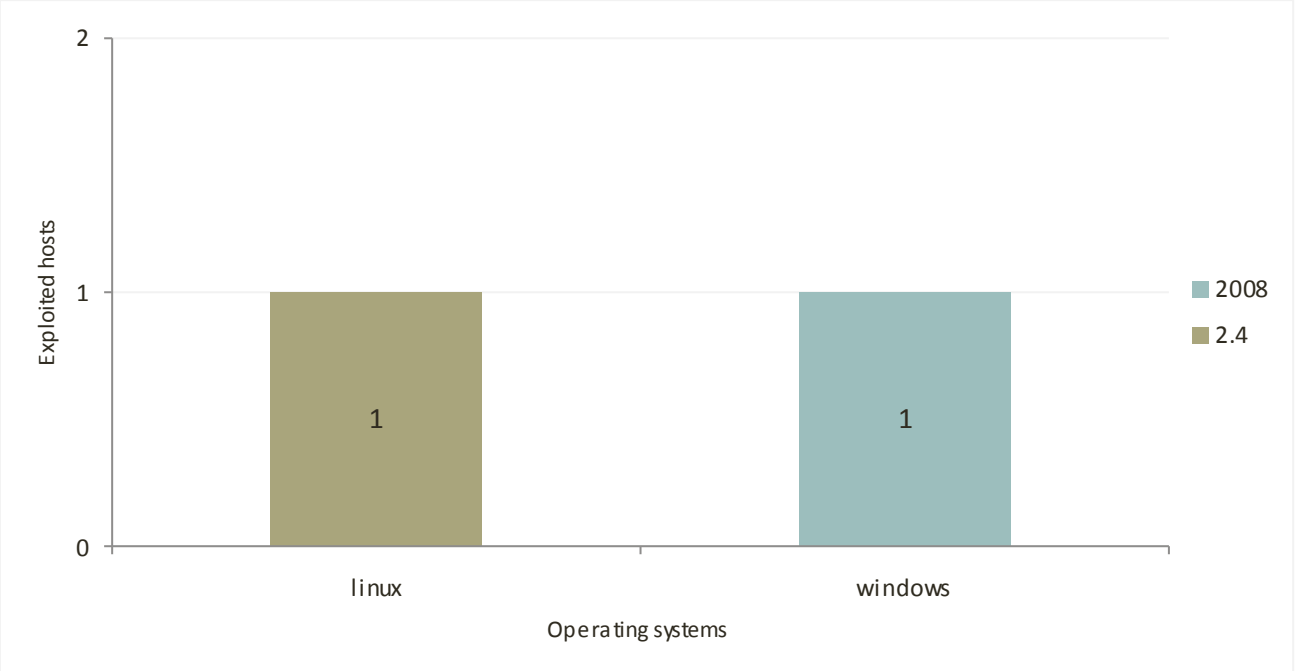


At most ten vulnerabilities are shown, and ties with the last shown vulnerability are not included.

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

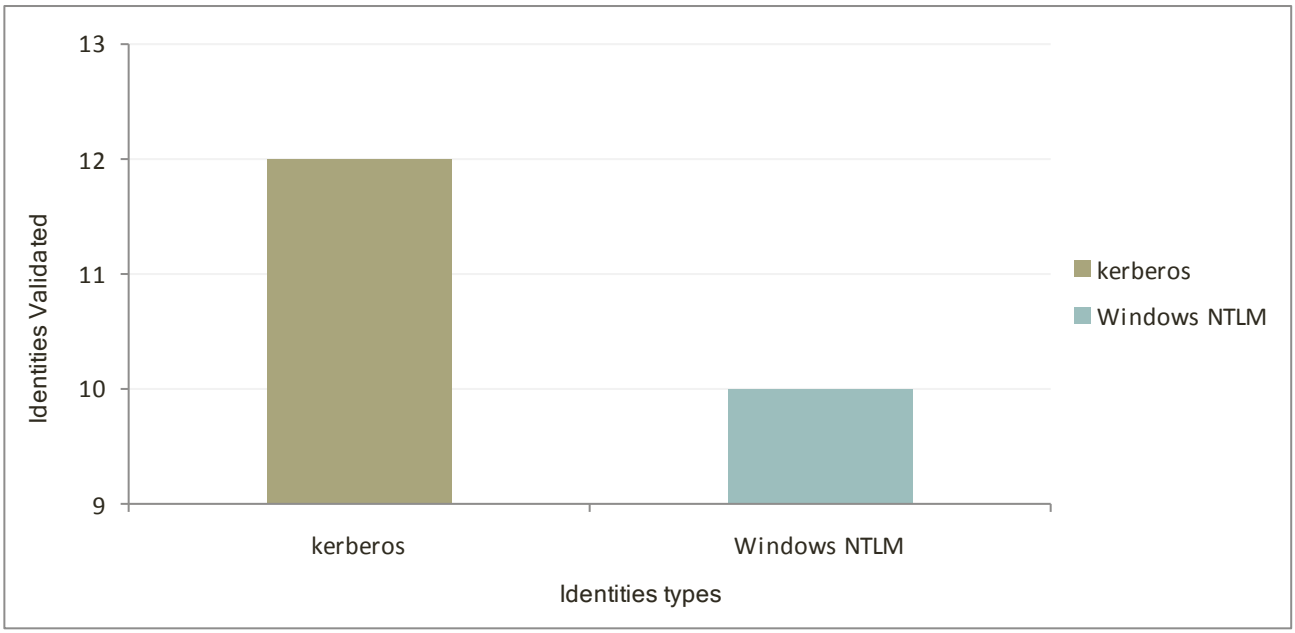
Critical vulnerabilities

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

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

Hosts

Workspace	Visibility Path	Host Name	IP	Architecture	OS Name	Version	Edition	SP	Distribution	Additional Info	Last Snapshot
Demo	/192.168.123.100	FREEFLY-DC	192.168.123.100	x86-64	windows	2012R2	Standard	unknown			
Demo	/192.168.123.11	192.168.123.11	192.168.123.11	i386	linux				unknown		
Demo	/192.168.123.55	192.168.123.55	192.168.123.55	i386	windows	XP	unknown	2			
Demo	/192.168.123.77	win12377	192.168.123.77	i386	windows	2008	Standard	1			C:/Users/User/AppData/Roaming/IMPACT/components/modules/classic/install/Reports/win12377_Jan_13_2017_14_29_21.bmp
Demo	/192.168.123.77/10.1.16.1	10.1.16.1	10.1.16.1	Unknown	unknown						
Demo	/192.168.123.77/10.1.16.11	10.1.16.11	10.1.16.11	Unknown	unknown						
Demo	/192.168.123.77/10.1.16.21	10.1.16.21	10.1.16.21	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.1	192.168.123.1	192.168.123.1	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.100	192.168.123.100	192.168.123.100	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.11	192.168.123.11	192.168.123.11	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.120	192.168.123.120	192.168.123.120	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.200	192.168.123.200	192.168.123.200	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.22	192.168.123.22	192.168.123.22	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.33	192.168.123.33	192.168.123.33	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.44	192.168.123.44	192.168.123.44	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.55	192.168.123.55	192.168.123.55	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.66	192.168.123.66	192.168.123.66	Unknown	unknown						
Demo	/192.168.123.77/192.168.123.77	192.168.123.77	192.168.123.77	Unknown	unknown						

Identities

Workspace	Visibility Path	Host Name	ID	Validated	Protocol	Username	Password	Domain	Module Name	Source Host	Valid on	Comment
Demo	/192.168.123.77	win12377	0	true	Windows NTLM	admin	AitbISP4eCiG				/192.168.123.77	
Demo	/192.168.123.77	win12377	1	false	None	admin			Get Users and Groups	/192.168.123.77		
Demo	/192.168.123.77	win12377	10	true	Windows NTLM	IUSR_WIN-JFACNQKQSUS			Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	11	true	Windows NTLM	jim	s3cr3t!	FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	12	true	Windows NTLM	jim	s3cr3t!	FREEFLY	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	13	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	14	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	15	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	16	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	17	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	18	true	kerberos	WIN12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	19	true	kerberos	WIN12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	2	false	None	Administrator			Get Users and Groups	/192.168.123.77		
Demo	/192.168.123.77	win12377	20	true	kerberos	WIN12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	21	true	kerberos	WIN12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	22	true	kerberos	win12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	23	true	kerberos	win12377$		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	24	true	kerberos	jim		FREEFLY.NET	Mimikatz	/192.168.123.77	/192.168.123.77	
Demo	/192.168.123.77	win12377	25	true	Windows NTLM	WIN12377$		FREEFLY	Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77	

Demo	/192.168.123.77	win12377	26	true	Windows NTLM	joe@FREEFLY.NET	C0mpl3xP2ssw0rd!	Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77
Demo	/192.168.123.77	win12377	3	false	None	Backdoor		Get Users and Groups	/192.168.123.77	
Demo	/192.168.123.77	win12377	4	false	None	Guest		Get Users and Groups	/192.168.123.77	
Demo	/192.168.123.77	win12377	5	false	None	IUSR_WIN-JFACNQKQSUS		Get Users and Groups	/192.168.123.77	
Demo	/192.168.123.77	win12377	6	true	Windows NTLM	admin		Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77
Demo	/192.168.123.77	win12377	7	true	Windows NTLM	Backdoor		Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77
Demo	/192.168.123.77	win12377	8	true	Windows NTLM	Administrator		Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77
Demo	/192.168.123.77	win12377	9	true	Windows NTLM	Guest		Windows Secrets Dump (L)	/192.168.123.77	/192.168.123.77