

TECHNOLOGY INTEGRATION PROJECT

MAY 4, 2006

ROB HILTBRAND

***A Comparison of Proprietary
and Open Source Software as
a Way to Maintain Availability
in an Open Access
Environment***

www.ProjectWhiteHat.org

SPONSORING ORGANIZATION

- *TECHNOLOGY FOR ALL* (TFA) IS A 501(c) (3) NON-PROFIT ORGANIZATION WHOSE MISSION IS TO EMPOWER UNDER-RESOURCED COMMUNITIES THROUGH THE TOOLS OF TECHNOLOGY.
- *MISSION MILBY* COMMUNITY TECHNOLOGY CENTER (CTC)
- *WILL REED*, PRESIDENT
- *JIM FORREST*, BUSINESS DEVELOPMENT OFFICE & PROJECT SPONSOR
- *NIKKI PAYNE*, LAB MONITOR



OVERVIEW OF COMPUTER SECURITY

- COMPUTER SECURITY RESTS ON *CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY.*
- OPEN ACCESS ENVIRONMENTS AND “UNTRUSTED USERS”

COMMON THREATS & VULNERABILITIES

- *250,000*
- *9,163*
- *1,000*
- *49*
- *11.9*

LiveCD

- A LiveCD IS AN OPERATING SYSTEM & APPLICATIONS STORED ON A *BOOTABLE* COMPACT DISC (CD)
- THE LiveCD CREATS A *RAMDISK* WITHIN THE RANDOM ACCESS MEMORY (RAM) WHERE THE OS & APP FILES "RUN"
- A CLIENT SYSTEM CAN BE RETURNED TO ITS *ORIGINAL STATE* BY REBOOTING THE PC AND EJECTING THE CD

METHODOLOGY

- EXPERIMENTATION
- HOST INTEGRITY
- CORPORATE COMPUTER FORENSICS
- FOR CORPORATE INVESTIGATORS
AVAILABILITY OF SERVICE IS THE PRIMARY OBJECTIVE

TOOLS & EQUIPMENT

- GFI LANGUARD SYSTEM INTEGRITY MONITOR
- HOST LOGS
- STEEL INVENTORY
- ETHEREAL
- GFI LANGUARD NETWORK SCANNER
- MICROSOFT BASELINE SECURITY ANALYZER
- NeWT (NESSUS FOR WINDOWS)
- HELIX INCIDENT RESPONSE & COMPUTER FORENSICS
- SECUREPOINT NETWORK TEST TOOL
- AD-AWARE
- DELL OPTIPLEX GX110 DESKTOP PC
- COMPAQ 1720 FLAT PANEL MONITOR
- LINKSYS ETHERFAST 10/100 5-PORT WORKGROUP SWITCH
- DELL LATITUDE C600 & ACER ASPIRE 3623 LAPTOPS

USER TASKS

- DOWNLOAD *EXTRA* SOFTWARE
- CREATE A *WORD* DOCUMENT
- SEND AN *EMAIL* WITH A FILE ATTACHED
- PLAY SEVERAL *ONLINE GAMES*

WINDOWS 2000

BASELINE

- WINDOWS 2000 PROFESSIONAL W/SP4 AND OFFICE XP
- DEFAULT USER PRIVILEGES (NO ADMIN RIGHTS)
- FLASH PLUG-IN ALREADY INSTALLED
- 45 PATCHES FOR OS & OFFICE SUITE
- OPEN PORTS
 - SMTP (25/TCP)
 - POP3 (110/TCP)
 - EPMAP (135/TCP)
 - NETBIOS-SSN (139/TCP)
 - MICROSOFT-DS (445/TCP)
 - BLACKJACK (1025/TCP)
 - NETBIOS-NS (137/UDP)

WINDOWS 2000 TESTING

- WINDOWS HIGHLIGHTS
 - NONE OF THE MALWARE FULLY INSTALLED – EXCEPTION WAS ACTIVESHOPPER.COM
 - 1 SECOND EACH FOR INTERNET EXPLORER & MS WORD TO LAUNCH
 - NETWORK “CHATTER”
 - SETUP FILES FOR MALWARE RESIDED IN THE TEMPORARY INTERNET FILES DIRECTORY
 - COOKIES

WINDOWS 2000

ETHERREAL PACKET SNIFFING

No.	Time	Source	Destination	Protocol	Info
512	445.954897	192.168.1.36	192.168.1.37	SMB	Logoff AndX Request
514	445.956600	192.168.1.36	192.168.1.37	SMB	Tree Disconnect Request
516	445.957133	192.168.1.36	192.168.1.37	TCP	1055 > netbios-ssn [FIN, ACK] Seq=1360 Ack=11
518	445.957446	192.168.1.36	192.168.1.37	TCP	1055 > netbios-ssn [ACK] Seq=1361 Ack=1188 wi
25	17.863670	192.168.1.37	192.168.1.255	BROWSE	Get Backup List Request
26	17.863905	192.168.1.37	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
28	18.613417	192.168.1.37	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
29	19.364516	192.168.1.37	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
39	28.659101	192.168.1.37	192.168.1.255	BROWSE	Domain/workgroup Announcement WORKGROUP, NT w
325	328.663598	192.168.1.37	192.168.1.255	BROWSE	Domain/workgroup Announcement WORKGROUP, NT w
428	422.816364	192.168.1.37	192.168.1.255	NBNS	Name query NB ROB<00>
432	422.816914	192.168.1.37	192.168.1.36	BROWSE	Get Backup List Response
438	425.064814	192.168.1.37	192.168.1.36	TCP	netbios-ssn > 1052 [SYN, ACK] Seq=0 Ack=1 win
440	425.065225	192.168.1.37	192.168.1.36	NBSS	Positive session response
442	425.070355	192.168.1.37	192.168.1.36	SMB	Negotiate Protocol Response
444	425.078608	192.168.1.37	192.168.1.36	SMB	Session Setup AndX Response, NTLMSSP_CHALLENG

Frame 25 (216 bytes on wire, 216 bytes captured)
 Ethernet II, Src: 192.168.1.37 (00:b0:d0:b4:c1:7f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Internet Protocol, Src: 192.168.1.37 (192.168.1.37), Dst: 192.168.1.255 (192.168.1.255)
 User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
 Source port: netbios-dgm (138)
 Destination port: netbios-dgm (138)
 Length: 182
 Checksum: 0x21b9 [correct]
 NetBIOS Datagram Service
 SMB (Server Message Block Protocol)

WINDOWS 2000













ACTIVESHOPPER IN THE TEMPORARY INTERNET FILES FOLDER

Activshopper Object Recognized!

```
Type           : File
Data           : setupactiv[1].exe
TAC Rating     : 1
Category       : Misc
Comment        :
Object         : C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\O1QFSHIJ\
```

Alexa Object Recognized!

```
Type           : File
Data           : AlexaInstaller[1].exe
TAC Rating     : 5
Category       : Data Miner
Comment        :
Object         : C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\WLABO1Q3\
```

Name	In Folder
 test@activeshopper[1].txt	C:\Documents and Settings\test\Cookies
 test@www.activeshopper[2].txt	C:\Documents and Settings\test\Cookies
 ActiveShopper Comparative Shopping	C:\Documents and Settings\test\Desktop
 ActiveShopper Comparative Shopping	C:\Documents and Settings\test\Favorites
 ActiveShopper Comparative Shopping	C:\Documents and Settings\test\Favorites\Links
 ActiveShopper[1].gif	C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\O1QFSHIJ
 activeshopper[1].gif	C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\WLABO1Q3
 activeshopper[1].htm	C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\WLABO1Q3
 ActiveShopper Comparative Shopping	C:\Documents and Settings\test\Start Menu
 ActiveShopper	C:\Documents and Settings\test\Start Menu\Programs
 ActiveShopper HomePage	C:\Documents and Settings\test\Start Menu\Programs\ActiveShopper
 Test ActiveShopper	C:\Documents and Settings\test\Start Menu\Programs\ActiveShopper

KNOPPIX LiveCD BASELINE

- KNOPPIX 4.0.2 DEBIAN-BASED LINUX
- LiveCD AS A PLATFORM
- ZERO CONFIGURATION
- OPEN PORTS
 - SMTP (25/TCP)
 - BOOTPC (68/TCP)
 - POP3 (110/TCP)

KNOPPIX LiveCD TESTING

- KNOPPIX DURING TESTING
 - 17 SECONDS FOR MOZILLA FIREFOX TO LAUNCH
 - 59 SECONDS FOR OPEN OFFICE WRITER TO LAUNCH
 - WINE UTILITY ENABLED PHOTOGIZMO TO INSTALL VIA AN ActiveX CONTROL. ALSO CREATED A FOLDER NAMED “MY PICTURES” IN THE HOME DIRECTORY
 - SETUP FILES FOR MALWARE RESIDED IN THE INTERNET CACHE
 - COOKIES
 - NOT AS MUCH NETWORK “CHATTER”
 - PROPRIETARY FLASH PLUG-IN WOULDN’T INSTALL

KNOPPIX LiveCD

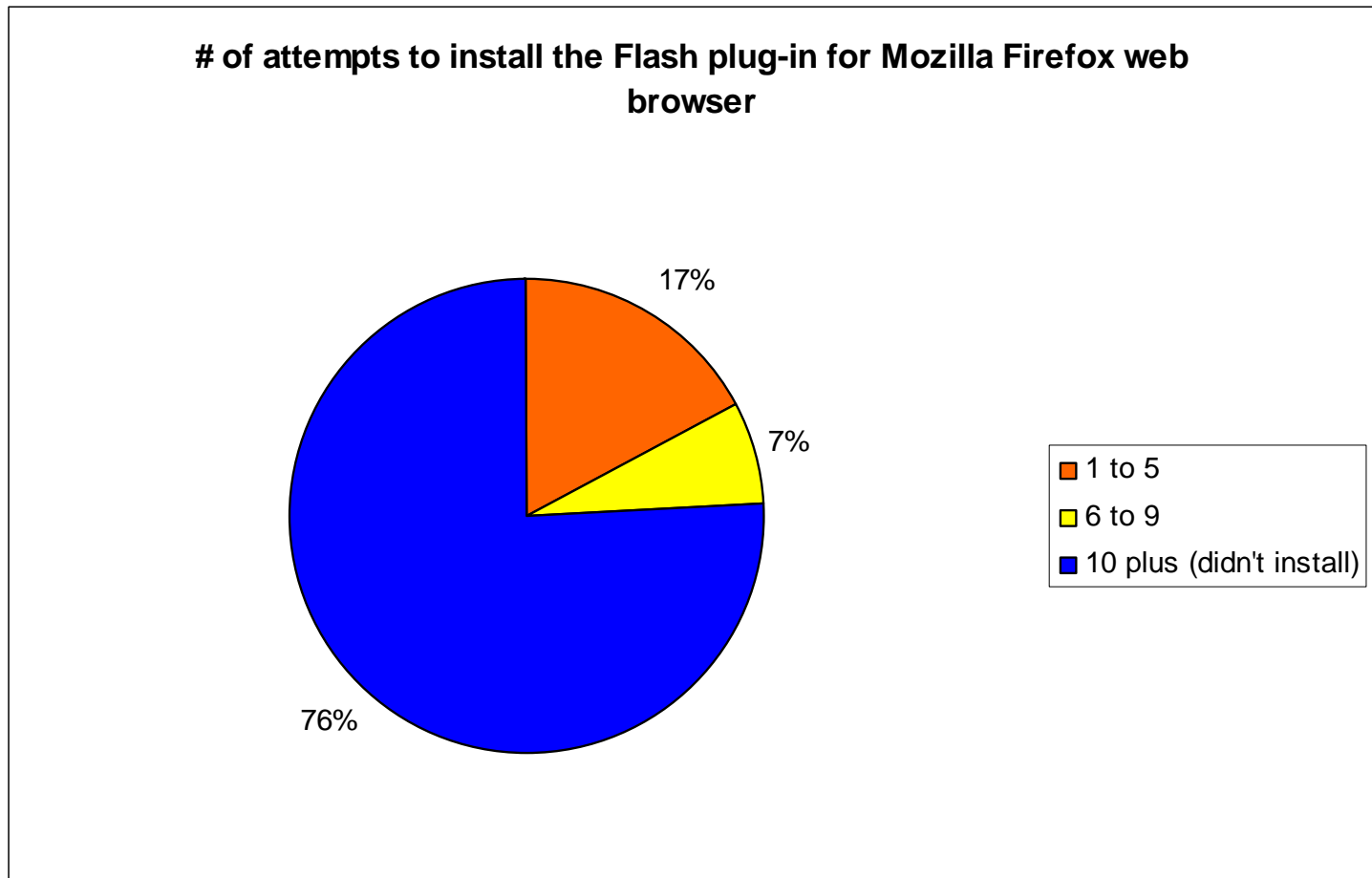
ETHERREAL PACKET SNIFFING

No. ↓	Time	Source	Destination	Protocol	Info
105	101.98688	192.168.1.36	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>
106	101.98709	192.168.1.37	192.168.1.36	ICMP	Destination unreachable (Port unreachable)
108	103.46389	192.168.1.36	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>
109	103.46419	192.168.1.37	192.168.1.36	ICMP	Destination unreachable (Port unreachable)
111	104.96391	192.168.1.36	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>
112	104.96419	192.168.1.37	192.168.1.36	ICMP	Destination unreachable (Port unreachable)
117	106.48649	172.17.6.151	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>
121	107.96395	172.17.6.151	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>
124	109.46396	172.17.6.151	192.168.1.37	NBNS	Name query NBSTAT *<00><00><00><00><00><00>

⊞ Frame 111 (92 bytes on wire, 92 bytes captured)
⊞ Ethernet II, Src: 192.168.1.36 (00:0a:e4:f1:3d:16), Dst: 192.168.1.37 (00:b0:d0:b4:c1:7f)
⊞ Internet Protocol, Src: 192.168.1.36 (192.168.1.36), Dst: 192.168.1.37 (192.168.1.37)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
Source port: netbios-ns (137)
Destination port: netbios-ns (137)
Length: 58
checksum: 0xbc53 [correct]
⊞ NetBIOS Name Service

KNOPPIX LiveCD FLASH PLUG-IN

- MACROMEDIA FLASH PLUG-IN FOR FIREFOX WEB BROWSER



SUMMARY & CONCLUSIONS

- *WINDOWS IS VIABLE*
- *LiveCD NEEDS CUSTOMIZATION*
- *COST vs. USABILITY*

MY THOUGHTS

- *NON PROFITS*
- *BUSINESSES*
- *AVAILABILITY*

LESSONS LEARNED

- CUSTOMIZE THE LiveCD

FIN

- COMMENTS?
- QUESTIONS?

www.ProjectWhiteHat.org