System Hacking

Chapter 7

Gaining Access

- **What is gaining access?**
  - Breaking passwords
  - Opening up a system
  - Can lead to further actions

Password Cracking

The ability to crack passwords is a required skill to you as a penetration tester as passwords represent an effective way to gain access to a system.

- Passwords are the most widely used form of authentication.
- Usernames and passwords are a commonly targeted item.
- Enumeration may have gathered usernames in some cases.
- Password cracking is used to obtain passwords.
- Password cracking refers to a group of techniques.
- It is an essential skill for penetration testers.

What Makes a Password Susceptible to Cracking?

Passwords are intended to be something that is easy to remember but at the same time not easily guessed or broken.

- Passwords that contain letters, special characters, and numbers: stud@52
- Passwords that contain only numbers: 23698217
- Passwords that contain only special characters: &*#@!(%)
- Passwords that contain letters and numbers: meetl23
- Passwords that contain only uppercase or only lowercase: POTHMYDE
- Passwords that contain only letters and special characters: rex@&ba
- Passwords that contain only special characters and numbers: 123@$4
- Passwords of 11 characters or less

Password Cracking Types

Passive Online	• Sniffing
Active Online	• Brute force • Guessing
Offline	• Rainbow tables
Nonelectronic	• Social engineering

There are numerous techniques used to reveal or recover a password that you must explore, and each uses a different approach that can yield a password. Each method offers advantages and disadvantages that you should be familiar with.

Passive Online

A passive online attack is any attack where the individual carrying out the process takes on a "sit back and wait" attitude.

Characteristics of passive online

- Passive attacks adopt a "sit back and wait" attitude.
- Packet sniffers are a common mechanism to gather passwords.
- Weak password protection schemes are at risk.
- Many protocols of older varieties are vulnerable.

Protocols Vulnerable to Sniffing

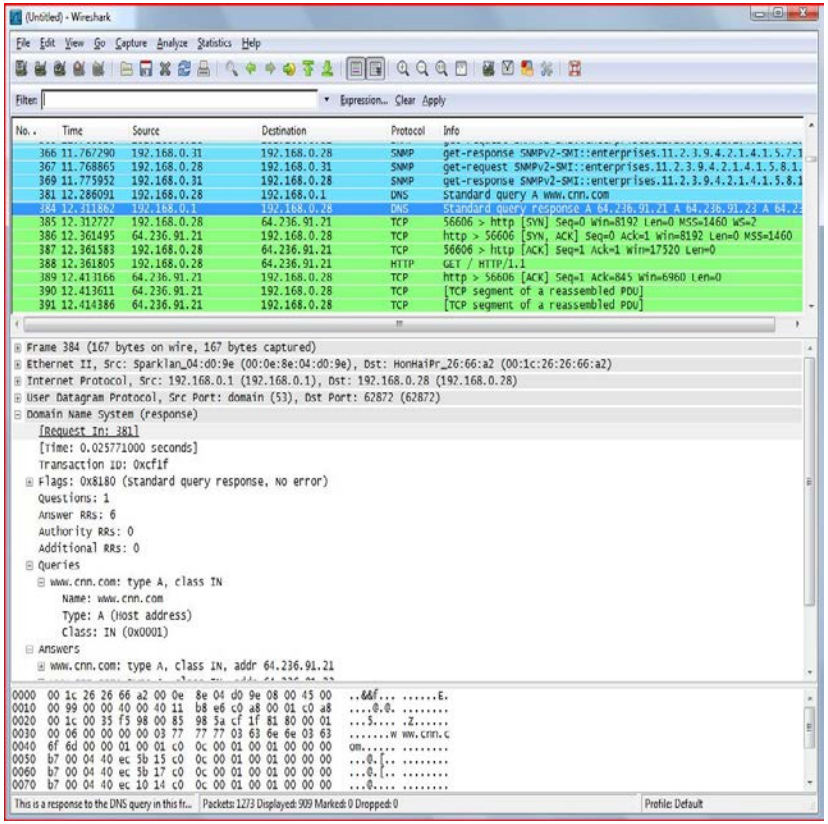
There are thousands of protocols that allow people to communicate via networks while also being used to hack into them.

- Telnet and rlogin (remote login): Using these protocols, anyone can access your keystrokes.
- HTTP: This protocol sends usernames and passwords in cleartext.
- SNMP: This is like HTTP; it sends passwords in cleartext.
- POP: This sends passwords in cleartext.
- FTP: This sends passwords in cleartext.
- NNTP: This sends passwords in cleartext.
- IMAP: This sends passwords in cleartext.

Tools for Passive Attacks

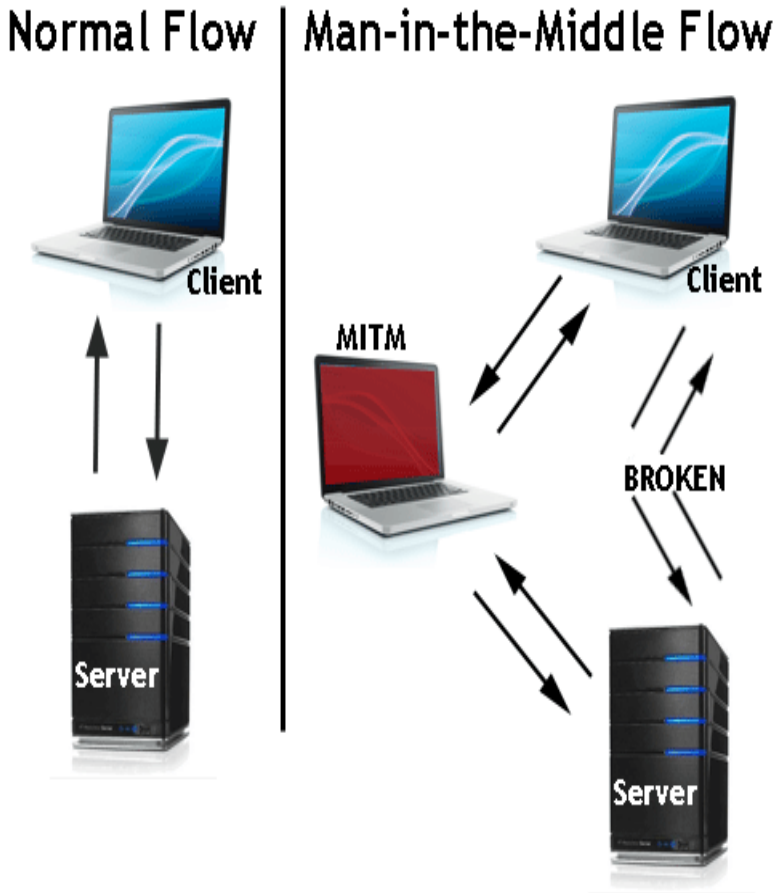
A network sniffers monitors data flowing over a network, which can be a software program or a hardware device with the appropriate software or firmware programming.

- **Wireshark**
- **Network Miner**
- **Network Monitor**
- **Dsniff**



Man-in-the-Middle

This type of attack takes place when two different parties communicate with one another with a third party listening in.



- Designed to listen in on the communication between two parties
- Can be completely passive if attacker just listens to communication
- Could become active attack if an attacker takes over the session
- Some protocols vulnerable to sniffing

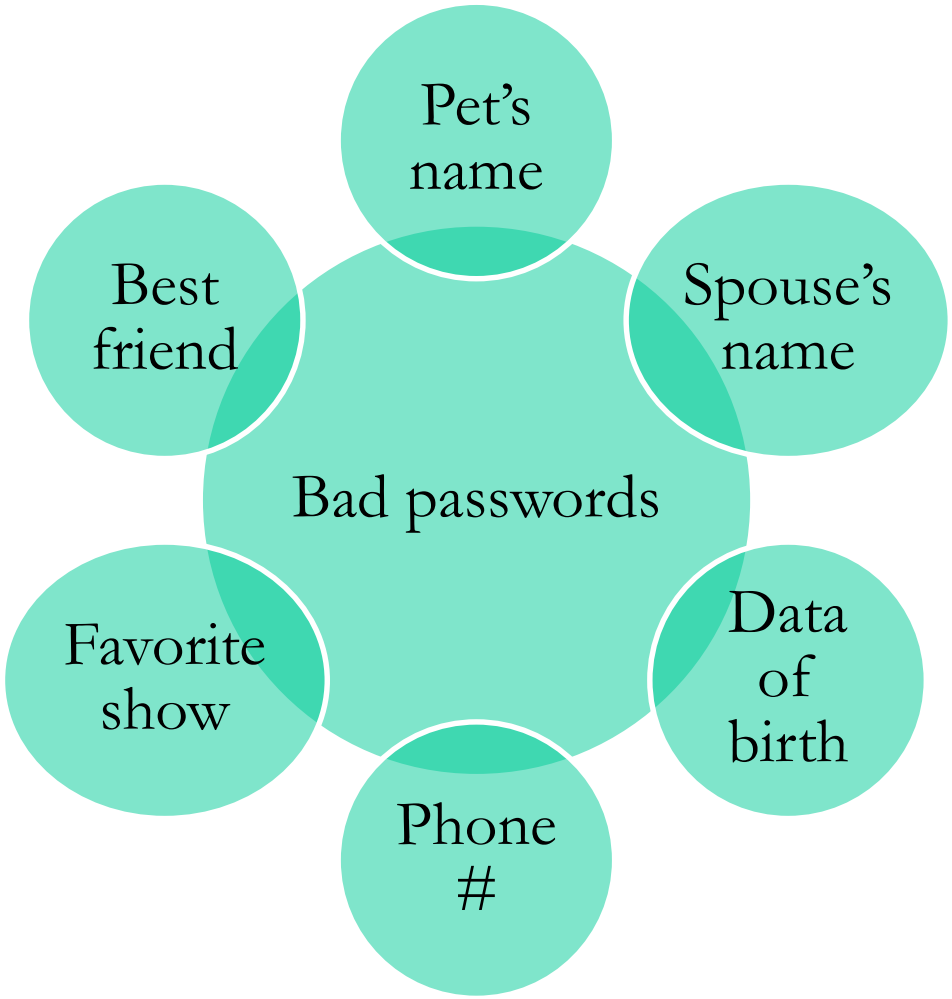
Active Online

Attacks that fit into this category are those that require direct interaction with a system in an attempt to break a password.

- **Guessing**
- **Malware**

Password Guessing

Password guessing is a valid and somewhat effective form of obtaining a password. During this process an attacker will attempt to gain a password by using a piece of software designed to test passwords.



Using Malware

In February 2005, Joe Lopez, a businessman from Florida, filed a suit against Bank of America after unknown hackers stole $90,000 from his Bank of America account. The money had been transferred to Latvia.

An investigation showed that Mr. Lopez's computer was infected with a malicious program, Backdoor.Coreflood, which records every keystroke and sends this information to malicious users via the Internet.

Malware is a class of software with no beneficial use.

Using Malware

- Keyloggers are a good example of malware.
- Keyloggers can be used to gain countless pieces of information.

Offline

- **Rainbow tables**
  - Uses precomputed hashes to identify password

What Is a Rainbow Table?

```
root@mybox:/usr/share/rainbowcrack# ls
alglib0.so  charset.txt  rcrack  readme.txt  rt2rtc  rtc2rt  rtgen  rtsort
root@mybox:/usr/share/rainbowcrack# rtgen md5 loweralpha-numeric 6 8 0 3800 334553
2 0
rainbow table md5_loweralpha-numeric#6-8_0_3800x3345532_0.rt parameters
hash algorithm:         md5
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 7
4 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
charset length:         36
plaintext length range: 6 - 8
reduce offset:          0x00000000
plaintext total:        2901650853888

sequential starting point begin from 0 (0x0000000000000000)
generating...
32768 of 3345532 rainbow chains generated (0 m 50.2 s)
e65536 of 3345532 rainbow chains generated (0 m 50.0 s)
98304 of 3345532 rainbow chains generated (0 m 51.3 s)
131072 of 3345532 rainbow chains generated (0 m 51.9 s)
163840 of 3345532 rainbow chains generated (0 m 50.3 s)
196608 of 3345532 rainbow chains generated (0 m 49.7 s)
229376 of 3345532 rainbow chains generated (0 m 50.9 s)
262144 of 3345532 rainbow chains generated (0 m 49.6 s)
294912 of 3345532 rainbow chains generated (0 m 49.9 s)
327680 of 3345532 rainbow chains generated (0 m 53.2 s)
360448 of 3345532 rainbow chains generated (0 m 52.0 s)
393216 of 3345532 rainbow chains generated (0 m 49.8 s)
425984 of 3345532 rainbow chains generated (0 m 56.2 s)
458752 of 3345532 rainbow chains generated (0 m 55.9 s)
491520 of 3345532 rainbow chains generated (0 m 53.5 s)
524288 of 3345532 rainbow chains generated (0 m 54.0 s)
557056 of 3345532 rainbow chains generated (0 m 55.1 s)
589824 of 3345532 rainbow chains generated (0 m 52.8 s)
622592 of 3345532 rainbow chains generated (0 m 50.6 s)
655360 of 3345532 rainbow chains generated (0 m 51.9 s)
688128 of 3345532 rainbow chains generated (0 m 53.5 s)
720896 of 3345532 rainbow chains generated (0 m 57.0 s)
753664 of 3345532 rainbow chains generated (0 m 51.1 s)
786432 of 3345532 rainbow chains generated (0 m 52.3 s)
819200 of 3345532 rainbow chains generated (0 m 52.6 s)
```

Rainbow tables are the end result of a process where every possible combination of characters is generated within certain limits.

- **Reduces difficulty in brute-force methods**
- **Generates hashes for every possible password**
- **Takes time to create hash table**
- **Faster than other types of attacks**
- **Effective against LAN Manager systems**

Privilege Escalation

Not every system hack will initially provide an unauthorized user with full access to the targeted system. In those circumstances, privilege escalation is required.

Privilege escalation

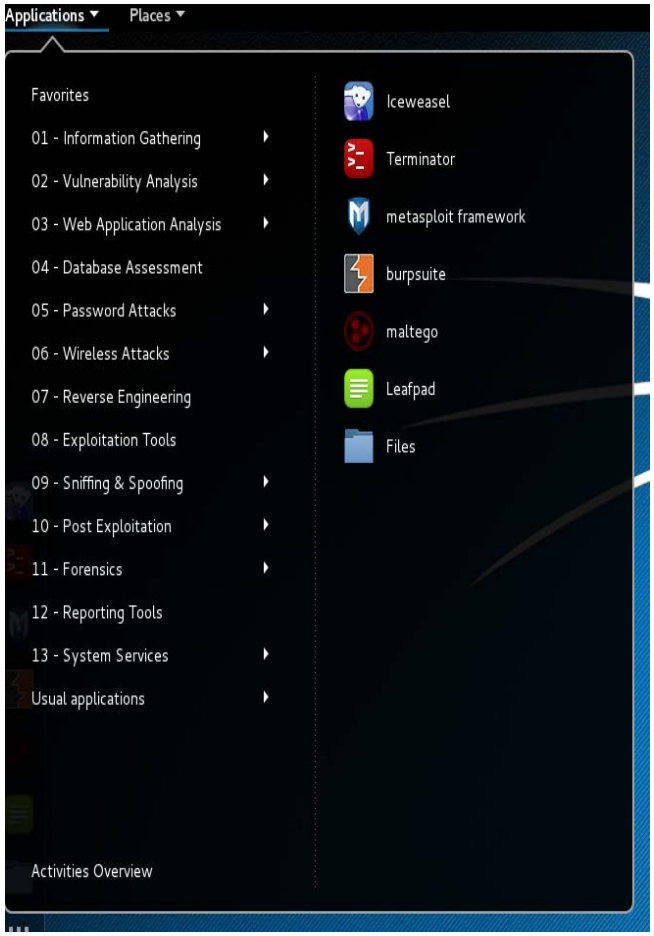
- Increasing access for compromised account
- Typically, breached account will not have broad privileges
- Raising privileges to a level where more actions can take place
- Can be vertical or horizontal

Privilege Escalation Types

Privilege escalation is the process where the access that is obtained is increased to a higher level where more actions can be carried out. The reality is that the account accessed typically will end up being a lower privileged one and therefore one with less access.

- **Vertical**
  - Raising the privileges of an account that has already been compromised
- **Horizontal**
  - Compromising one account and then another and another, each with an increased level of access

Tools for Privilege Escalation



- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Kali Linux
- Parrot OS
- Windows Recovery Environment (WinRE)
- Windows Password Recovery

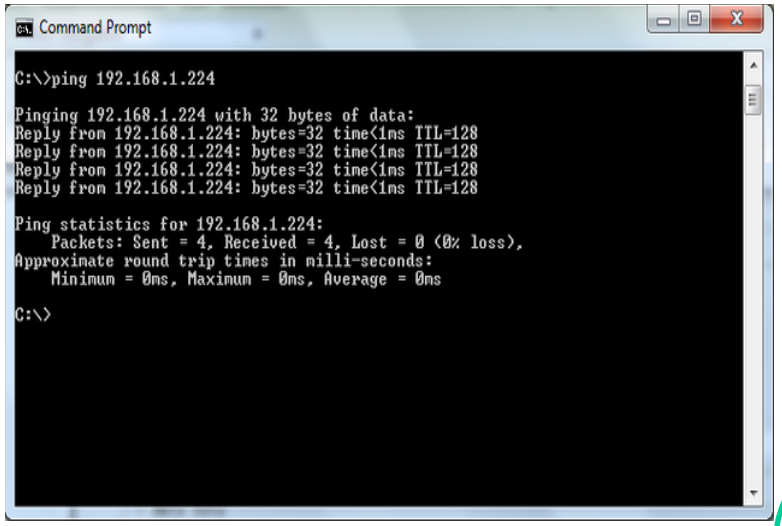
Opening a Shell

- LAN Turtle is a remote access pen testing tool
- Housed with USB network adapter
- Allows opening of a remote shell on a system
- With shell, open commands can be transmitted to remote system

What LAN Turtle enables is the ability to perform several attacks such as man-in-the-middle, sniffing, and many others.

Running Applications

When an attacker is executing applications on a system, they are doing so with specific goals in mind.



- Backdoors
- Crackers
- Keyloggers
- Malware

Covering Tracks

Important step in removing evidence

Leave no trace behind

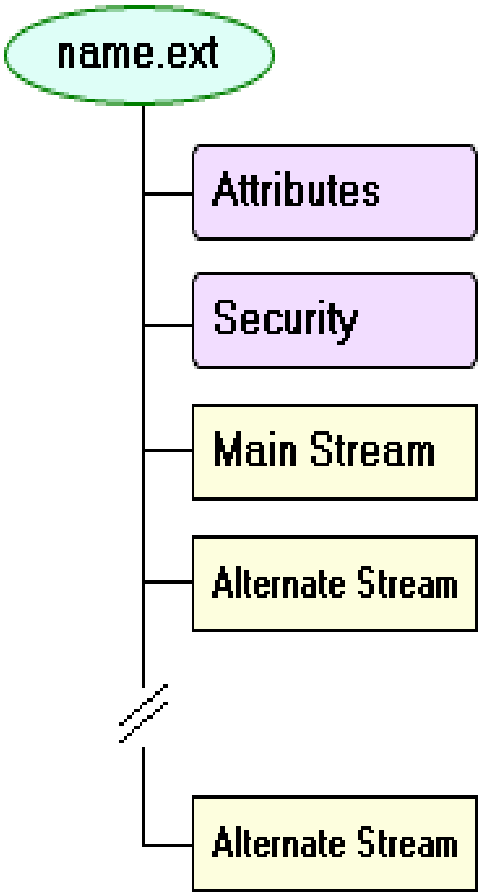
Eliminate or alter logs, error messages, and files

More evidence or tracks means greater chance of being detected

Working with Log Files

- Prevent leaving of information
- Disabling of auditing on a system
- May prevent or slow detection
- Surgical removal of entries in log files is possible

Alternate Data Streams



ADS was introduced into the Windows NTFS file system starting in Windows NT 3.1. This was implemented in order to allow compatibility with the Macintosh Hierarchical File System (HFS).

- Feature of NTFS file system
- Allows for compatibility with Macintosh file system
- Stores data in a nearly undetectable resource fork
- Tough to reveal presence of data stream
- Special software required to detect files

Summary

- What the process looks like
- Steps to take
- Tools to use
- Information to be obtained