iNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 1.2

Enumeration and System hacking

Aim

To learn the significance and techniques used in Enumeration for Windows and System hacking methods.

Instructional Objectives

Objectives of this chapter are:

- Explain the concept of Enumeration and techniques used for Windows enumeration
- List the tools used for Windows enumeration
- Explain SNMP enumeration technique
- Describe the System hacking, particularly by password cracking method
- Explain what are Trojans and their goals.
- Describe Trojan infection mechanism and Trojan tools

Learning Outcomes

At the end of this chapter, you are expected to:

- List four methods that can be used for Windows enumeration
- Interpret the result from Net View command from a computer in a domain
- Interpret the result of running NBTSTAT on a machine in a local network
- Research on some more tools that are available on the internet, for NetBIOS exploiting
- Describe SNMP Enumeration method, with the help of how it is done using enumeration tools
- Explain important countermeasure steps for each type of enumeration technique for windows discussed in this book

Enumeration and its techniques

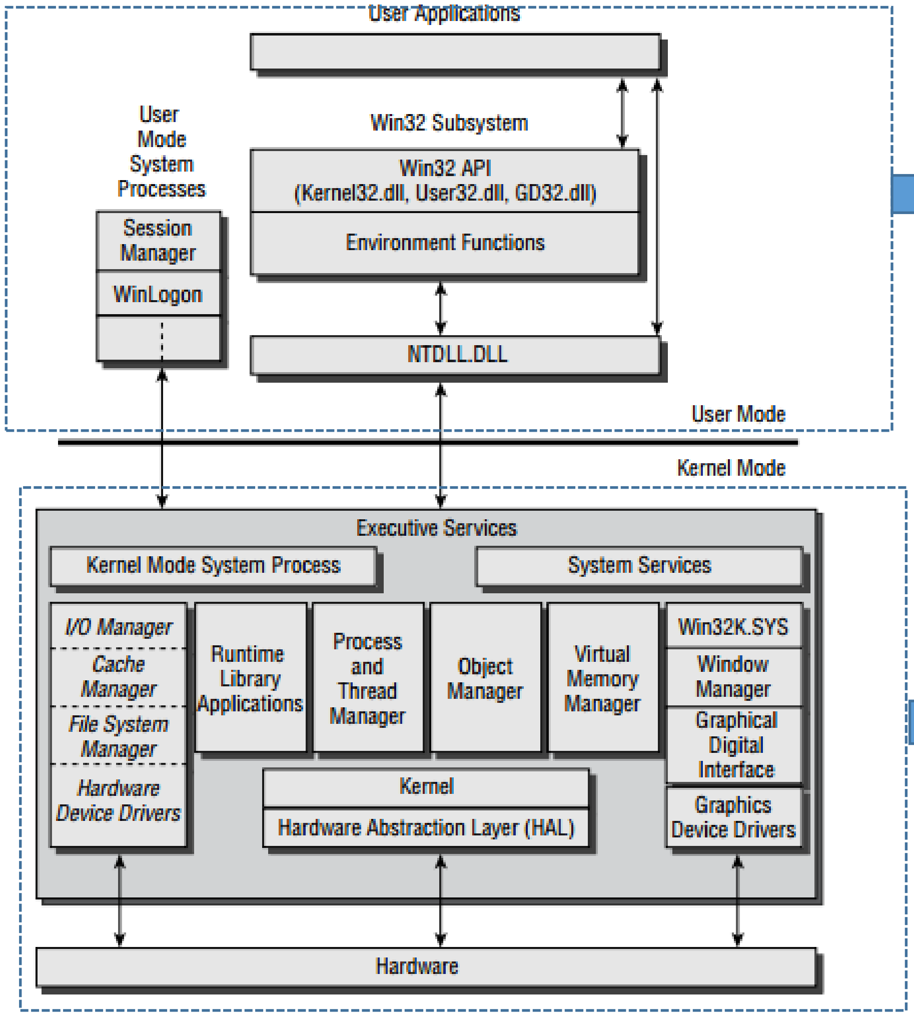
Introduction to Enumeration

Searching for much more information

About users, their passwords , services and ports

Windows enumeration Techniques

Windows Architecture



User mode

Kernel mode

Techniques used by the hacker for Enumeration are:

1. Establish a null sessions and to enumerate
2. NetBIOS names
3. Enumerating SNMP
4. Querying DNS
5. Retrieving information from Active Directory

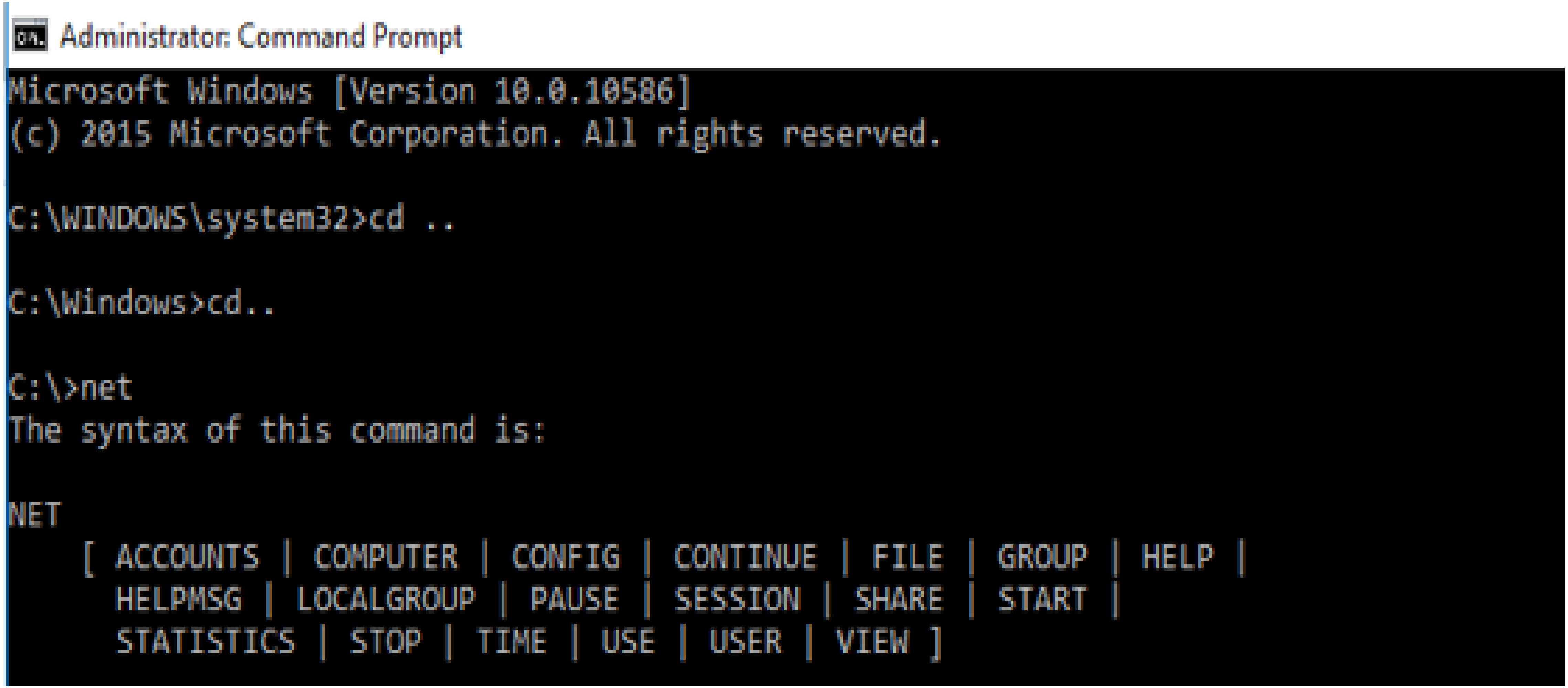
NetBIOS enumerating

1. Specific protocol and port
2. Name Resolution
3. Datagram Service
4. Session Service

NetBIOS service and ports

Application Protocol	Protocol	ports
NetBIOS Datagram Service	**UDP**	**138**
NetBIOS Name Resolution	**UDP**	**137**
NetBIOS Session Service	**TCP**	**139**

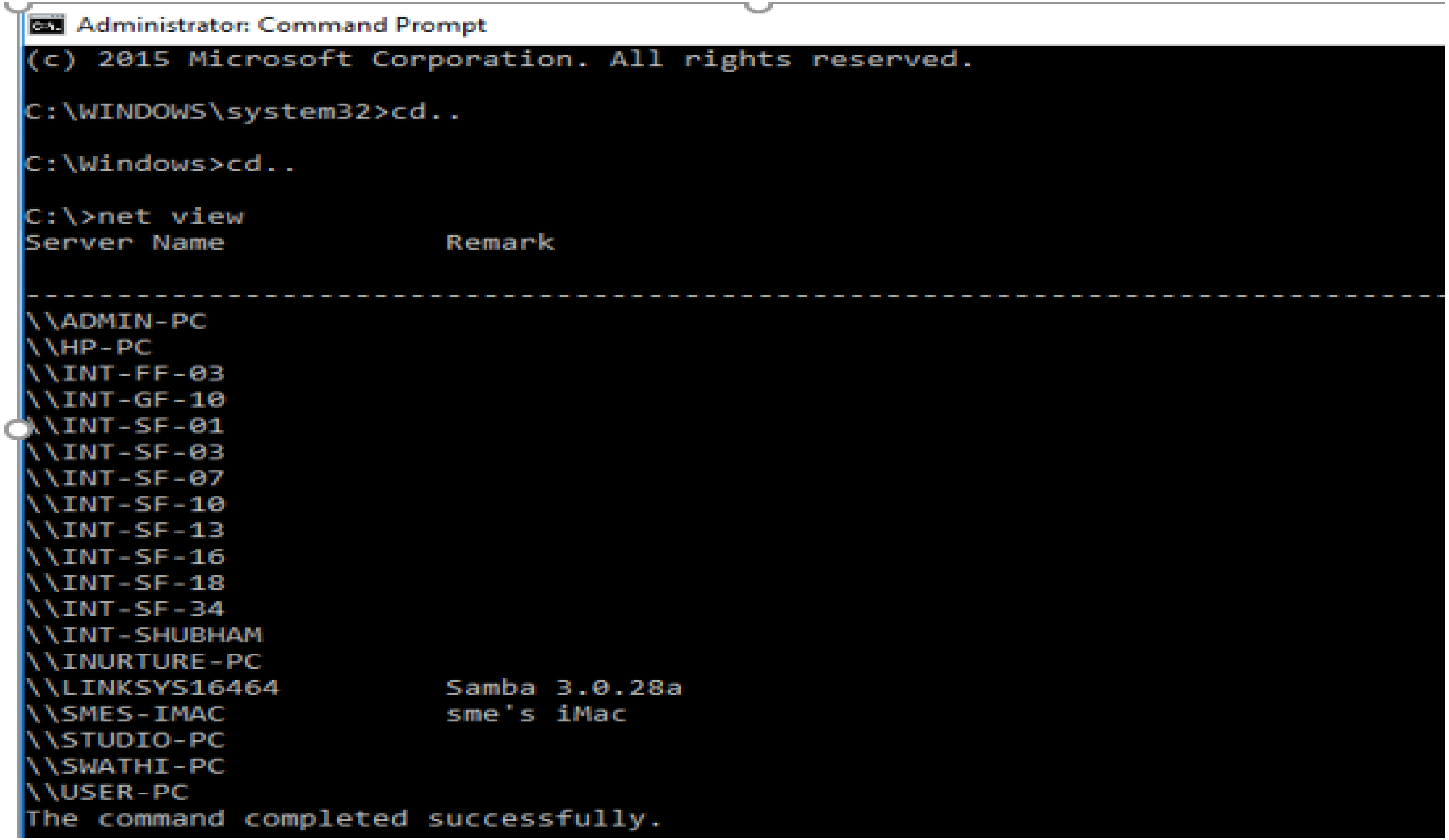
Net View



Administrator: Command Prompt

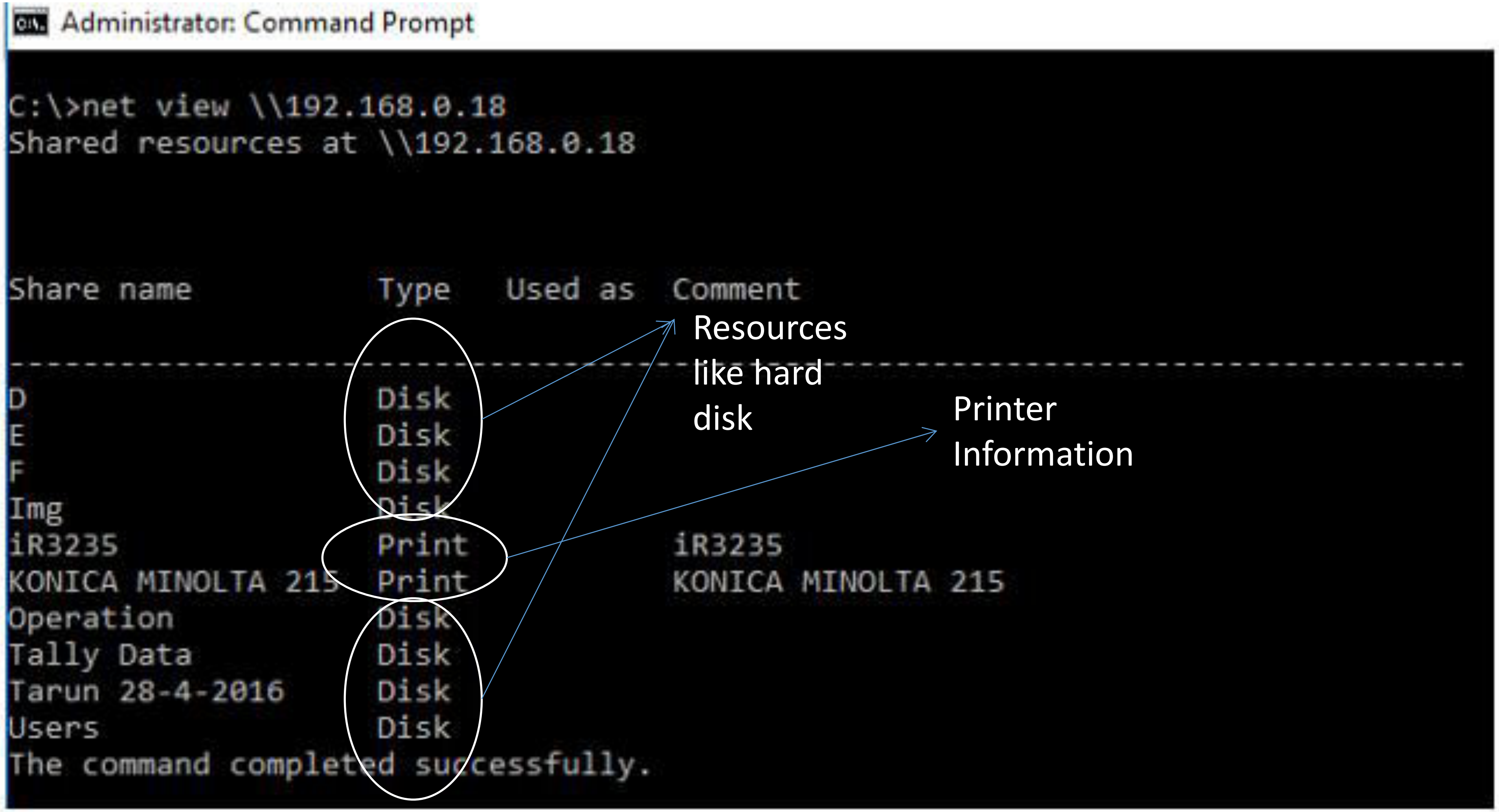
```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd ..

C:\Windows>cd..

C:\>net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Net View



```
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd..

C:\Windows>cd..

C:\>net view
Server Name            Remark

-------------------------------------------------------------------------------
\\ADMIN-PC
\\HP-PC
\\INT-FF-03
\\INT-GF-10
\\INT-SF-01
\\INT-SF-03
\\INT-SF-07
\\INT-SF-10
\\INT-SF-13
\\INT-SF-16
\\INT-SF-18
\\INT-SF-34
\\INT-SHUBHAM
\\INURTURE-PC
\\LINKSYS16464         Samba 3.0.28a
\\SMES-IMAC            sme's iMac
\\STUDIO-PC
\\SWATHI-PC
\\USER-PC
The command completed successfully.
```

Net View

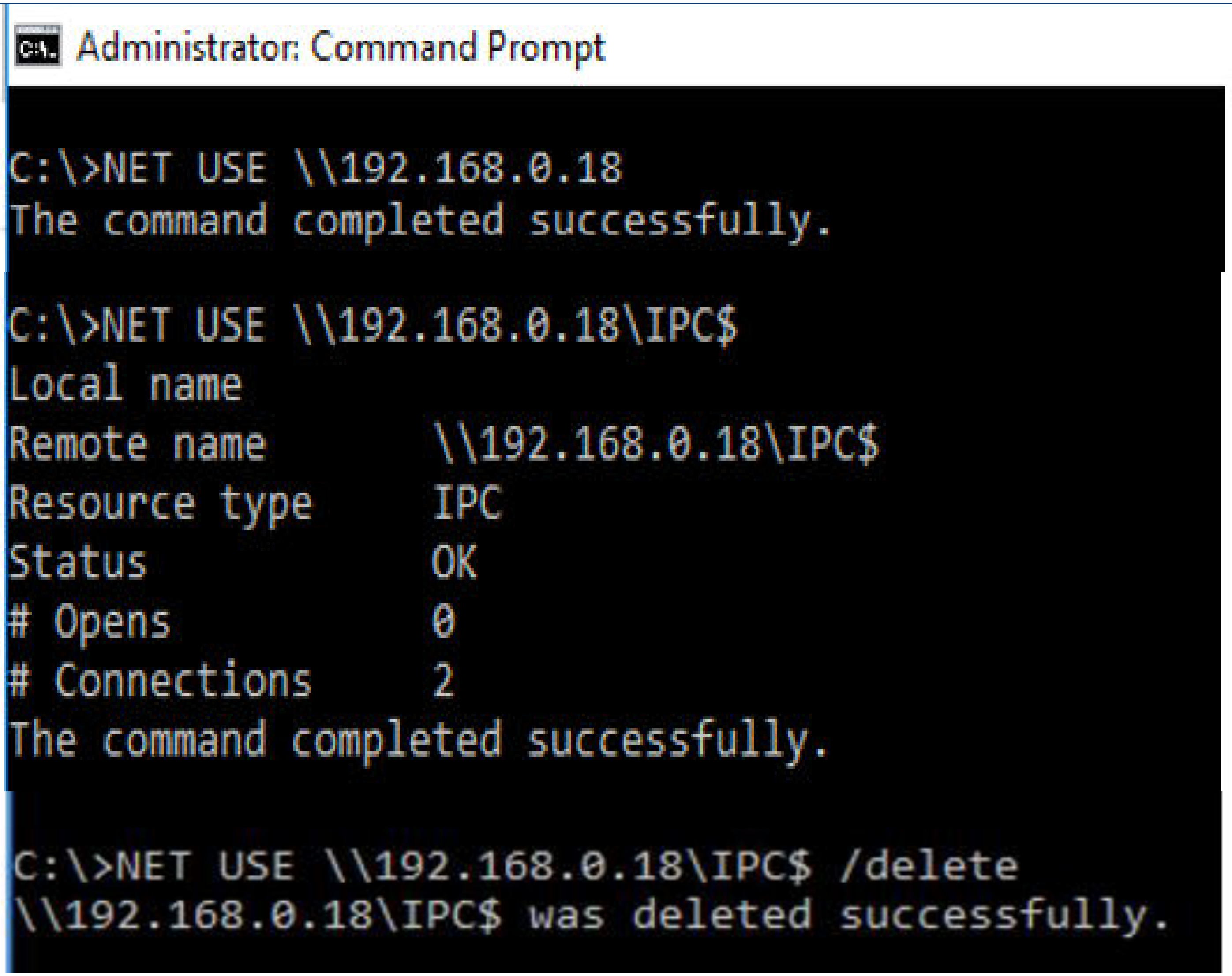


```
C:\>net view \\192.168.0.18
Shared resources at \\192.168.0.18



Share name           Type   Used as  Comment

-------------------------------------------------------------------------------
D                    Disk
E                    Disk
F                    Disk
Img                  Disk
iR3235               Print           iR3235
KONICA MINOLTA 215   Print           KONICA MINOLTA 215
Operation            Disk
Tally Data           Disk
Tarun 28-4-2016      Disk
Users                Disk
The command completed successfully.
```

Resources like hard disk

Printer Information

Net View



Administrator: Command Prompt

```
C:\>NET USE \\192.168.0.18
The command completed successfully.

C:\>NET USE \\192.168.0.18\IPC$
Local name
Remote name       \\192.168.0.18\IPC$
Resource type     IPC
Status            OK
# Opens           0
# Connections     2
The command completed successfully.

C:\>NET USE \\192.168.0.18\IPC$ /delete
\\192.168.0.18\IPC$ was deleted successfully.
```

Quiz / Assessment

1) Among the following, which doesn't belong to the set of information obtained by the hacker in the Enumeration phase?			
a) Users	b) Service Settings	c) Host names	d) DNS Infrastructure
2) An example of a NetBIOS exploiting tool is			
a) DumpSec	b) SNMP Informant	c) Userinfo	d) IP Network Browser

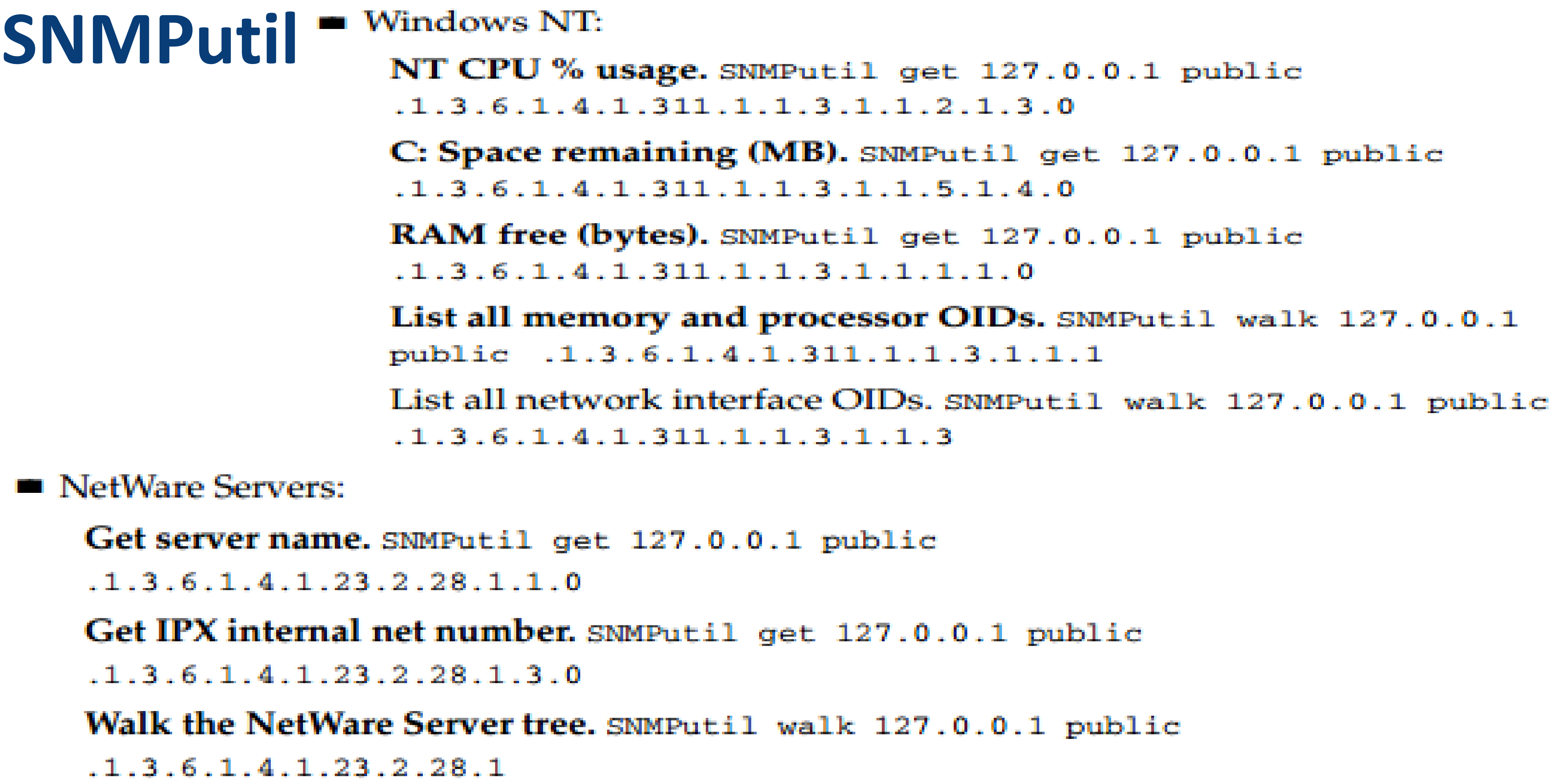
SNMP Enumeration

- Works on management station and agent
- Polling the network
- SMS alert in case of Failures
- Repeated validation
- Vulnerabilities
  - Default as ‘public’
  - Missing SNMP Community name
  - Unauthorized write access
  - Remote packet capturing

Tools in SNMP Enumeration

Tool	Source
SNMPutil	**Command line utility**
IP Network Browser	http://www.solarwinds.com/topics/ip-network-browser/
SNMP Informant	www.snmp-informant.com
Getif	http://www.wtcs.org/snmp4tpc/getif.htm
Trap Receiver and Trap Generator	http://www.trapreceiver.com/

SNMPutil



- Windows NT:

  NT CPU % usage. `SNMPutil get 127.0.0.1 public .1.3.6.1.4.1.311.1.1.3.1.1.2.1.3.0`

  C: Space remaining (MB). `SNMPutil get 127.0.0.1 public .1.3.6.1.4.1.311.1.1.3.1.1.5.1.4.0`

  RAM free (bytes). `SNMPutil get 127.0.0.1 public .1.3.6.1.4.1.311.1.1.3.1.1.1.1.0`

  List all memory and processor OIDs. `SNMPutil walk 127.0.0.1 public .1.3.6.1.4.1.311.1.1.3.1.1.1`

  List all network interface OIDs. `SNMPutil walk 127.0.0.1 public .1.3.6.1.4.1.311.1.1.3.1.1.3`

- NetWare Servers:

  Get server name. `SNMPutil get 127.0.0.1 public .1.3.6.1.4.1.23.2.28.1.1.0`

  Get IPX internal net number. `SNMPutil get 127.0.0.1 public .1.3.6.1.4.1.23.2.28.1.3.0`

  Walk the NetWare Server tree. `SNMPutil walk 127.0.0.1 public .1.3.6.1.4.1.23.2.28.1`

IP Network Browser

To identify the SNMP enabled devices

SNMP Informant

Used to monitor Servers

Getif

GUI Feature

Trap Receiver and Trap Generator

Either sending or receiving SNMP Traps

Counter Measures

1. Turning OFF SNMP
2. Additional restrictions for anonymous connections and, null sessions
3. SNMP with higher versions
4. ACN Filtering

Quiz / Assessment

3) Pick the odd man out and state your reasons

a) Querying DNS

b) Enumerating SNMP

c) Executing Whois Command

d) Retrieving information from the active directory

4) Which of the below is not a tool used for SNMP Enumeration

a) IP Network Browser

b) SNMP Informant

c) Getif

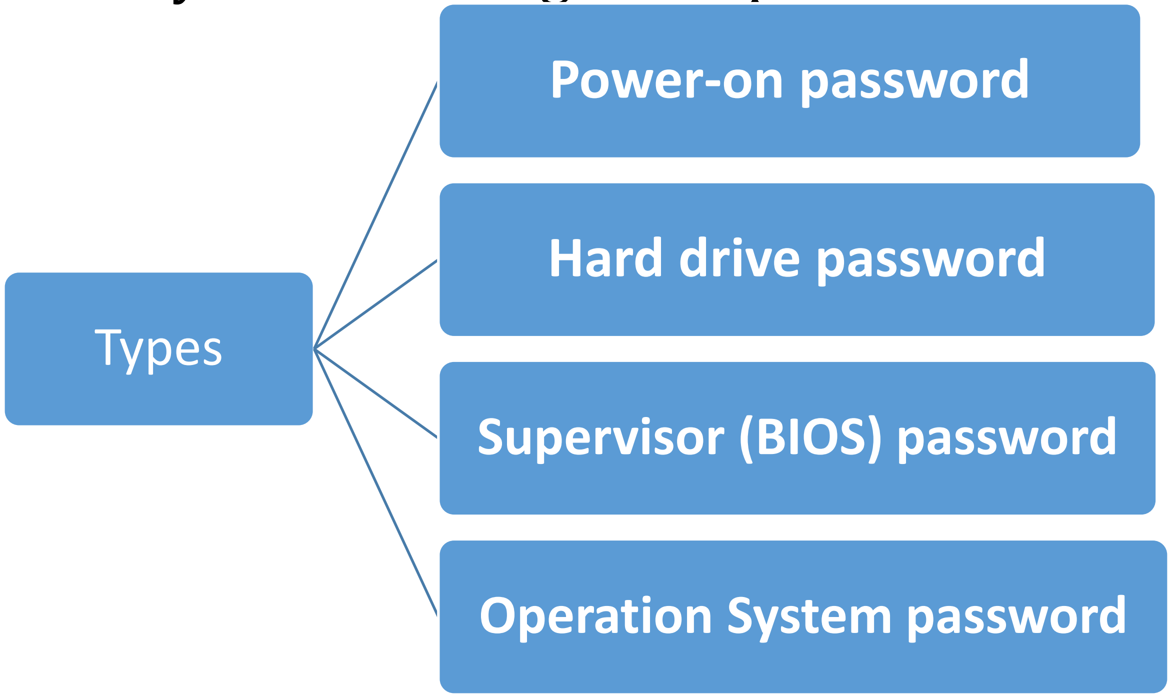
d) None of the above

System Hacking

To acquire	You need
Passwords for active user names	Knowledge of Password cracking techniques and tools
Allow yourself highest level of access possible by exploiting operating system vulnerabilities	Know how to escalate privilege
Crack password hashes	Know how to crack passwords using keyloggers and rootkits
Erase evidences of your presence, after the whole process	Hide files, cover tracks. Knowledge of steganography

Password Definition

- “a secret word or phrase that must be used to gain access to a computer, interface or system”
- Sequence of alphabets, numbers and special characters which is used as a secret key for accessing a computer or a network”



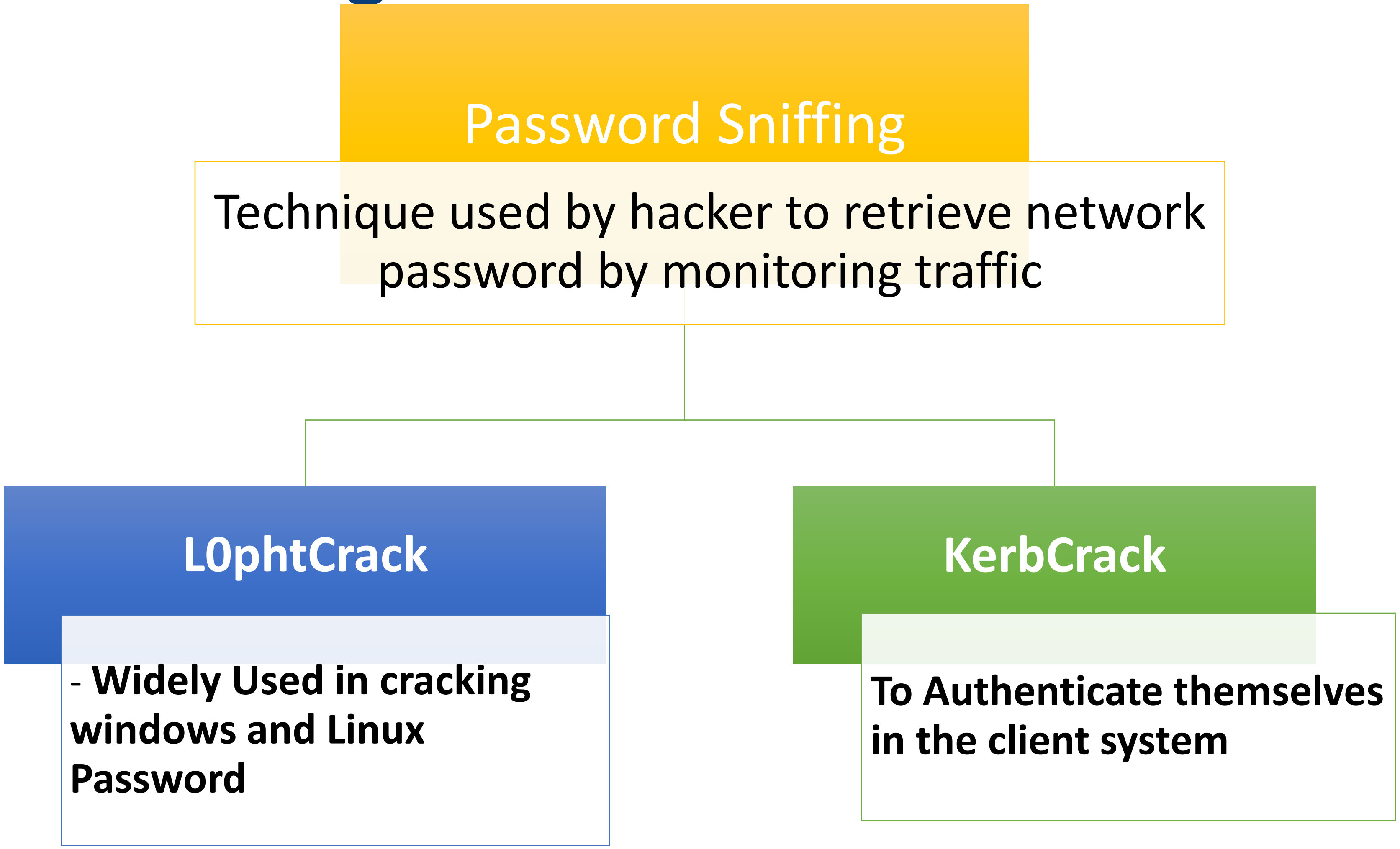
Password Guessing

```
Net use * \\target_IP \share * u:name
This will generate a password promt as below
C:\net use * \\10.1.1.13\c$ * /u:rusty
Type the password for \\10.1.1.13\$:
The command completed successfully
```

EXAMPLE

Automated Password Guessing (Legion, NetBIOS Auditing Tool)

Password Sniffing



Password Sniffing

Technique used by hacker to retrieve network password by monitoring traffic

L0phtCrack

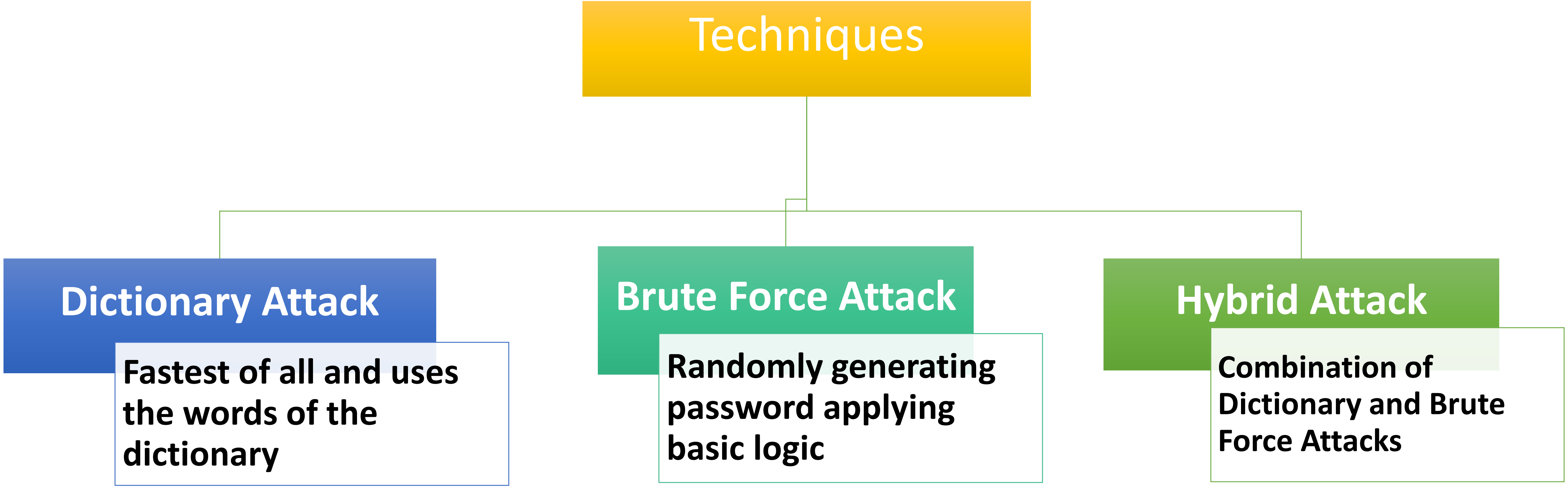
- Widely Used in cracking windows and Linux Password

KerbCrack

To Authenticate themselves in the client system

Password Cracking

- Two kinds of challenge/ response authentication
  - LanManager (LM) challenge/response
  - NTLM challenge/ response



Techniques

Dictionary Attack

Fastest of all and uses the words of the dictionary

Brute Force Attack

Randomly generating password applying basic logic

Hybrid Attack

Combination of Dictionary and Brute Force Attacks

Password Cracking Tools

Brutus

- Performs both dictionary and Brute Force Attack
- Applicable for multiple authentication types

WebCracker

- Implicates authentication password guessing
- Can recover username and password

Crack 5

- Fastest way for UNIX passwords
- Scans the content of the password file

Countermeasures for Password Cracking

Password between 7 to 12 chracters

- Includes lowercase, uppercase, numerical and special characters

Pocily on Password

- Change the password for every 30 days

Physical Safe Location for Servers

SYEKEY utility

- Store Password and hashes

Monitoring of event logs

Log all the failed login attempts

Block access to TCP and UDP ports

Quiz / Assessment

5) Which among the options is not a password sniffing tool?

a) KerbCrack b) ScoopLM c) Ethereal d) ISpyNow

6) Which one of the below options is not a password cracking technique?

a) Brute force attack b) Dictionary attack c) Rootkits d) Hybrid attack

Keystroke loggers

Hardware Key logger

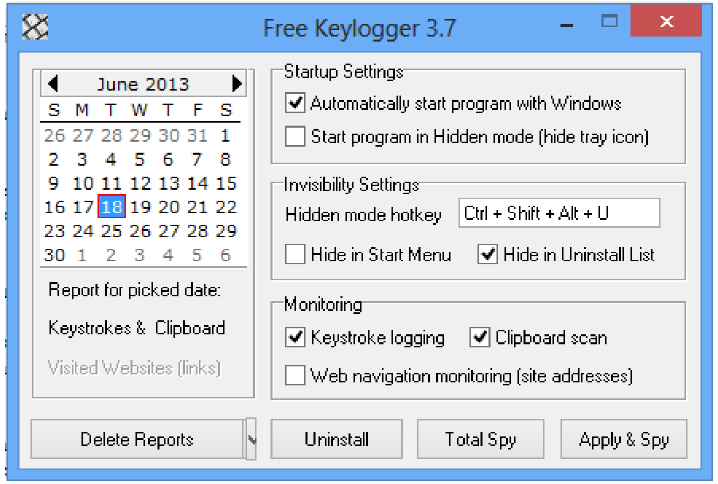
- When connect to the system it records and stores the user identity

Software Key logger

- It comprises of DLL and EXE to generate Troian files and costs much lesser

Key logging tools

- Refogkeylogger
- PC Activity Monitor
- IKS Software Keylogger
- KeyCaptor



Free Keylogger 3.7

June 2013

S	M	T	W	T	F	S
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Report for picked date:

Keystrokes & Clipboard

Visited Websites (links)

Startup Settings

☑ Automatically start program with Windows

□ Start program in Hidden mode (hide tray icon)

Invisibility Settings

Hidden mode hotkey: Ctrl + Shift + Alt + U

□ Hide in Start Menu ☑ Hide in Uninstall List

Monitoring

☑ Keystroke logging ☑ Clipboard scan

□ Web navigation monitoring (site addresses)

Quiz/Assessment

3) Normally, a software keylogger consists of two files

a) TXT and EXE	**b)** TXT and DLL	**c)** DLL and EXE	**d)** DOC and EXE

4) Which of the below options is *not* a keylogger tool

a) Remote Spy	**b)** PC Activity Monitor	**c)** Snort	**d)** ISpyNow

Rootkits

collection of software tools used by the cracker to obtain as well maintain administrative level access to the computer or network

Ntrootkit

Most commonly used ROOTKIT functions are

- monitors traffic and keystrokes
- creates a backdoor into the system
- modify log files
- attack other machines
- modify system tools

Some other Rootkits:

- Hack Defender
- Machiavelli
- Greek wiretapping
- Zeus
- Stuxnet
- Flame

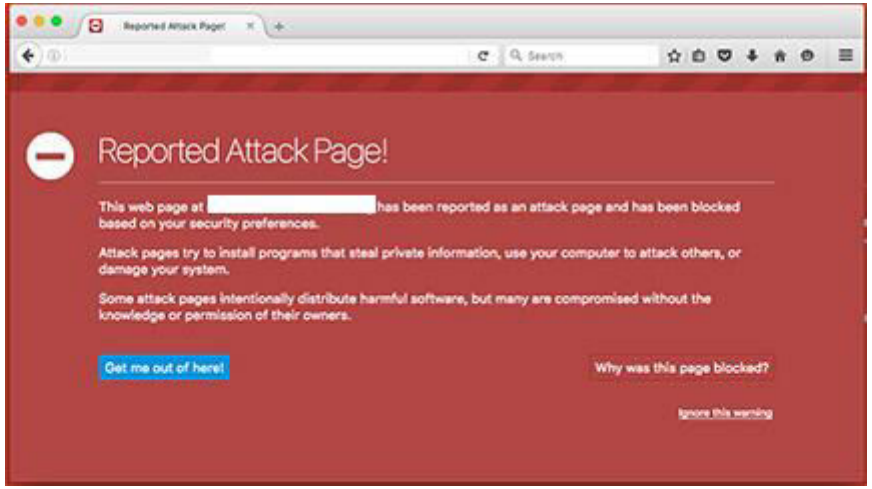
Countermeasures

1. backup information 2. Guanine Software 3. monitoring event viewer logs

Trojans

malicious piece of code used to install hacking software on target system, thereby helping the hacker to gain as well maintain access to that system

Trojan may manifest itself on the target by



Reported Attack Page!

This web page at [redacted] has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Most common way the Trojan horse is entered is by e-mail attachments and works on the register entries

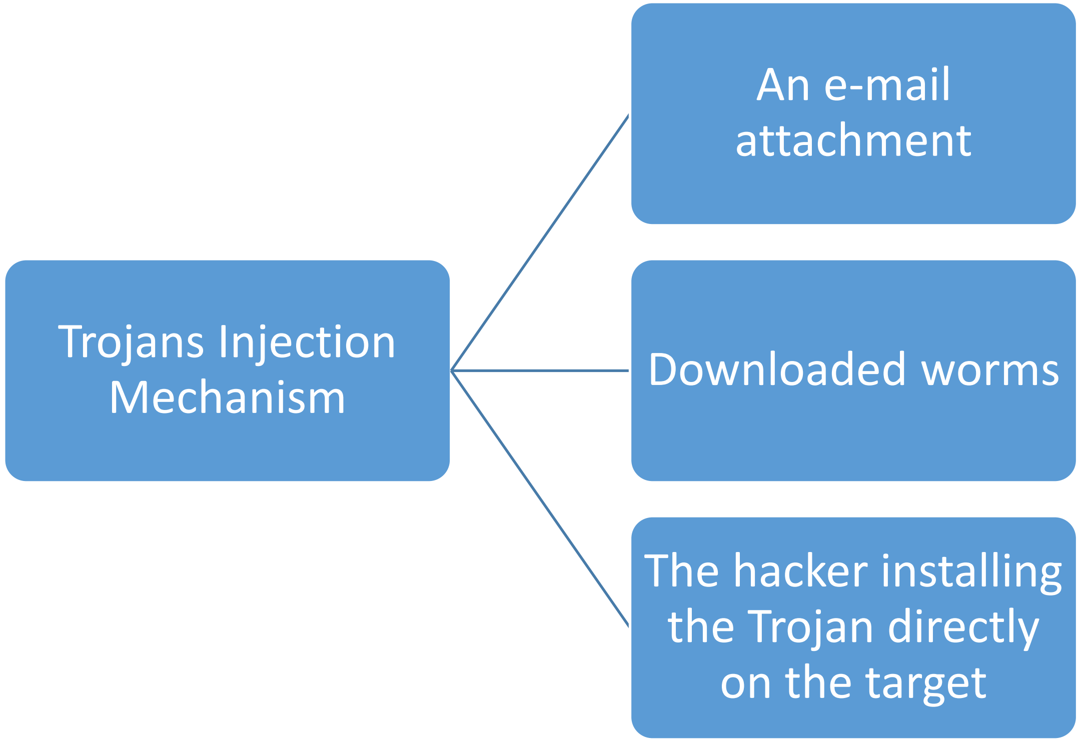
Trojans types

- Remote Access Trojans or RATS
- Keystroke loggers or password sending Trojans
- Software detection killers
- Purely destructive or service denying Trojans
- FTP Trojans

Goals

Data modification like *deletion*, *modification*, *blocking* and *copying* and leading to **disruptions like** performance of the computer and personal data collection

Trojans Injection Mechanism


Trojans Injection Mechanism
An e-mail attachment
Downloaded worms
The hacker installing the Trojan directly on the target

Attachment Vectors

- Email attachment
- Deception and Social Engineering
- Web bugs and drive -by downloads
- NetBIOS remote plants
- Physical access
- Attacks due to Windows and IE vulnerabilities
- Fake Executables and freeware
- Web pages that urge the users to install Spyware and adware

Trojans and its Countermeasures

- Programs that secretly allow access to a computers
- It comprises of both server and client components

Remote Access Trojans (RATS)

- Counseling the Trojan
- Wrappers

Distributing Trojans

Countermeasures

- Unknown Source usage to be stooped
- e-mails from the unknown source need to be blocked

Quiz/Assessment

7) You may become the victim of a Trojan attack when you just visit a website, without even downloading anything from it. This is referred to as

a) Freeware	b) NetBIOS remote plants	c) Drive-by downloads	d) backdoor

8) What is the attack vector used by counterfeit websites?

a) Physical access	b) Web bugs	c) Deception	d) Social Engineering

Summary

- ✓ In Enumeration, hacker will attempts to retrieve user account information, system groups and roles, password and any unprotected shares.
- ✓ Establishing null sessions and enumerating NetBIOS names, SNMP enumeration, DNS Querying and gathering Active Directory information are four techniques used for Windows enumeration
- ✓ Dumpsec and The NetBIOS Auditing Tool are two enumerating tools
- ✓ Value of default SNMP community string being PUBLIC, Missing SNMP Community name and Unauthorized write access are some of the SNMP vulnerabilities
- ✓ Disabling TCP 139 or TCP 445 ports, SMB Services and by restricting the anonymous user by modifying the registry entry are some of the means by which we can avoid NetBIOS null sessions
- ✓ Removing SNMP agent or turning off SNMP Services, maintaining guess community strings values that are not easy to guess. And restricting access to null session pipes and null session shares are recommended practices for preventing SNMP hacking
- ✓ Automated password guessing and Password sniffing are the two methods used for guessing a password
- ✓ Hardware keylogger and Software keylogger are the two types of keystroke loggers available
- ✓ Dictionary attack, brute force attack and Hybrid attack are the three types of password cracking techniques

e-References & External Resources

1. Read about ‘vulnerabilities of SNMP here. http://www.alphaguardian.net/the-failures-and-vulnerabilities-of-snmp/
2. A useful website to read all about rootkits ishttps://securelist.com/analysis/36055/rootkits-and-how-to-combat-them/
3. Different password types https://forums.lenovo.com/t5/General-Discussion-Knowledge/What-are-the-various-types-of-computer-passwords/ta-p/1166371
4. Differences between a hardware keylogger and a software keylogger https://www.microkeylogger.com/whats-the-difference-between-hardware-keylogger-and-keylogger-software.html

1. The CEH Prep Guide, the comprehensive guide to Certified Ethical Hacking by Ronald L. Krutz and Russell Dean Vines
2. Official Certified Ethical Hacker Review Guide by Kimberly Graves
3. Unofficial Guide to Ethical Hacking by Ankit Fadia

Activity

Online Activity
(20min)

Brief description of activity

Description:
Explain the working of Net View, NBTSTAT and Nbtscan by practically running these utilities on your computer and take the screen shots of the output result to make a report of the same.