Penetration Testing: Creating A Hacking Lab

Magdy Saeb

www.great-wall-security.com

GWiS

FAQ

Q: Is Penetration Testing developed to teach today's hackers how to cause more damage in more effective ways?

- A: No! Next Question

Then Why Pentest?

- A: Know your opponent!

Q: Are hacker communities fixed?

- A: No, they are changing.
- Attack surface continuously changes

Facts

- No absolute secure systems
- Crypto does not need to be broken but by-passed
- Economics: to half the system vulnerability, you have to spend double the cost

Hat Colors:

- In computing slang, hackers and crackers are identified according to their intentions:
  - White hat hacker, who hacks for beneficial motivations (Ethical Hacking)
  - Black hat hacker, who hacks for malevolent motivations
  - Grey hat hacker, who hacks with ambiguous motivations
- Also in computing is a business company called Red Hat.

- In the educational theories of Edward de Bono, six colored hats represent six thinking states.
  - White hat – Facts & Information
  - Red hat – Feelings & Emotions
  - Black hat – Critical Judgement
  - Yellow hat – Positive
  - Green hat – New Ideas
  - Blue hat – The Big Picture

Recent Detrimental Attacks

- Three Indian defendants (2008) hacked a brokerage firm using pump and dump scheme.
- Russian hacking group (RBN) stole millions of dollars from CiTi Bank using “Black Energy” (2009).
- German Banks lost 300 K Euros using new malware (2009).
- A massive joint operation between US and Egyptian law enforcement that is called “Phish Pry” to catch 100 American and Egyptian defendants who hacked America Banking Systems collecting individual account information(2009).
- Iraqi insurgents intercepted live videos from US Predator drones using on-line available software.

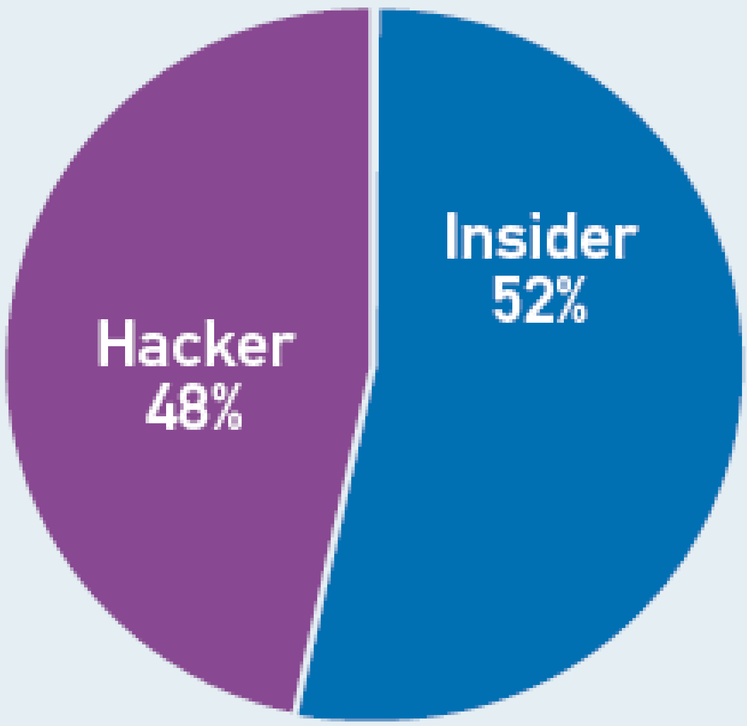
There is a particularly devious type of malicious software that locks users out of their own computer systems until an individual agrees to pay a ransom to the hackers. In these cases, the FBI has surprisingly suggested just ponying up the dough.

“The ransomware is that good,” said Bonavolonta at the 2015 Cyber Security Summit in Boston, as quoted by Security Ledger. “To be honest, we often advise people just to pay the ransom.”

“Have they lost the technical battle?” !!! ☺

Insider vs. The Hacker

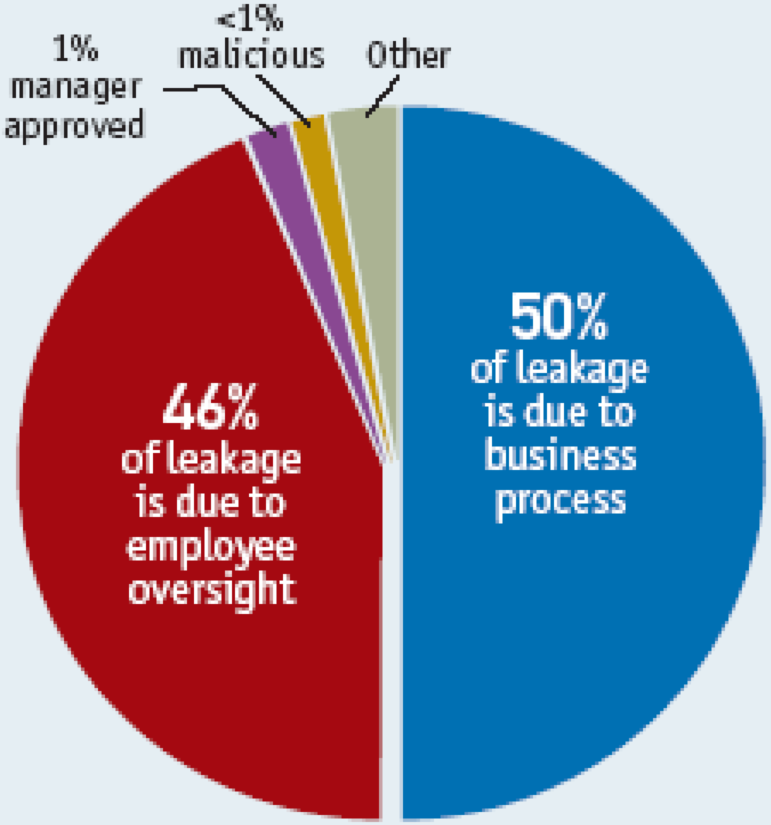
2005 Data Security Breaches



Data compiled from industry sources including EPIC.org and PerkinsCoie.com.

Inadvertent vs. Malicious

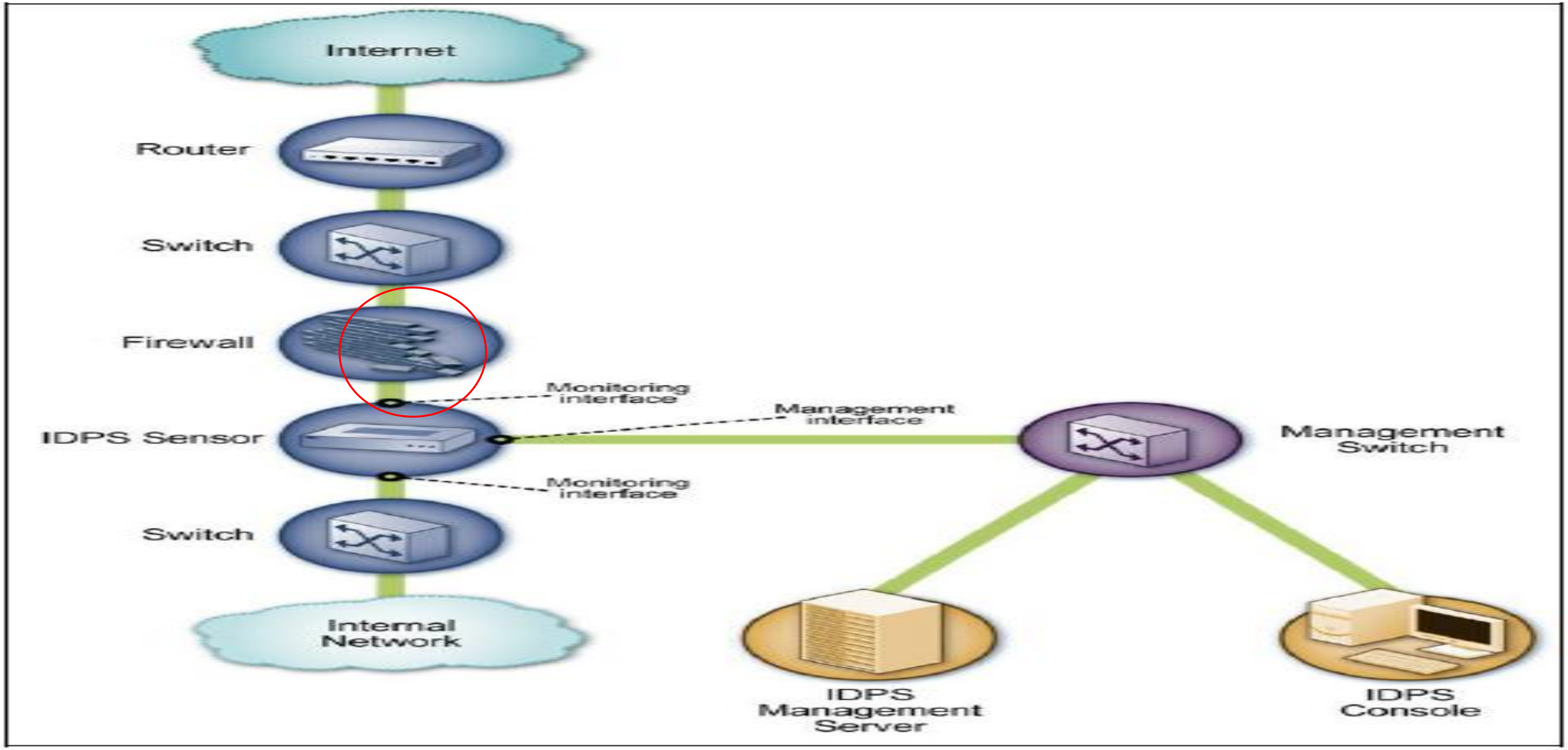
96% of leaks are due to faulty processes or oversight



Source:Vontu risk assessment findings.

- For the fifth straight year, identity theft ranked first of all fraud complaints.
- Ten million cases of Identity Theft annually.
- 59% of companies have detected some internal abuse of their networks

DID YOU EVER THINK ABOUT SELLING OUR CONFIDENTIAL DATABASE OF CUSTOMER INFORMATION?
scottadams@aol.com
www.dilbert.com
IT WOULD BE MASSIVELY PROFITABLE WHILE VIRTUALLY UNDETECTABLE.
BUT HIGHLY UNETHICAL.
©2004 Scott Adams, Inc./Dist. by UFS, Inc.
I DON'T KNOW YOU ANYMORE.
I'M YANKING YOUR CHAIN. WHEN DO WE START?
© UFS, Inc.

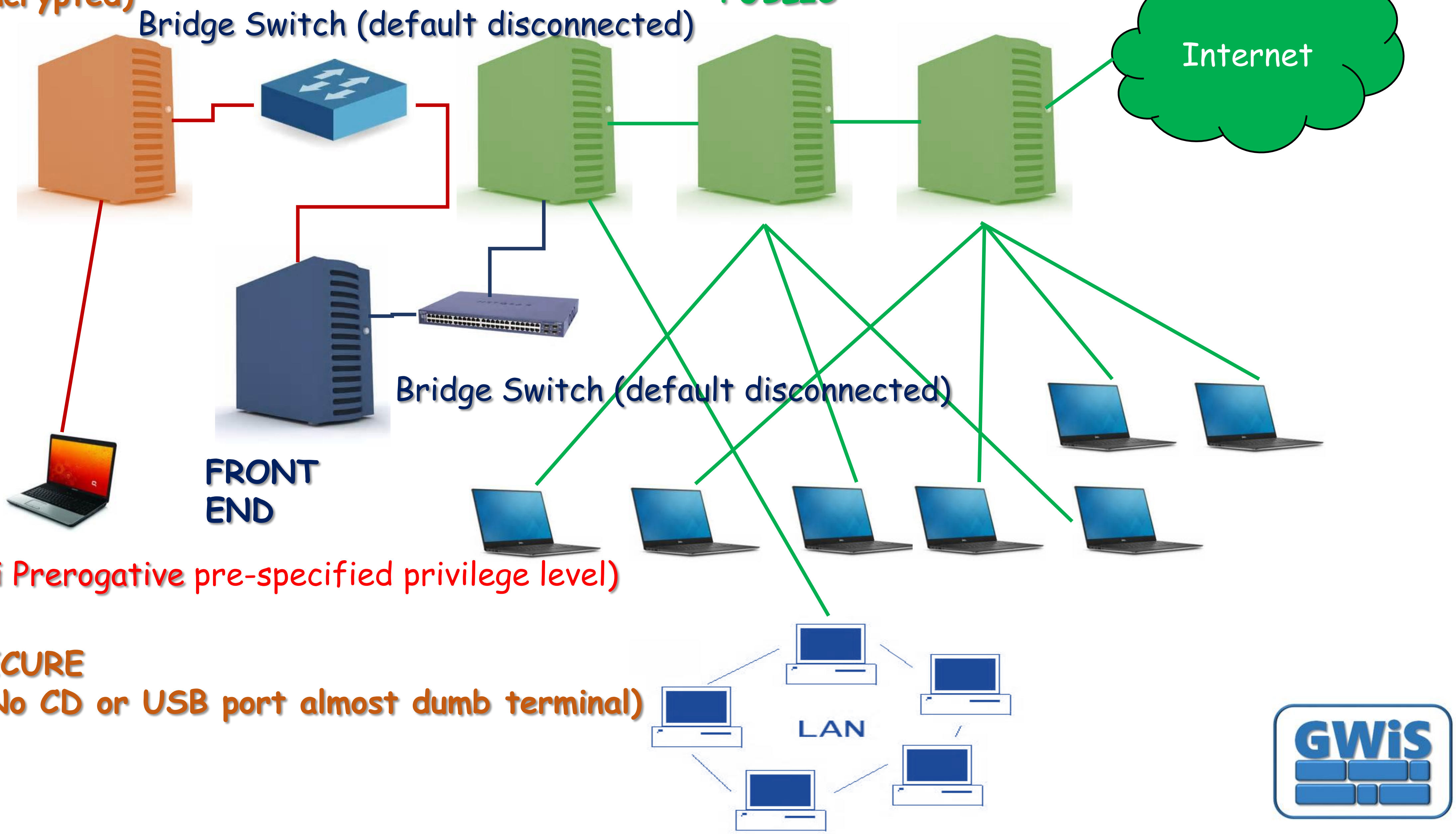


Inline Network-Based IDPS Sensor Architecture Example

Quiz 1: From where we get more serious attacks from the inside or outside a corporation?

Quiz 2: What is the cause of most data leaks (breach) ?

So, What is the Solution?



SECURE
(Encrypted)

Bridge Switch (default disconnected)

PUBLIC

Internet

Bridge Switch (default disconnected)

FRONT
END

(Hi Prerogative pre-specified privilege level)

SECURE
(No CD or USB port almost dumb terminal)

LAN

Most Serious Attacks

- Use Advanced Persistent Threat (APT)
- Attack Subcontractors!

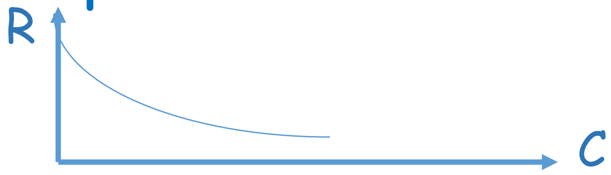
Introduction

- Ethics and Hacking:
  - Getting Permission to hack
  - Code of Ethics Canons
  - Stay Ethical
  - Gray Hat and Black Hat Hackers
  - Ethical hacking Standards
  - Laws
- Setting up a lab
- Download Links and Support Files
- HackingDojo.com

Vulnerability Assessment

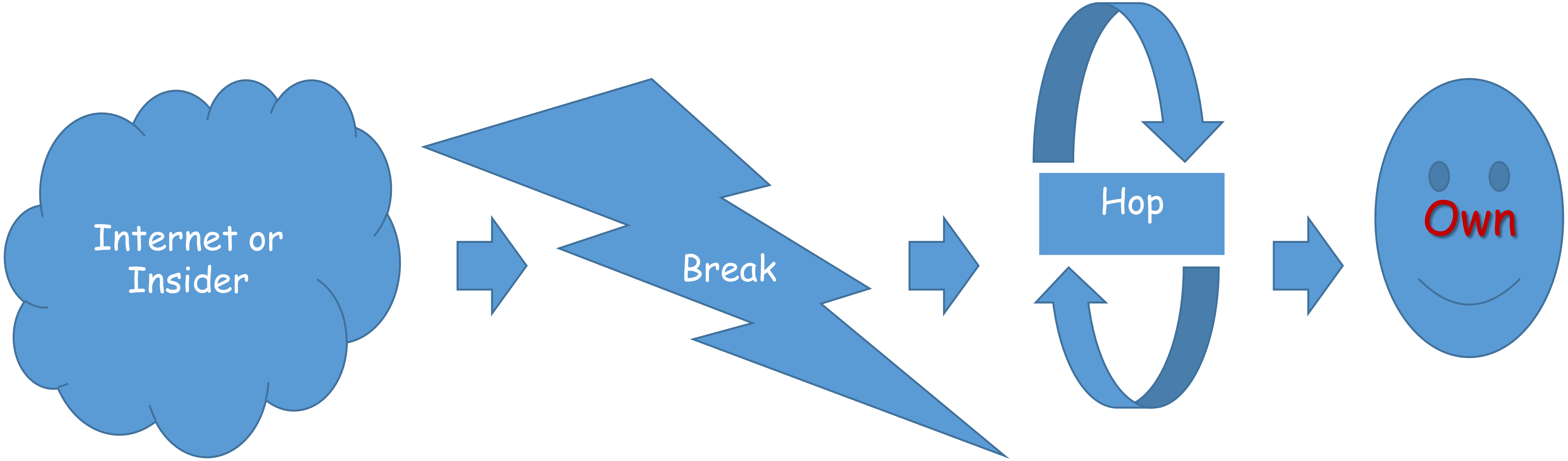
- The vast amount of functionality provided by an organization's networking database and desktop software can be used against them.

Reliability versus Complexity!



  - Using a network scanner to probe ports and services on a range of IP addresses. It provides a list of vulnerabilities and counter measures.
  - Sounds easy..?
  - No, the problem these automatically generated reports don't understand the proper context of its findings. Some vulnerabilities are called "Hi" which are less probable in practice. Other are called "Lo" which are highly probable in practice.
  - Hackers, in some cases, know this.

PenTesting



Internet or Insider

Break

Hop

Own

Own!

- Have root privileges on the most critical UNIX or Linux system.
- Have administrator account.
  - Trophies:
    - CEO passwords
    - Laptops of CFO and CIO
    - Company trade secrets
    - Secret files
    - Router PW(s)

Penetration Testing Process (i)

1. Form Three teams:
   - Red (Attackers)
   - White (Administrators)
   - Blue (Management overseeing the test)

2. Rules
   1. Objectives
   2. What to attack
   3. Who knows what about the other teams (single or double blind)
   4. Start and stop times
   5. Legal issues
   6. Nondisclosure
   7. Reporting
   8. Formal approval (get Out of Jail Card).

Penetration Testing Process (ii)

3. Passive Scanning
   - Website and source code, News groups and Social networking
   - Whois database
   - Edgar database (EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file forms with the U.S. Securities and Exchange Commission the "SEC")
   - ARIN (ARIN, a nonprofit member-based organization, supports the operation of the Internet through the management of Internet number resources throughout its service region; coordinates the development of policies by the community for the management of Internet Protocol number resources; and advances the Internet through informational outreach.)
   - RIPE (Réseaux IP Européens (**RIPE**, French for "European IP Networks") is a forum open to all parties with an interest in the technical development of the Internet.)
   - Google, Monster.com,..etc.
   - Dumpster diving (**Dumpster diving** is the practice of sifting through commercial or residential waste to find items that have been discarded by their owners, but that may prove useful to the picker.)

Penetration Testing Process (iii)

4. Active Scanning
   - Probe the target's public exposure with scanning tools, this may include:
     - Commercial scanning tools
     - Banner grapping
     - Social engineering
     - War Dialing

       (**War dialing** refers to the use of various kinds of technology to automatically **dial** many phone numbers, usually in order to find weak spots in an IT security architecture. Hackers often use **war dialing** software, sometimes called "**war** dialers" or "demon dialers," to look for unprotected modems.)
     - DNS zone transfer

       (**DNS zone transfer**, also sometimes known by the inducing DNS query type **AXFR**, is a type of DNS transaction. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. Zone transfers may be performed using two methods, full AXFR[1] and incremental IXFR.)
     - Sniffing traffic
     - Wireless War Driving

       (**Wardriving** is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant(PDA).)

Penetration Testing Process (iv)

5. Attack Surface Enumeration
   - Probe the target network to identify, enumerate, and document each exposed device:
     - Network mapping
     - Perimeter firewalls
     - Router and switch locations
     - LAN, MAN and WAN connections
6. Fingerprinting
   - Identify:
     - Operating systems and patch level
     - Open ports
     - Running Services
     - User accounts

Penetration Testing Process (v)

7. Target System Selection

    Identify the most useful and vulnerable target

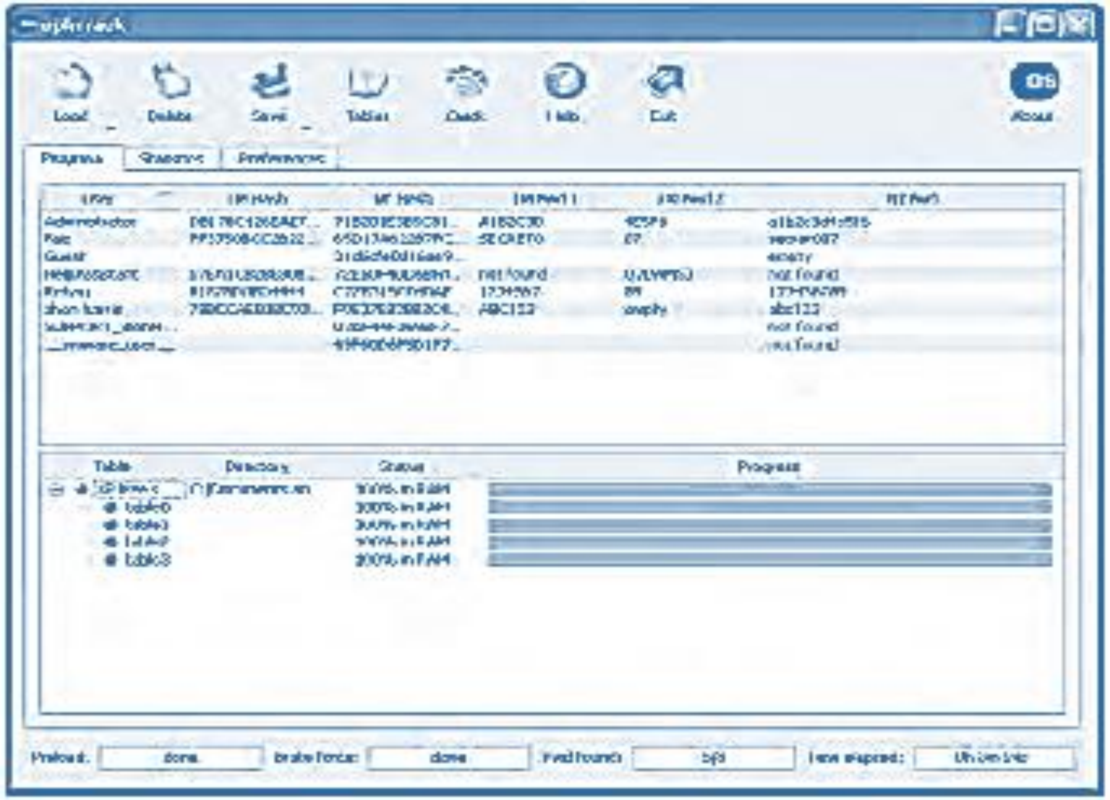
8. Exploiting the uncovered vulnerabilities
    - Network
    - Kill Services
    - Kill Server

9. Escalation of Privileges
    - Administrative Rights
    - Cracked Passwords
    - Buffer overflow to gain local versus remote control

10. Documentation and Reporting

Dual Nature of Tools (The Good, The Evil)

- Hacking tools to test strength of PW (password cracking software for dictionary and brute force attacks on individual passwords)



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	DB1 78C126BAE7...	71B20BE3B9C81...	A1B2C3D	4E5F6	a1b2c3d4e5f6
Kate	FF37508CC2622...	65D17465287FC...	SECRETO	07	secret007
Guest		31d6cfe0d16ae9...			empty
HelpAssistant	[illegible]	[illegible]	not found	[illegible]	not found
Robert	[illegible]	[illegible]	1234567	89	123456789
shon harris	7BDCCAE0B8C7D...	F0C3762B2BB2C6...	ABC123	empty	abc123
SUPPORT_388945...		[illegible]			not found
__vmware_user__		[illegible]			not found

Table	Directory	Status	Progress
XP free small	C:\[illegible]	100% in RAM	
table0		100% in RAM	
table1		100% in RAM	
table2		100% in RAM	
table3		100% in RAM	

Preload: done Brute force: done Pwd found: 5/8 Time elapsed: 0h 0m 1s

Check if they are built of Upper & Lower-case letters, Numeric Values and Their Length.

Setting up Your Lab

- Targets in a PenTest Lab
- Problems with Learning to Hack
- Live CD
- De-ICE
- Hackerdemia
- Security Projects
- Virtual NW PenTest Labs
- Protecting PenTest Data

Protecting Penetration Test Data

- Encryption Schemes
  - Encrypt HD
  - Lock HD in a secure place
  - Store systems in a physically secure room
  - Perform penetration tests against pentest systems
- Hash Functions
  - File fingerprint

Advanced Pentest labs

- Hardware Considerations
  - Routers
  - Firewalls
  - Intrusion Detection/Intrusion Prevention Systems (IDIP)
  - Hardware Configuration
  - De-ICE Network Challenges
  - Network Architecture
- Analyzing Malware
  - Viruses
  - Worms

Creating a Controlled Environment

- Harvesting Malware
- Information Analysis
- More Target Ideas
- Capture The Flag (CTF) Events
- Web Based Challenges
- Vulnerability Announcements

Insider Attacks

- Hired employees are essentially strangers a company pays to perform a task. There is no guarantee that the people tasked with handling sensitive data won't steal it or misuse it.
- To conduct an insider attack, use familiar tools and techniques mentioned in this presentation. The primary difference is that you are working inside the company with pre-specified privilege level.
- Tools and Preparations:
  - A good Network Security Monitoring (NSM) system
  - Packet Analyzer Software
  - Intrusion Detection System monitoring binary hacking downloads or unfamiliar IP addresses.
  - These tools should be carried in your flash memory.
  - For fully locked CMOS and full disk encryption, you need a hard drive with a prepared operating system on it to gain access to the subject network from the provided equipment.

Local Administrator Privileges (Security Account manager SAM file)

- To see the local administrators group use the prompt command:
  - net localgroup Administrators
  - The SAM file contains password hashes and windows protect this file while OS is running. Accessing this file while OS is running will set an alarm for a centrally managed enterprise system.
  - While recovering the administrator password in on our agenda, we will remove the password from the administrator account altogether. We keep the SAM file for cracking later.
  - We will boot the system from a USB drive and use the offline NT password and registry editor tool.
  - Some machines are configured to bypass removable media devices.
  - In the worst case, you can use your own HD as a primary to boot from and then access the target windows as a secondary to recover the SAM file.

Using Offline Password and Registry Editor

Offline NT password runs in command-line mode. In most cases the default options will step you through mounting primary drive and removing the administrator account password as shown next:

1. The tool presents a list of drives and guess which one contains the operating system as shown in Figure 1.
2. The tool tries to guess the location of the SAM file as shown in Figure 2. Copy SAM and SECURITY files to the USB drive. Offline NT Password mounts the boot disk in the directory /disk

```
cp/drive/WINDOWS/system 32/config/SAM/mnt
cp/drive/WINDOWS/system 32/config/SECURITY/mnt
```

Figures of Selecting the Boot device and finding the SAM file

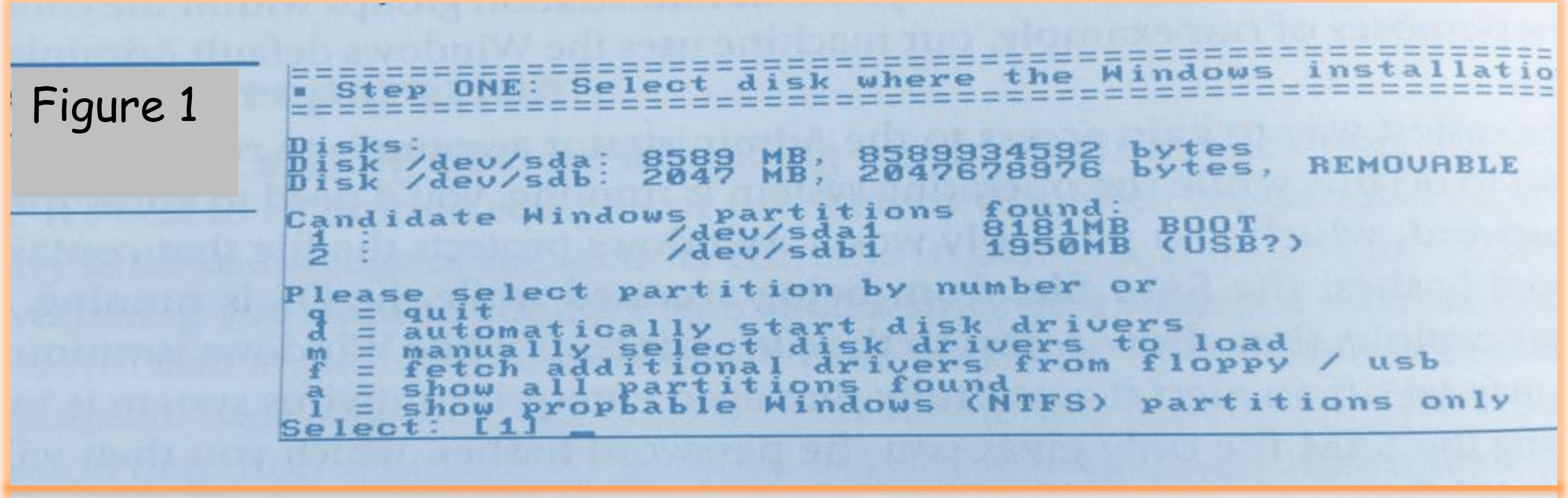


Figure 1

```
===============================================================
• Step ONE: Select disk where the Windows installatio
===============================================================

Disks:
Disk /dev/sda: 8589 MB, 8589934592 bytes
Disk /dev/sdb: 2047 MB, 2047678976 bytes, REMOVABLE

Candidate Windows partitions found:
 1 :                /dev/sda1       8181MB BOOT
 2 :                /dev/sdb1       1950MB (USB?)

Please select partition by number or
 q = quit
 d = automatically start disk drivers
 m = manually select disk drivers to load
 f = fetch additional drivers from floppy / usb
 a = show all partitions found
 l = show propbable Windows (NTFS) partitions only
Select: [1] _
```

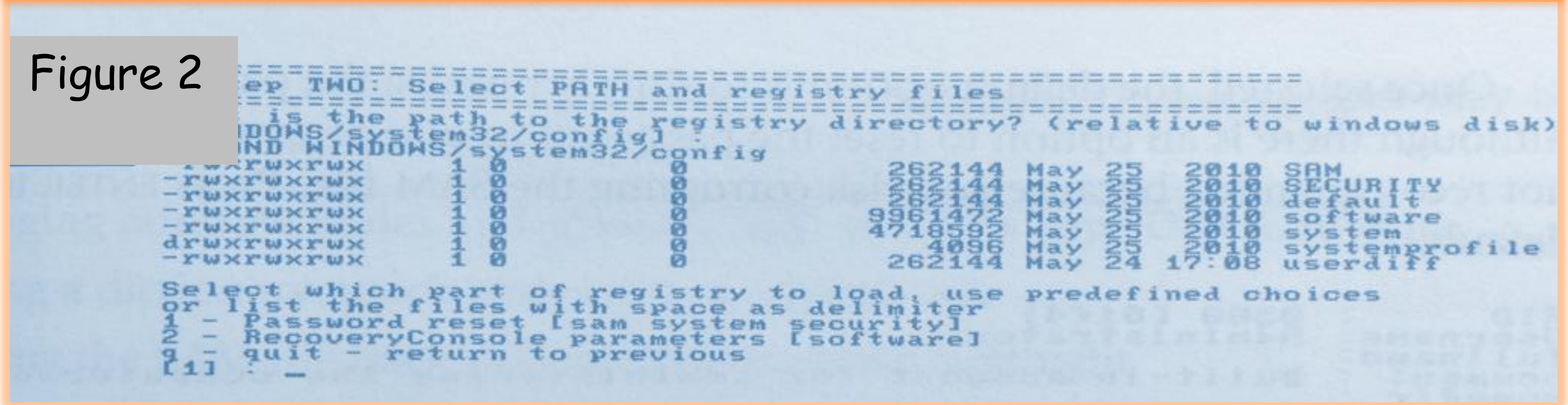


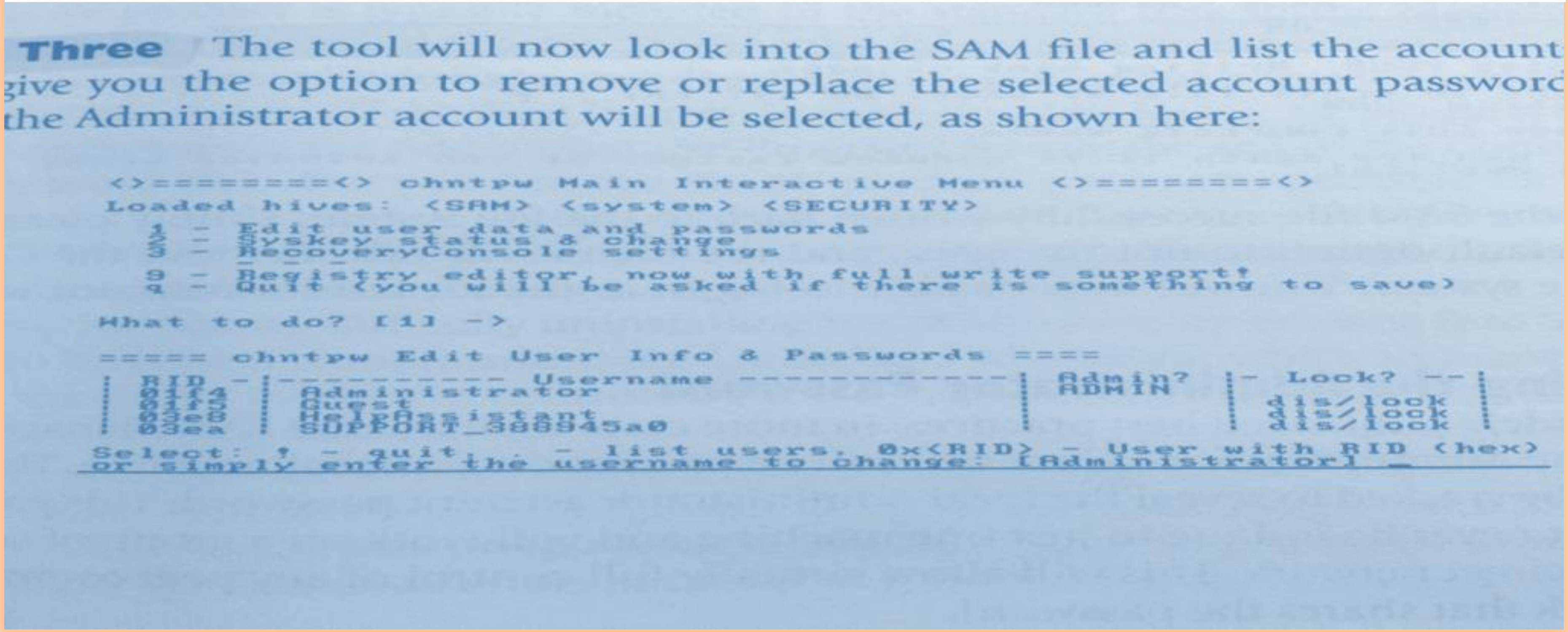
Figure 2

```
=====================================================
ep TWO: Select PATH and registry files
=====================================================
 is the path to the registry directory? (relative to windows disk)
NDOWS/system32/config] :
ND WINDOWS/system32/config
rwxrwxrwx     1 0          0          262144 May 25  2010 SAM
-rwxrwxrwx    1 0          0          262144 May 25  2010 SECURITY
-rwxrwxrwx    1 0          0          262144 May 25  2010 default
-rwxrwxrwx    1 0          0         9961472 May 25  2010 software
-rwxrwxrwx    1 0          0         4718592 May 25  2010 system
drwxrwxrwx    1 0          0            4096 May 25  2010 systemprofile
-rwxrwxrwx    1 0          0          262144 May 24 17:08 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _
```

SAM File

3. The tool looks into the SAM file and lists all accounts. It will give the option to remove or replace the selected account password. By default, the Administrator account will be selected, as shown in Figure 3.
4. Once the password is successfully removed from the SAM file, it must be written back to the file system. The default option will just do that and report id success or fail.
5. In most cases, the Lan Manger LM hash can be cracked to reveal the local Administrator account password. This password will almost never be unique to just one machine and will work on a group of machine in the target network.

SAM File Figures

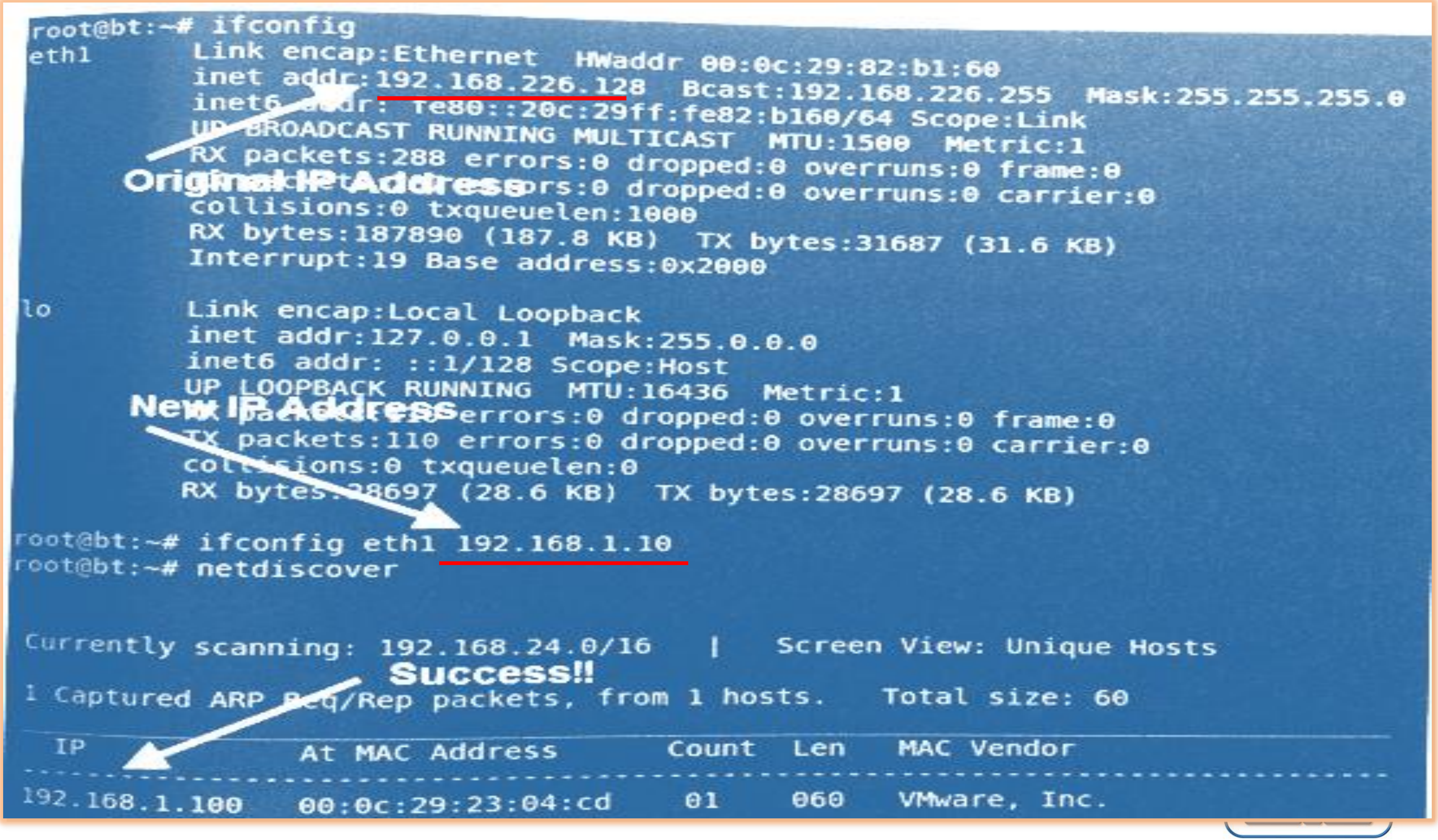


Three The tool will now look into the SAM file and list the account give you the option to remove or replace the selected account passwor the Administrator account will be selected, as shown here:

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM> <system> <SECURITY>
  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
  - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |
| 03e8 | HelpAssistant                  |        | dis/lock |
| 03ea | SUPPORT_388945a0               |        | dis/lock |
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] _
```

De-ICE IP Addresses

- The De-ICE virtual images have been configured with static IP addresses. To know what the IP address for each system, simply add "192.168" to the image number. A simple solution is change the default interface from 192.168.226.128 to 192.168.1.100 as shown below:



```
root@bt:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:82:b1:60
          inet addr:192.168.226.128  Bcast:192.168.226.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe82:b160/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:288 errors:0 dropped:0 overruns:0 frame:0
          TX packets:[illegible] errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:187890 (187.8 KB)  TX bytes:31687 (31.6 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28697 (28.6 KB)  TX bytes:28697 (28.6 KB)

root@bt:~# ifconfig eth1 192.168.1.10
root@bt:~# netdiscover

 Currently scanning: 192.168.24.0/16   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address      Count   Len   MAC Vendor
 -----------------------------------------------------------------------------
 192.168.1.100   00:0c:29:23:04:cd    01     060   VMware, Inc.
```

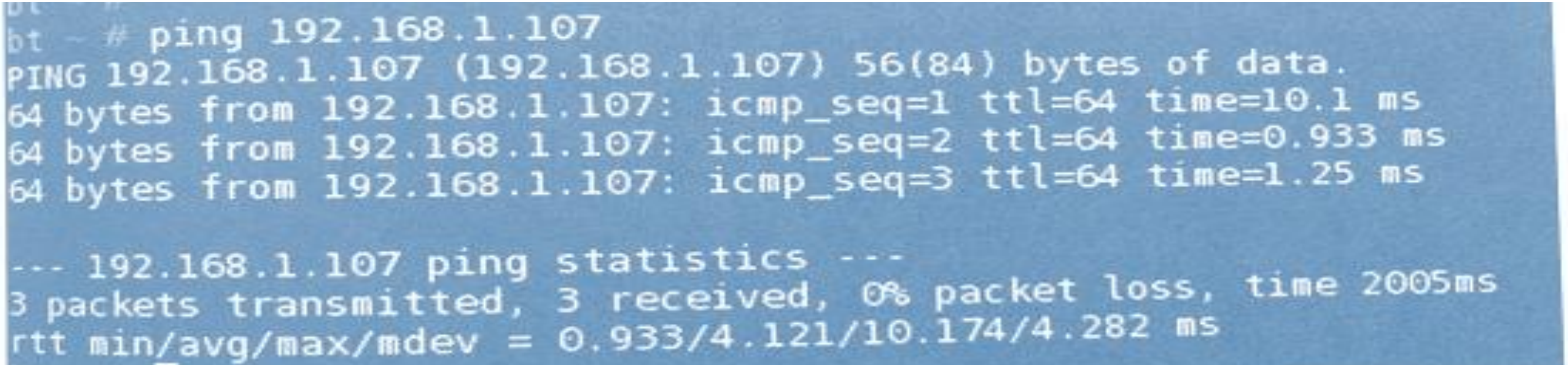
Vulnerability Identification and Exploitation

- Collecting information on Op System, Internet Protocol (IP) addresses, application data and more, we proceed to identify vulnerabilities and potential threats.
  - Port scanning: To verify existence of target system and obtain a list of all communication channels (ports) that accept connections.
  - Target Verification: Using Transport Control Protocol (TCP), User Data Gram Protocol (UDP) and PING command, which uses Internet Control Message Protocol (ICMP) that occurs at the Network Layer of OSI.

32 bits		
0	15	31
Type	CODE	Check Sum
Identifier		Sequence Number
Data (for padding)		

ICMP message header:
8= Echo Request
0= Echo Reply

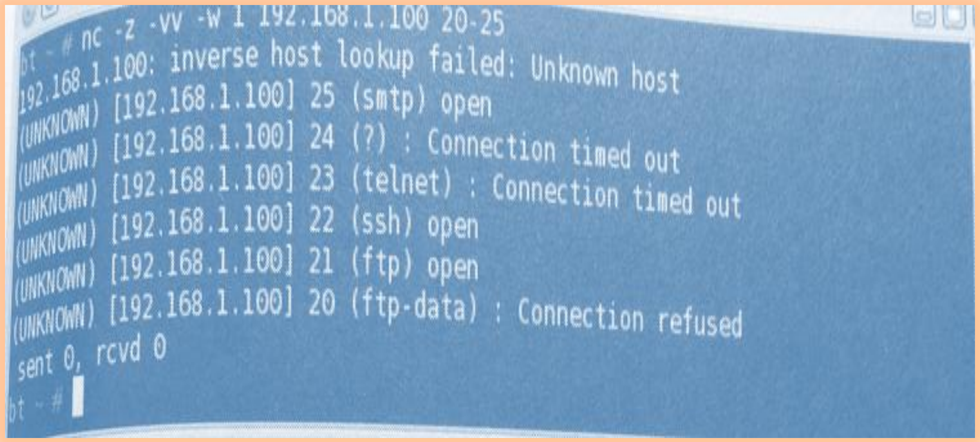
Successful Ping Request



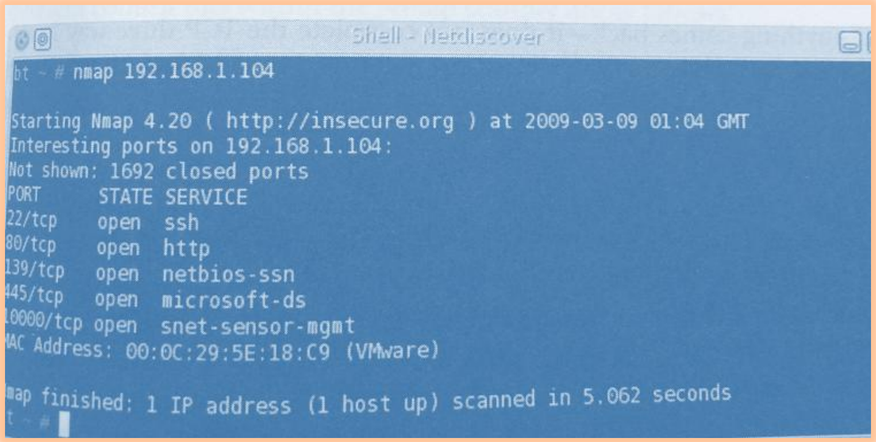
```
bt ~ # ping 192.168.1.107
PING 192.168.1.107 (192.168.1.107) 56(84) bytes of data.
64 bytes from 192.168.1.107: icmp_seq=1 ttl=64 time=10.1 ms
64 bytes from 192.168.1.107: icmp_seq=2 ttl=64 time=0.933 ms
64 bytes from 192.168.1.107: icmp_seq=3 ttl=64 time=1.25 ms

--- 192.168.1.107 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.933/4.121/10.174/4.282 ms
```

TCP and UDP Scanning

- The TCP header contains particular interest parts:
  - The control bits starting at 106th bit labeled URG, ACK, PSH, RST, SYN and FIN. These are used to provide reliable connection between two entities.
  - Use NETCAT tool and probe the De-ICE1.100 disk for a list of ports available.



```
bt ~ # nc -z -vv -w 1 192.168.1.100 20-25
192.168.1.100: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.100] 25 (smtp) open
(UNKNOWN) [192.168.1.100] 24 (?) : Connection timed out
(UNKNOWN) [192.168.1.100] 23 (telnet) : Connection timed out
(UNKNOWN) [192.168.1.100] 22 (ssh) open
(UNKNOWN) [192.168.1.100] 21 (ftp) open
(UNKNOWN) [192.168.1.100] 20 (ftp-data) : Connection refused
sent 0, rcvd 0
bt ~ # 
```



```
bt ~ # nmap 192.168.1.104

Starting Nmap 4.20 ( http://insecure.org ) at 2009-03-09 01:04 GMT
Interesting ports on 192.168.1.104:
Not shown: 1692 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:5E:18:C9 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 5.062 seconds
bt ~ # 
```

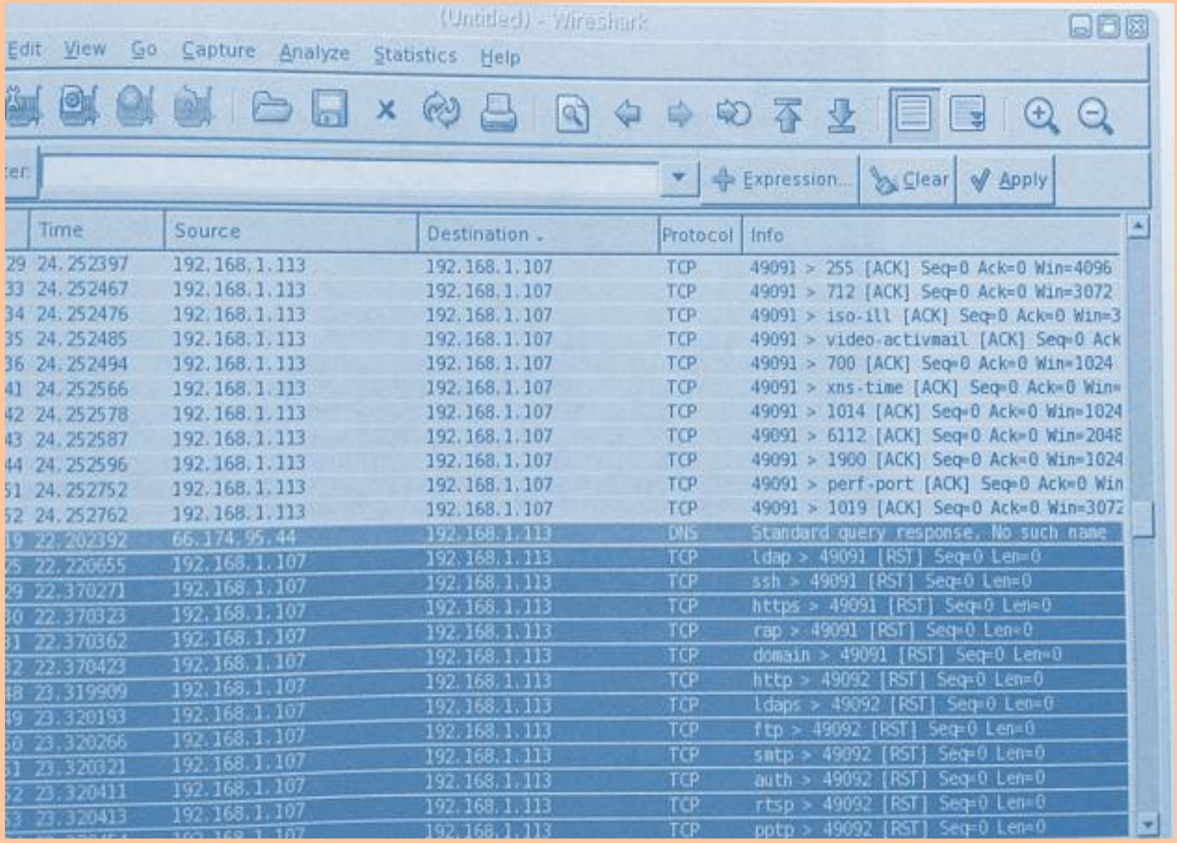
Perimeter Avoidance Scanning

- Nmap is used to scan a system or network segment sometimes to avoid firewalls by manipulating the control bits mentioned before. These are:
  - ACK scan sends an ACK
  - FIN scan
  - Null scan
  - Xmas scan

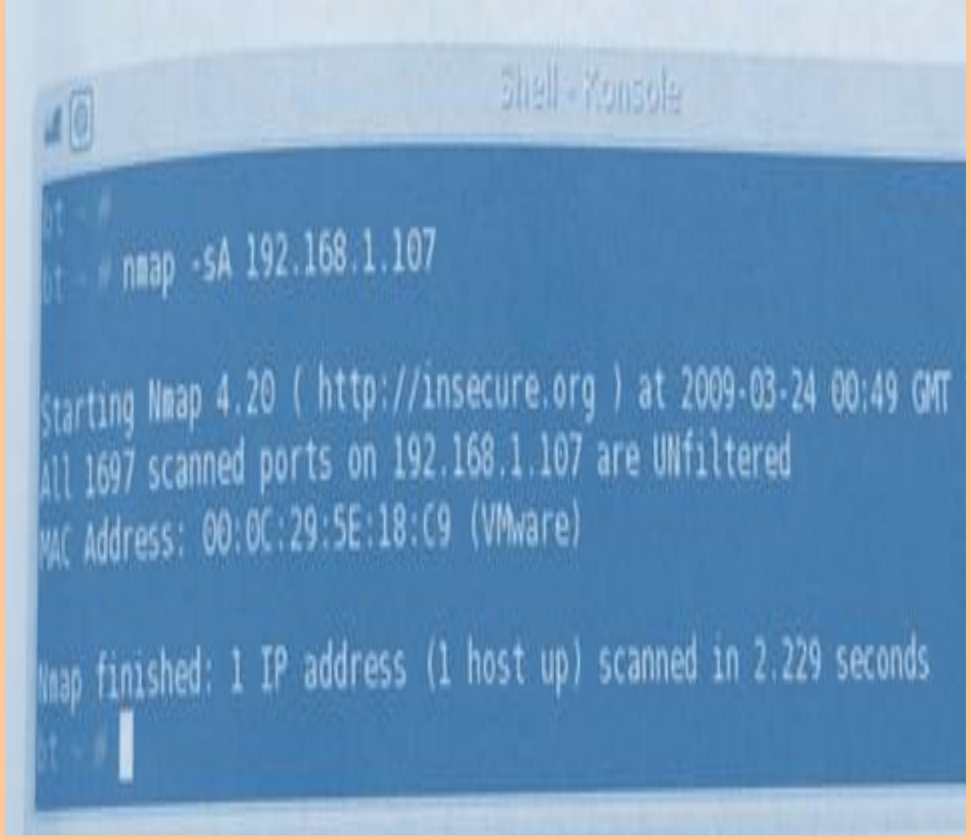
Wireshark capture during Nmap ACK scan

- The first Figure shown below capture traffic of an ACK scan against a target system using Nmap. The attack system with IP address 192.168.1.113 sends a series of TCP packets with ACK control; bit to the target system (192.168.1.107). The target system replies with a RST request, because the ACK was unexpected and not part of any established communication stream.
- When the target system returns RST to the attack system, Nmap reports the port as unfiltered as seen in the second Figure

Wireshark capture during Nmap ACK scan



	Time	Source	Destination	Protocol	Info
29	24.252397	192.168.1.113	192.168.1.107	TCP	49091 > 255 [ACK] Seq=0 Ack=0 Win=4096
33	24.252467	192.168.1.113	192.168.1.107	TCP	49091 > 712 [ACK] Seq=0 Ack=0 Win=3072
34	24.252476	192.168.1.113	192.168.1.107	TCP	49091 > iso-ill [ACK] Seq=0 Ack=0 Win=3
35	24.252485	192.168.1.113	192.168.1.107	TCP	49091 > video-activmail [ACK] Seq=0 Ack
36	24.252494	192.168.1.113	192.168.1.107	TCP	49091 > 700 [ACK] Seq=0 Ack=0 Win=1024
41	24.252566	192.168.1.113	192.168.1.107	TCP	49091 > xns-time [ACK] Seq=0 Ack=0 Win=
42	24.252578	192.168.1.113	192.168.1.107	TCP	49091 > 1014 [ACK] Seq=0 Ack=0 Win=1024
43	24.252587	192.168.1.113	192.168.1.107	TCP	49091 > 6112 [ACK] Seq=0 Ack=0 Win=2048
44	24.252596	192.168.1.113	192.168.1.107	TCP	49091 > 1900 [ACK] Seq=0 Ack=0 Win=1024
51	24.252752	192.168.1.113	192.168.1.107	TCP	49091 > perf-port [ACK] Seq=0 Ack=0 Win
52	24.252762	192.168.1.113	192.168.1.107	TCP	49091 > 1019 [ACK] Seq=0 Ack=0 Win=3072
19	22.202392	66.174.95.44	192.168.1.113	DNS	Standard query response, No such name
25	22.220655	192.168.1.107	192.168.1.113	TCP	ldap > 49091 [RST] Seq=0 Len=0
29	22.370271	192.168.1.107	192.168.1.113	TCP	ssh > 49091 [RST] Seq=0 Len=0
30	22.370323	192.168.1.107	192.168.1.113	TCP	https > 49091 [RST] Seq=0 Len=0
31	22.370362	192.168.1.107	192.168.1.113	TCP	rap > 49091 [RST] Seq=0 Len=0
32	22.370423	192.168.1.107	192.168.1.113	TCP	domain > 49091 [RST] Seq=0 Len=0
48	23.319909	192.168.1.107	192.168.1.113	TCP	http > 49092 [RST] Seq=0 Len=0
49	23.320193	192.168.1.107	192.168.1.113	TCP	ldaps > 49092 [RST] Seq=0 Len=0
50	23.320266	192.168.1.107	192.168.1.113	TCP	ftp > 49092 [RST] Seq=0 Len=0
51	23.320321	192.168.1.107	192.168.1.113	TCP	smtp > 49092 [RST] Seq=0 Len=0
52	23.320411	192.168.1.107	192.168.1.113	TCP	auth > 49092 [RST] Seq=0 Len=0
53	23.320413	192.168.1.107	192.168.1.113	TCP	rtsp > 49092 [RST] Seq=0 Len=0
[illegible]	[illegible]	192.168.1.107	192.168.1.113	TCP	pptp > 49092 [RST] Seq=0 Len=0



```
ot ~ #
ot ~ # nmap -sA 192.168.1.107

Starting Nmap 4.20 ( http://insecure.org ) at 2009-03-24 00:49 GMT
All 1697 scanned ports on 192.168.1.107 are UNfiltered
MAC Address: 00:0C:29:5E:18:C9 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 2.229 seconds
ot ~ #
```

Wireshark

Nmap ACK
scan response

The Lab

- Wireshark
- Nmap
- Password Cracking Software
- Live CD or Flash Memory
- De-ICE
- Hackerdemia
- Security Projects
- Virtual NW PenTest Labs
  - A good Network Security Monitoring (NSM) system
  - Intrusion Detection System monitoring binary hacking downloads or unfamiliar IP addresses.
  - These tools should be carried in your flash memory.
  - For fully locked CMOS and full disk encryption, you need a hard drive with a prepared operating system on it to gain access to the subject network from the provided equipment.
  - System boot from a USB drive
  - Offline NT password tool
  - Slax

Much More to Learn!

End of Presentation