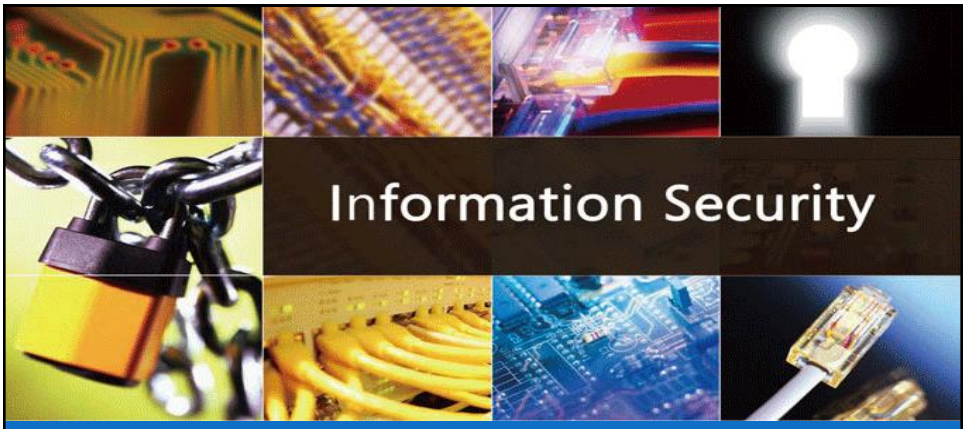

Operating Systems Security

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- OS vulnerability
- Operating Systems Hardening
- File system

File system

- Prepare
  - Install a Linux OS, ex Ubuntu
  - Practice some command in file system
    - Create directory: mkdir dir1
    - Create file: cat > f1
    - List file/directory: ls –la
    - Current directory: pwd
    - Change directory: cd dir1
    - Create user/group: useradd/groupadd

File system

- User Administration
  - Add user/ group, password
  - Set password policy - chage
  - Lock account
- File Permissions
  - umask, chmod
- File transfer
  - Install FTP server/client
  - Use specific accounts with limited permissions
- File sharing
  - Install Samba
  - Use specific accounts with limited permissions

Hardening OS

- Hardening Linux
  - Hardening Linux by John Terpstra, et al
  - Hardening Linux by James Turnbull
- Hardening Windows
  - Hardening Windows Systems by Roberta Bragg
  - Hardening Windows by Jonathan Hasell

5

Hardening OS - minimum

- Hardening Linux
  - Check services running on OS: cat /etc/services
  - Stop service: service <service_name> stop/start/restart
- Hardening Windows
  - Check services running on OS: run: **services**.msc
  - Disable/enable service

6

OS vulnerability

- List Windows/Linux OS vulnerability
- Prepare:
  - A PC as **victim** with OS vulnerability: windows (**xp** sp3) or linux
  - A PC as **attacker**: Kali Linux
    - Scan OS vulnerability using Nmap
    - Exploit OS vulnerability using Metasploit
  - Solution for OS vulnerability

OS vulnerability – Practice

- **Sử dụng Nmap và Nessus để scan các lỗ hổng trên máy client xp** sp3.
  - Sử dụng Script Engine của **Nmap** để scan lỗi hệ điều hành
  - Sử dụng **Nessus** để scan lỗi
  - Xác định lỗi cho phép từ xa truy cập và thực thi trái phép vào máy XP SP3
- **Khai thác lỗ hổng OS**
  - Thực thi quá trình attacker có thể dựa vào máy XP SP3 để chiếm quyền điều khiển máy Server
  - Crash windows xp bị blue screen với **Metasploit** using kali linux (Khai thác lỗ hổng **MS12-02** in Remote Desktop)
- **Đưa ra giải pháp khắc phục**
  - lỗi cho phép truy cập và thực thi từ xa máy XP SP 3

Practice Metasploit

- Start meta:

```
msfconsole
```

- Search:

```
msf>search ms12-020
```

- Set exploit:

```
msf> use exploit/windows/dcerpc/ms…
msf> set lhost <IP>
msf> set rhost <IP>
auxiliary/scanner/http/ms…
```


Q & A