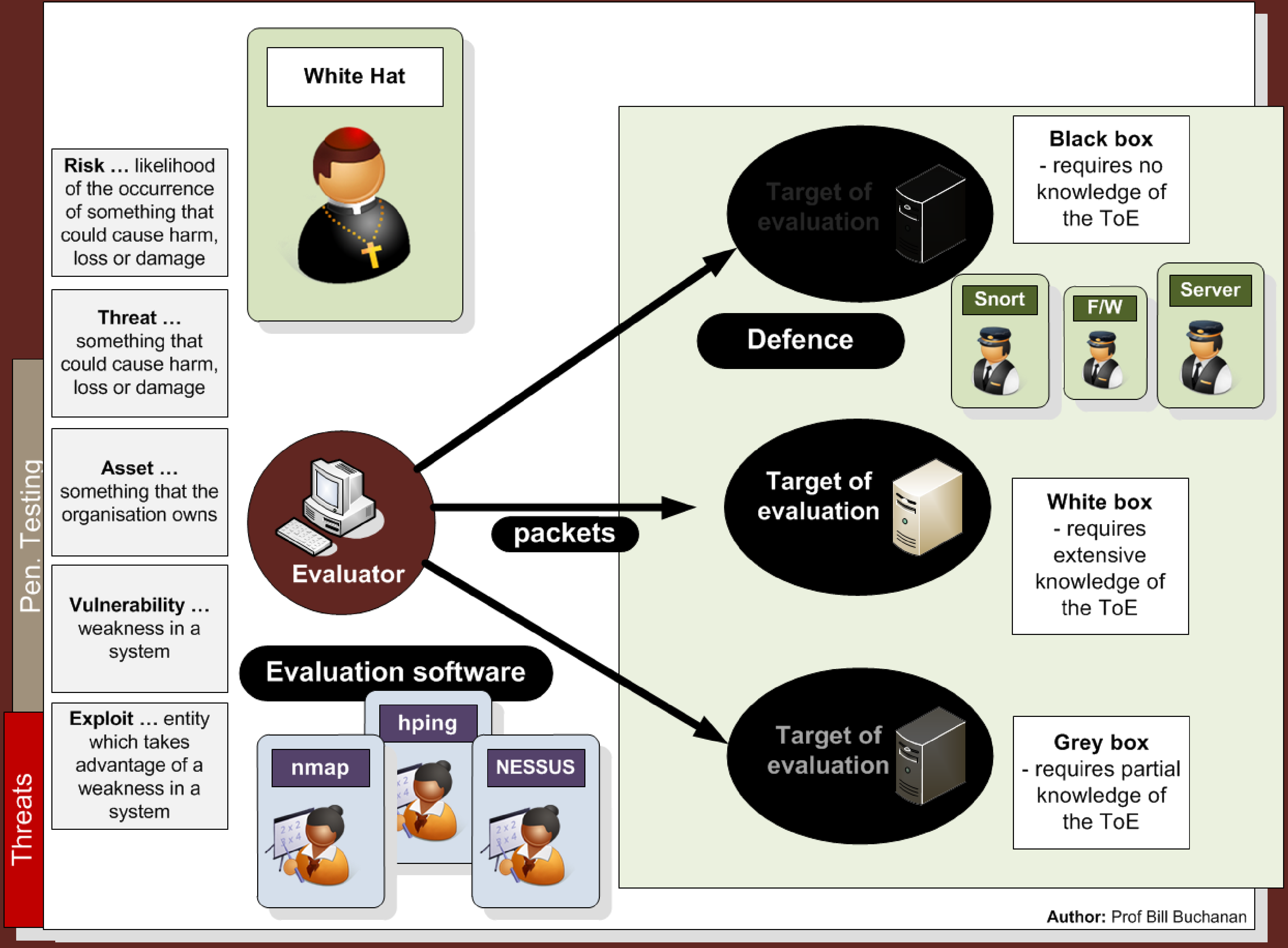
Digital

Investigator

Network Intrusions

Pen Testing: Adversarial Role [Enumeration/User Accounts]

White, grey and black box testing



Risk … likelihood of the occurrence of something that could cause harm, loss or damage

Threat … something that could cause harm, loss or damage

Asset … something that the organisation owns

Vulnerability … weakness in a system

Exploit … entity which takes advantage of a weakness in a system

Black box - requires no knowledge of the ToE

White box - requires extensive knowledge of the ToE

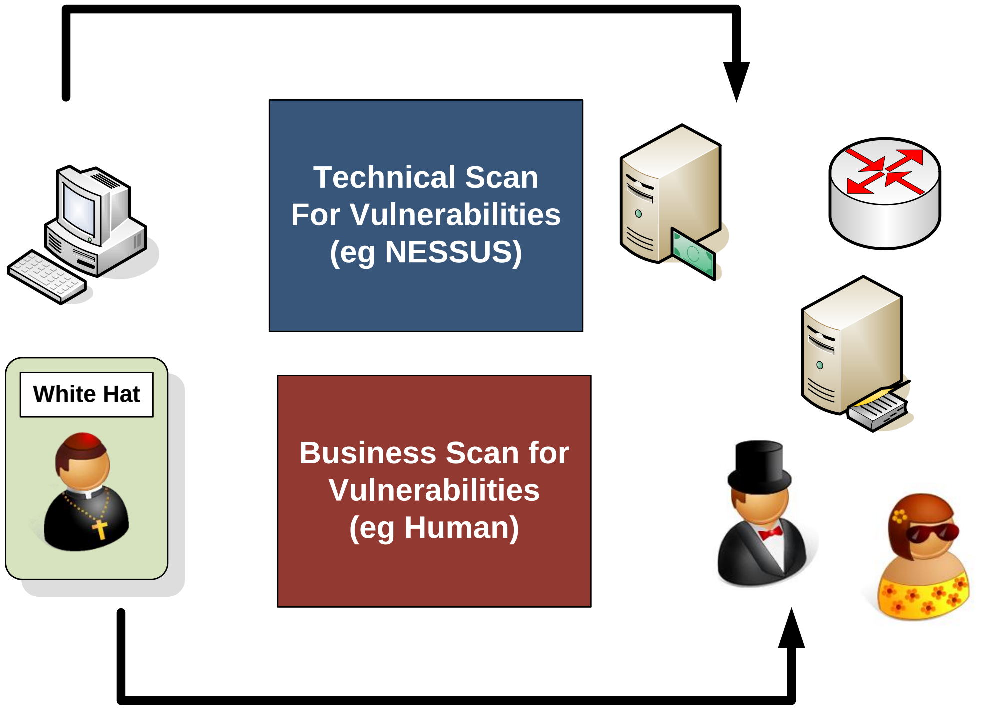
Grey box - requires partial knowledge of the ToE

Author: Prof Bill Buchanan

Pen Testing

Automated Testing

- Port scanning.
- Malware detection.
- SQL Database Exploits.



Technical Scan For Vulnerabilities (eg NESSUS)

Business Scan for Vulnerabilities (eg Human)

Adversarial Role

- Social Engineering.
- Password Cracking.
- Data Theft.

Risks

Adverse Disclosure
Service Availability
Business Disruption
Damage to or Modification to Assets
Fraud/E-Crime
Reputational Damage
Legal and Regulatory Censure

Threats

Malware
Hacking
Social
Misuse
Physical
Error
Environmental

Actor

Internal
External
Trusted Partner

Vulnerability

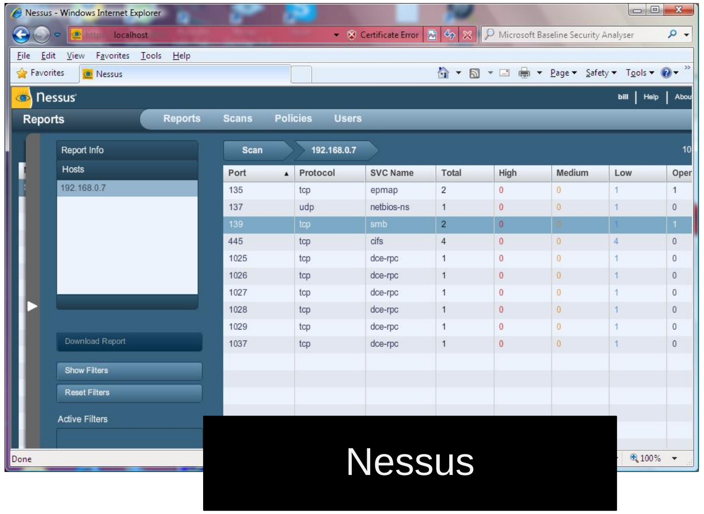
Threats

Author: Prof Bill Buchanan

Vulnerability Scanner

Threat Analysis

Scanners



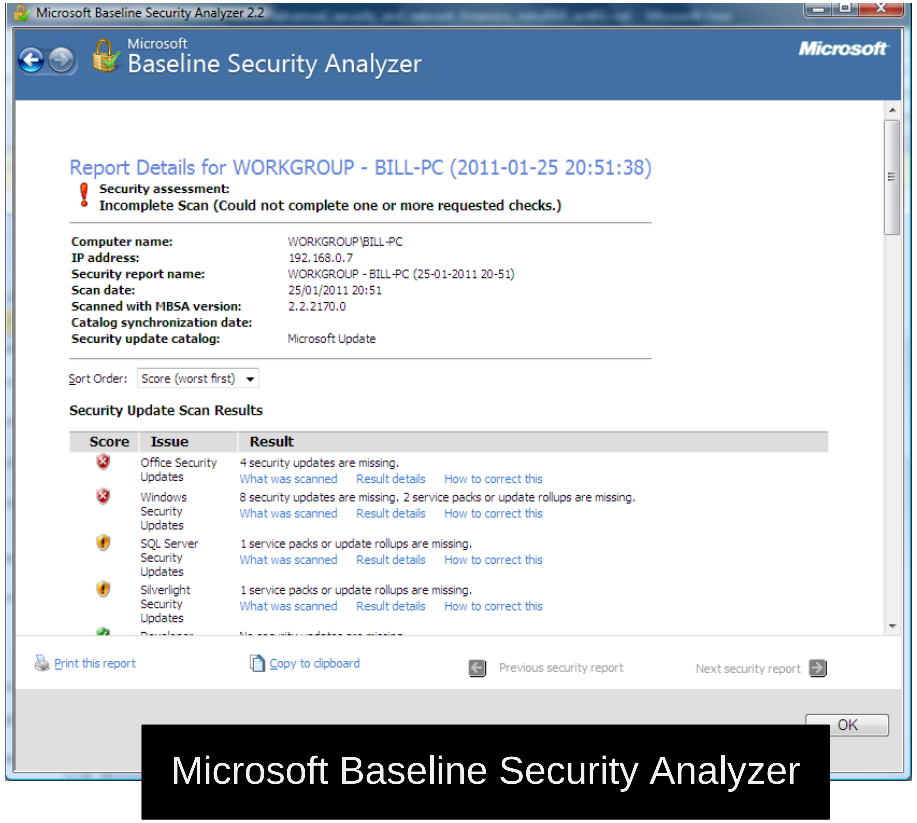
Nessus - Windows Internet Explorer

localhost | Certificate Error | Microsoft Baseline Security Analyser

Nessus — Reports | Scan | 192.168.0.7

Port	Protocol	SVC Name	Total	High	Medium	Low	Oper
135	tcp	epmap	2	0	0	1	1
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	2	0	0	1	1
445	tcp	cifs	4	0	0	4	0
1025	tcp	dce-rpc	1	0	0	1	0
1026	tcp	dce-rpc	1	0	0	1	0
1027	tcp	dce-rpc	1	0	0	1	0
1028	tcp	dce-rpc	1	0	0	1	0
1029	tcp	dce-rpc	1	0	0	1	0
1037	tcp	dce-rpc	1	0	0	1	0

Nessus



Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - BILL-PC (2011-01-25 20:51:38)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

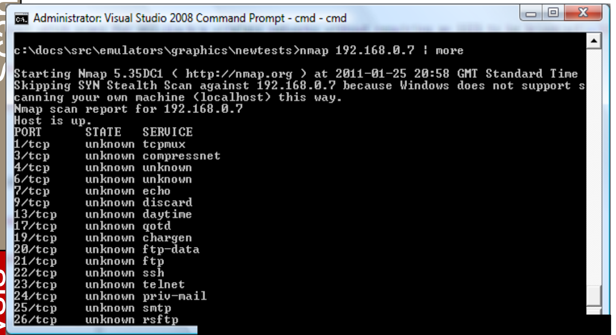
Computer name:	WORKGROUP\BILL-PC
IP address:	192.168.0.7
Security report name:	WORKGROUP - BILL-PC (25-01-2011 20-51)
Scan date:	25/01/2011 20:51
Scanned with MBSA version:	2.2.2170.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✗	Office Security Updates	4 security updates are missing. What was scanned Result details How to correct this
✗	Windows Security Updates	8 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
!	SQL Server Security Updates	1 service packs or update rollups are missing. What was scanned Result details How to correct this
!	Silverlight Security Updates	1 service packs or update rollups are missing. What was scanned Result details How to correct this

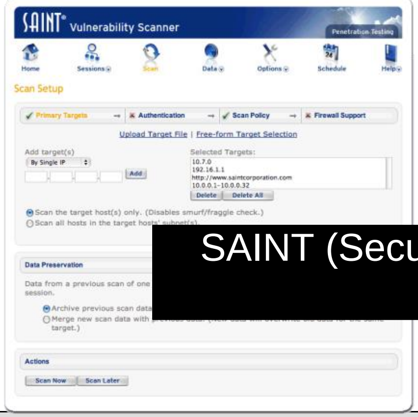
Microsoft Baseline Security Analyzer



Administrator: Visual Studio 2008 Command Prompt - cmd - cmd

```
c:\docs\src\emulators\graphics\newtests>nmap 192.168.0.7 | more

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-01-25 20:58 GMT Standard Time
Skipping SYN Stealth Scan against 192.168.0.7 because Windows does not support s
canning your own machine (localhost) this way.
Nmap scan report for 192.168.0.7
Host is up.
PORT      STATE   SERVICE
1/tcp     unknown tcpmux
3/tcp     unknown compressnet
4/tcp     unknown unknown
6/tcp     unknown unknown
7/tcp     unknown echo
9/tcp     unknown discard
13/tcp    unknown daytime
17/tcp    unknown qotd
19/tcp    unknown chargen
20/tcp    unknown ftp-data
21/tcp    unknown ftp
22/tcp    unknown ssh
23/tcp    unknown telnet
24/tcp    unknown priv-mail
25/tcp    unknown smtp
26/tcp    unknown rsftp
```

NMAP



SAINT Vulnerability Scanner

Scan Setup

✓ Primary Targets → ✗ Authentication → ✓ Scan Policy → ✗ Firewall Support

Add target(s): By Single IP

Selected Targets:
10.7.0
192.16.1.1
http://www.saintcorporation.com
10.0.0.1-10.0.0.32

● Scan the target host(s) only. (Disables smurf/fraggle check.)
○ Scan all hosts in the target hosts' subnet(s).

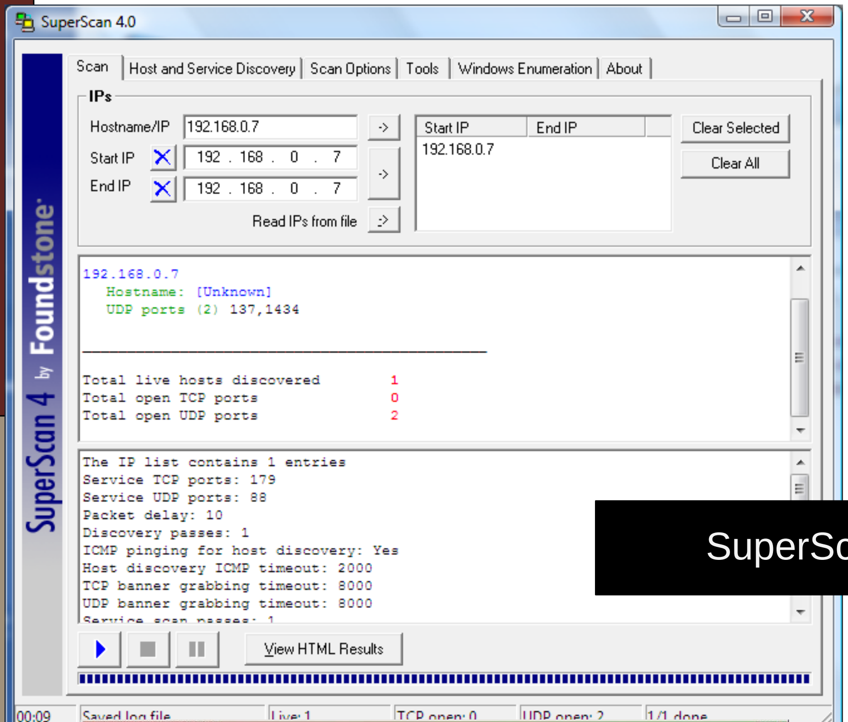
Data Preservation

Data from a previous scan of one session.

● Archive previous scan data
○ Merge new scan data with previous data. (New data will overwrite old data for the same target.)

SAINT (Security Administrator Integrated Network Tool)

Author: Prof Bill Buchanan



SuperScan 4.0
Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About
SuperScan 4 by Foundstone
IPs
Clear Selected
Clear All
Read IPs from file
View HTML Results

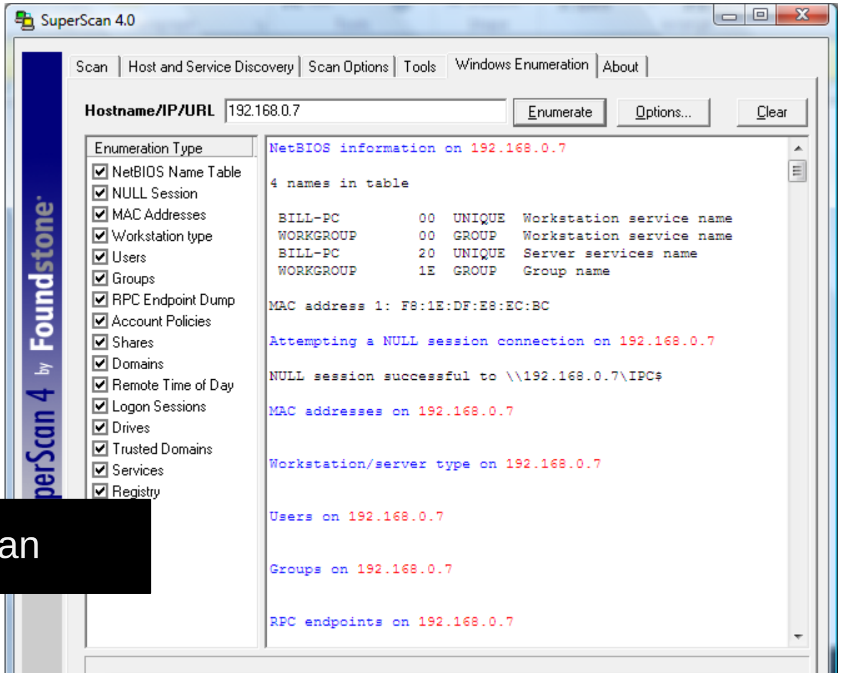
Hostname/IP: 192.168.0.7
Start IP: 192 . 168 . 0 . 7
End IP: 192 . 168 . 0 . 7

Start IP	End IP
192.168.0.7	

```
192.168.0.7
   Hostname: [Unknown]
   UDP ports (2) 137,1434

________________________________________________

Total live hosts discovered        1
Total open TCP ports               0
Total open UDP ports               2
```

```
The IP list contains 1 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
```

00:09 | Saved log file | Live: 1 | TCP open: 0 | UDP open: 2 | 1/1 done



SuperScan 4.0
Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About
SuperScan 4 by Foundstone
Enumerate
Options...
Clear

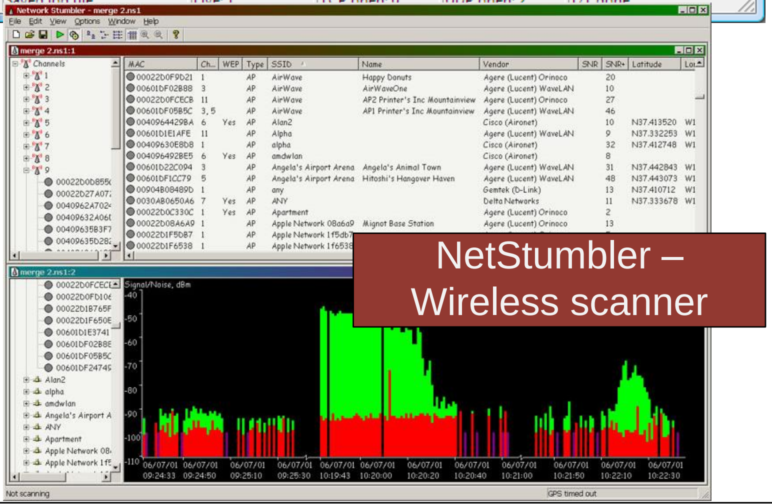
Hostname/IP/URL: 192.168.0.7

Enumeration Type
- ☑ NetBIOS Name Table
- ☑ NULL Session
- ☑ MAC Addresses
- ☑ Workstation type
- ☑ Users
- ☑ Groups
- ☑ RPC Endpoint Dump
- ☑ Account Policies
- ☑ Shares
- ☑ Domains
- ☑ Remote Time of Day
- ☑ Logon Sessions
- ☑ Drives
- ☑ Trusted Domains
- ☑ Services
- ☑ Registry

```
NetBIOS information on 192.168.0.7

4 names in table

 BILL-PC          00  UNIQUE  Workstation service name
 WORKGROUP        00  GROUP   Workstation service name
 BILL-PC          20  UNIQUE  Server services name
 WORKGROUP        1E  GROUP   Group name

MAC address 1: F8:1E:DF:E8:EC:BC

Attempting a NULL session connection on 192.168.0.7

NULL session successful to \\192.168.0.7\IPC$

MAC addresses on 192.168.0.7


Workstation/server type on 192.168.0.7


Users on 192.168.0.7


Groups on 192.168.0.7


RPC endpoints on 192.168.0.7
```

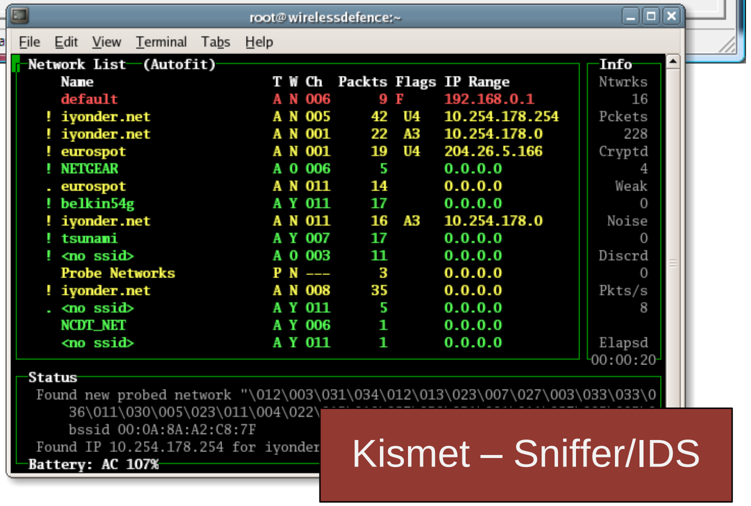
00:09

SuperScan



MAC	Ch...	WEP	Type	SSID	Name	Vendor	SNR	SNR+	Latitude	Lo...
00022D0F9D21	1		AP	AirWave	Happy Donuts	Agere (Lucent) Orinoco		20		
00601DF02B88	3		AP	AirWave	AirWaveOne	Agere (Lucent) WaveLAN		10		
00022D0FCECB	11		AP	AirWave	AP2 Printer's Inc Mountainview	Agere (Lucent) Orinoco		27		
00601DF05B5C	3, 5		AP	AirWave	AP1 Printer's Inc Mountainview	Agere (Lucent) WaveLAN		46		
0040964429BA	6	Yes	AP	Alan2		Cisco (Aironet)		10	N37.413520	W1
00601D1E1AFE	11		AP	Alpha		Agere (Lucent) WaveLAN		9	N37.332253	W1
00409630E8D8	1		AP	alpha		Cisco (Aironet)		32	N37.412748	W1
004096492BE5	6	Yes	AP	amdwlan		Cisco (Aironet)		8		
00601D22C094	3		AP	Angela's Airport Arena	Angela's Animal Town	Agere (Lucent) WaveLAN		31	N37.442843	W1
00601DF1CC79	5		AP	Angela's Airport Arena	Hitoshi's Hangover Haven	Agere (Lucent) WaveLAN		48	N37.443073	W1
00904B08489D	1		AP	any		Gemtek (D-Link)		13	N37.410712	W1
0030AB0650A6	7	Yes	AP	ANY		Delta Networks		11	N37.333678	W1
00022D0C330C	1	Yes	AP	Apartment		Agere (Lucent) Orinoco		2		
00022D08A6A9	1		AP	Apple Network 08a6a9	Mignot Base Station	Agere (Lucent) Orinoco		13		
00022D1F5DB7	1		AP	Apple Network 1f5db7						
00022D1F6538	1		AP	Apple Network 1f6538						

NetStumbler – Wireless scanner



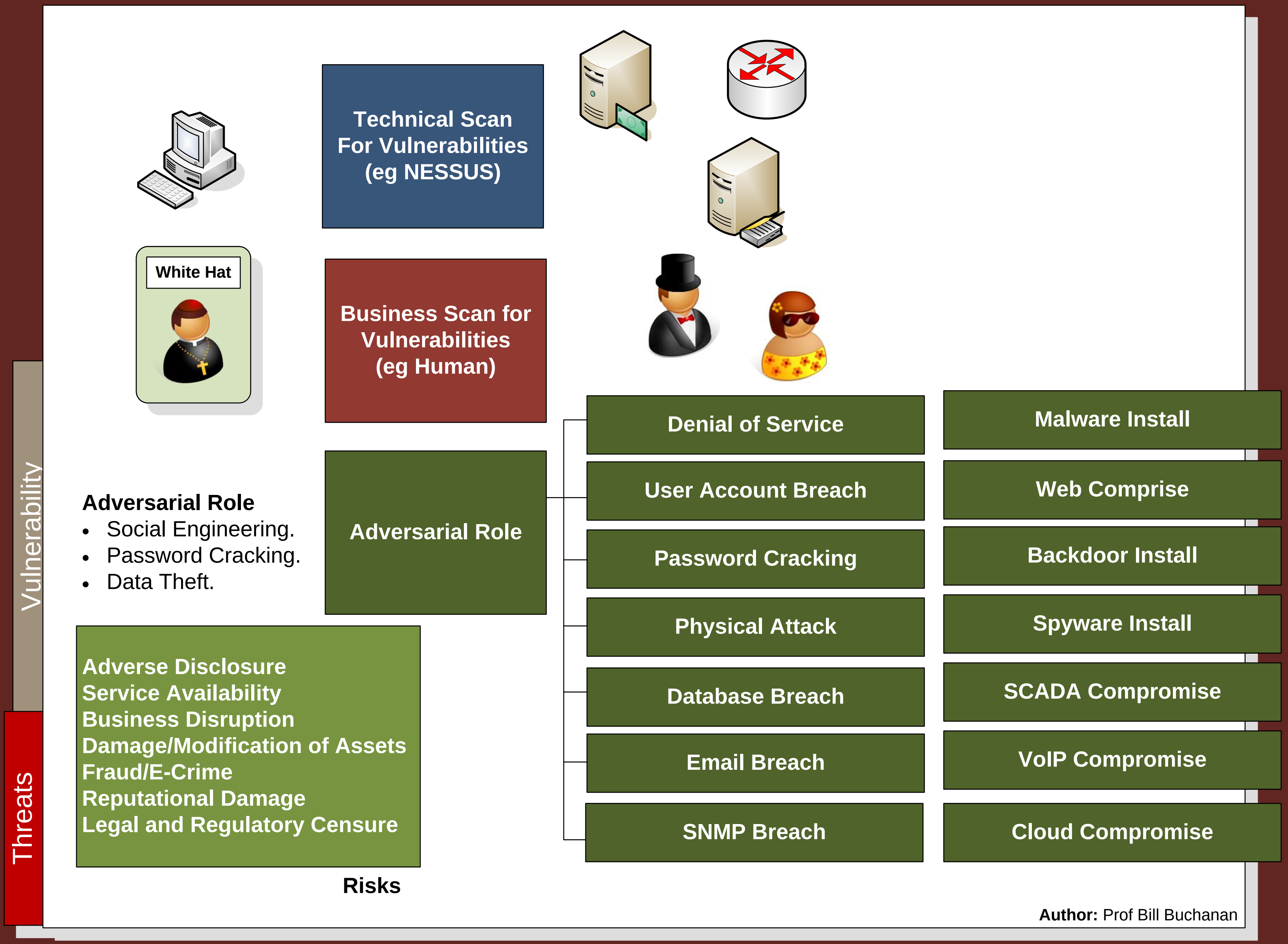
```
Network List  (Autofit)                                              Info
     Name                            T W Ch  Packts Flags IP Range       Ntwrks
     default                         A N 006      9 F     192.168.0.1        16
   ! iyonder.net                     A N 005     42  U4   10.254.178.254  Pckets
   ! iyonder.net                     A N 001     22  A3   10.254.178.0       228
   ! eurospot                        A N 001     19  U4   204.26.5.166    Cryptd
   ! NETGEAR                         A O 006      5       0.0.0.0              4
   . eurospot                        A N 011     14       0.0.0.0           Weak
   ! belkin54g                       A Y 011     17       0.0.0.0              0
   ! iyonder.net                     A N 011     16  A3   10.254.178.0     Noise
   ! tsunami                         A Y 007     17       0.0.0.0              0
   ! <no ssid>                       A O 003     11       0.0.0.0         Discrd
     Probe Networks                  P N ---      3       0.0.0.0              0
   ! iyonder.net                     A N 008     35       0.0.0.0         Pkts/s
   . <no ssid>                       A Y 011      5       0.0.0.0              8
     NCDT_NET                        A Y 006      1       0.0.0.0
     <no ssid>                       A Y 011      1       0.0.0.0         Elapsd
                                                                        00:00:20
Status
 Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
     36\011\030\005\023\011\004\022\
     bssid 00:0A:8A:A2:C8:7F
 Found IP 10.254.178.254 for iyonder
Battery: AC 107%
```

Kismet – Sniffer/IDS

Threat Analysis

Author: Prof Bill Buchanan

Vulnerability Scanner



Technical Scan For Vulnerabilities (eg NESSUS)

Business Scan for Vulnerabilities (eg Human)

Adversarial Role

Adversarial Role

- Social Engineering.
- Password Cracking.
- Data Theft.

Denial of Service

User Account Breach

Password Cracking

Physical Attack

Database Breach

Email Breach

SNMP Breach

Malware Install

Web Comprise

Backdoor Install

Spyware Install

SCADA Compromise

VoIP Compromise

Cloud Compromise

Adverse Disclosure
Service Availability
Business Disruption
Damage/Modification of Assets
Fraud/E-Crime
Reputational Damage
Legal and Regulatory Censure

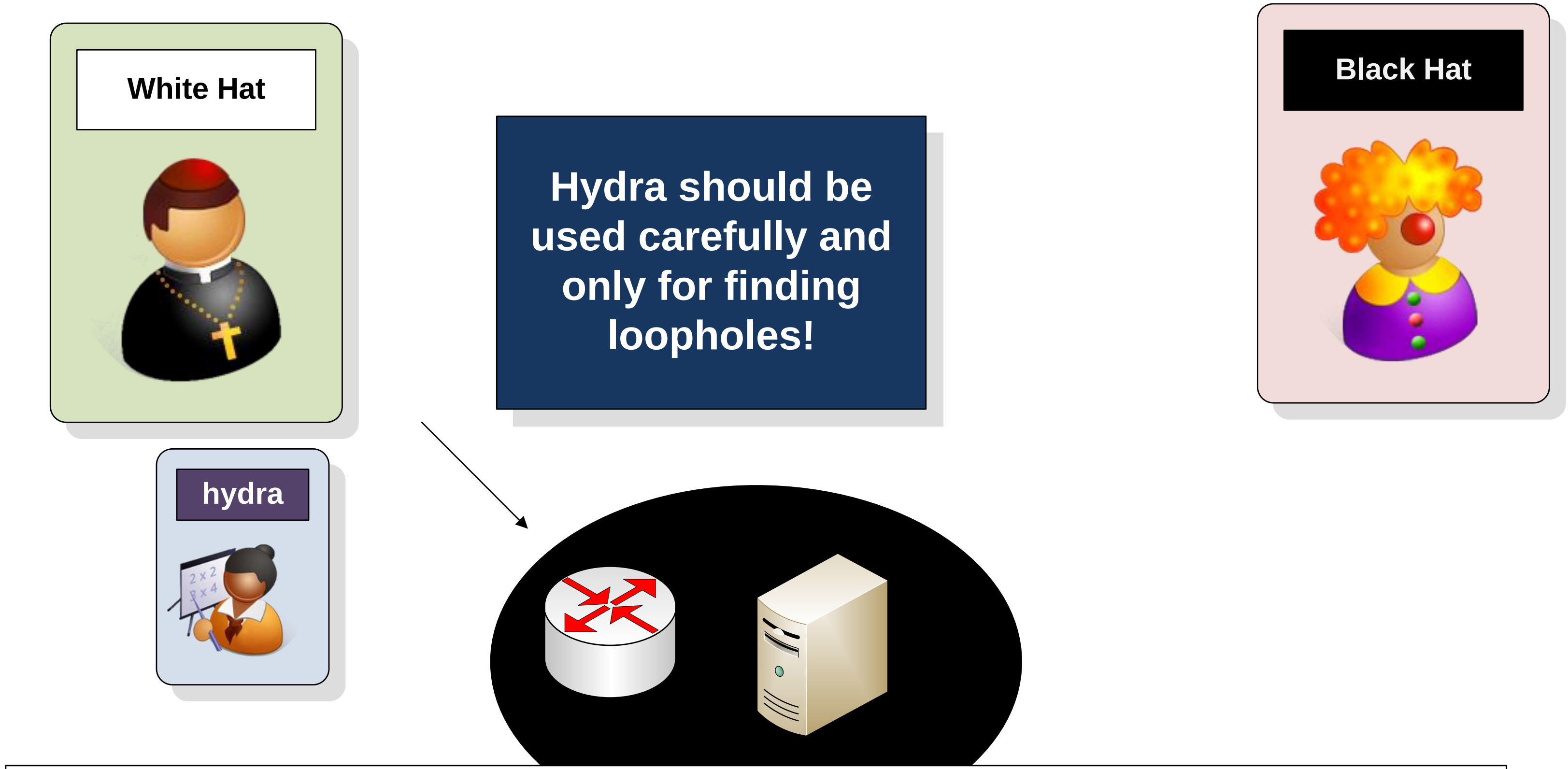
Risks

Author: Prof Bill Buchanan

Pen Testing

Threat Analysis

Password cracking



Hydra should be used carefully and only for finding loopholes!

```
C:\hydra>hydra -L user.txt -P pass.txt 192.168.47.132 ftp
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-08-28 20:13:19
[DATA] 16 tasks, 1 server, 25 login tries (l:5/p:5), ~1 try per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.47.132   login: fred   password: fred
[STATUS] attack finished for 192.168.47.132 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-08-28 20:13:39
```

Author: Prof Bill Buchanan

Hydra