Tool Demo: Metasploit/Armitage

Junkil Park

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

Penn Engineering

PRECISE

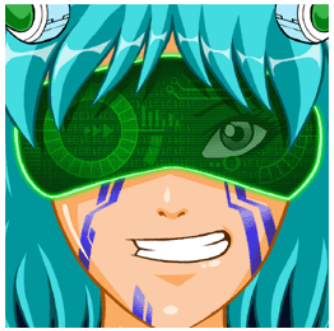
Outline

- Introduction to Metasploit/Armitage
- Demo
- Exercise

Metasploit/Armitage

- Metasploit
  - A **penetration testing** framework
  - Command-line user interface

- Armitage
  - A graphical user interface for Metasploit



Penetration test

- Also called
  - Pen test
  - Security test
  - White hat attack
- The practice of attacking a system to find vulnerabilities that an attacker could exploit
- Conducted with the system's owner's permission
  - Unlike black hat attack

Metasploit in a pen test

- Information gathering
  - Learning as much about a target as possible
  - E.g., open ports, running services, installed software
- Vulnerability scanning
  - Query systems for potential vulnerabilities
  - E.g., vsftpd 2.3.4 running on the system which has a backdoor
  - https://www.rapid7.com/db/
  - https://www.exploit-db.com/
- Exploitation
  - Triggering the vulnerability
- Post exploitation
  - Trying to gain further access to the target's internal networks by pivoting

Modules in Metasploit

- A module is a piece of software that can be used by the Metasploit Framework.

- Exploit module
  - Conducts an attack on the system that takes advantage of a particular vulnerability of the system
- Payload module
  - Executes in the vulnerable target system after exploitation of the system
- Auxiliary module
  - Typically, exploit without payload
  - E.g., Scanning and system enumeration

Demo

- Metasploitable
  - Intentionally vulnerable Linux virtual machine
- Metasploit console
  - Get a root shell through a backdoor in the ftp server
- Armitage

Exercise

- Install Kali Linux and Exploitable on Virtual Box
  - Kali: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
  - Exploitable: https://community.rapid7.com/thread/2007
- In Metasploit console, find out the version of ssh server of the target system using the following module:
  - auxiliary/scanner/ssh/ssh_version
- In Armitage, exploit the target system using the following exploit module without 'Hail Mary' command
  - exploit/multi/http/php_cgi_arg_injection

Thank you!

Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING