INFORMATION SECURITY
Lab course

Lab Assistant Karina Vilegzhanina
k.vilegzhanina@gmail.com

November 9, 2015

Contents

Encryption and Signing with GPG, Gpg4win package

GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories.

Objectives

After completing this module you will be able to:

1. Create digital certificates
2. Encrypt files
3. Sign files

Agenda

1. Study the description and launch graphic tool Kleopatra
2. Create a key pair with OpenPGP (File → New Certificate)
3. Export Certificate (File → Export Certificate)
4. Sign/Encrypt Files (File → Sign/Encrypt Files)
5. Load other users certificates,
6. Import a certificate, sign it
7. Verify the signature
8. Using your partner certificate encrypt, sign and send her a file
9. Accept, check and decrypt a file from your partner
10. Following the instructions in GNU Privacy handbook (a link is in REFERENCE section in a bottom of this module) play with gpg by CLI,i.e. without graphic tool.

REFERENCE

1. GnuPG.org
2. GNU Privacy handbook
3. Ggp4win

Tools

Gpg4win - Windows package with gpg utility and a set of graphic tools GPA Kleopatra

Nmap ("Network Mapper") – a free and open source utility for network discovery and security auditing

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

Objectives

- After completing this module you will be able to:
    1. perform network discovery with various TARGET SPECIFICATION (hostnames, IP addresses, networks, etc.)
    2. perform HOST DISCOVERY
    3. apply a variety of SCAN TECHNIQUES
    4. perform PORT SPECIFICATION AND set SCAN ORDER
    5. perform SERVICE/VERSION DETECTION
    6. perform SCRIPT SCAN
    7. perform OS DETECTION
    8. manage TIMING AND PERFORMANCE
- You will be aware about FIREWALL/IDS EVASION and SPOOFING techniques

Agenda

Perform SERVICE/VERSION DETECTION in a RANGE:

1. List targets to scan
2. Probe open ports to determine service/version info
3. Study `nmap-services`, `nmap-os-db`, `nmap-service-probes`

4. (OPTIONAL) Add new service to `nmap-service-probes` (create a minimal tcp server, get its name and version by nmap)

5. Output to xml-format file

6. Study nmap stages and modes using Wireshark

Perform VM Metasploitable2 scanning using `db_nmap` from metasploit-framework

Get 5 records from nmap-service-probes and describe them. Choose one Nmap Script and describe it

REFERENCE

1. Nmap

2. nmap-service-probes file description

3. Nmap Script Engine, NSE

Tools

1. Nmap

2. Kali linux with Nmap, Wireshark and metasploit-framework

Impactful Penetration Testing Solution Metasploit

To take advantage of a system vulnerability, you often need an `exploit`, a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system. `Exploits` often deliver a `payload` to the target system to grant the attacker access to the system.

The Metasploit Project host the worlds largest public database of quality-assured exploits.

Objectives

After completing this module you will be able to:

1. Describe the steps of penetration testing process
2. Perform the basic pen testing operations
3. Learn the MSFconsole core commands and a variety of Metasploit tools
4. Learn how to use exploits to gain the access to the system

Agenda

Study

1. Basic concepts using documentation - `auxiliary`, `payload`, `exploit`, `shellcode`, `nop`, `encoder`
2. How to launch `msfconsole` and list available commands (`help`)
3. MSFconsole core commands `search` (name, type, author etc. search), `info`, `load`, `use`
4. Using exploits
5. Database Backend Commands
6. Metasploit GUIs – Armitage GUI front-end for the Metasploit Framework
7. Metasploit GUIs – web-client GUI

Exercises Describe a workflow when using:

1. VNC Scanner
2. SMB Login Check Scanner
3. Get root using `vsftpd` vulnerability
4. Get root using `irc` vulnerability
5. Armitage Hail Mary

Study three exploit source code files and explain them

REFERENCE

1. Metasploit Unleashed

Tools

1. Kali linux, with Nmap, Wireshark and metasploit-framework

802.11 WEP and WPA-PSK keys cracking program AirCrack

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

Objectives

After completing this module you will be able to:

1. Explore WiFi nets with a set of tools for auditing wireless networks
2. Capture and analyse WiFi traffic
3. Perform password-cracking attacks on WEP/WPA/WPA2 PSK

Agenda

Study

1. The core utilities – `airmon-ng`, `airodump-ng`, `aireplay-ng`, `aircrack-ng`.
2. Start a monitor mode on your wireless card
3. Launch `airodump`, study its output and file format

Exercise Crack a WPA2 PSK WiFi net (see REFERENCE)

1. Start monitor using `airmon-ng`
2. Start capture and analyse WiFi traffic `airdump-ng`
3. Use aireplay-ng to deauthenticate the wireless client (if needed)
4. Perform a dictionary attack

OPTIONAL Crack WEP (see REFERENCE)

REFERENCE

1. AirCrack
2. Airmon-ng
3. Airodump-ng
4. Aireplay-ng
5. Aircrack-ng
6. How to crack WPA/WPA2
7. How to crack WEP using AirCrack

Tools

1. Kali linux with AirCrack

A free online service Qualys SSL Labs – SSL Server Test

SSL Server Test performs a deep analysis of the configuration of any SSL web server on the public Internet.

Objectives

Agenda

Study

1. Learn how to deploy SSL/TLS correctly (see REFERENCE)
2. Learn SSL security issues – POODLE, HeartBleed (see REFERENCE)

Exercises

1. Choose one domain from a list of Recent Best and one from Recent Worst at SSL Server Test – study reports and explain their summary
2. Analyse a SSL-based domain:
    - Explain Summary
    - Explain the abbreviations in Configuration
    - Comment on Protocol Details
    - Conclude about SSL status

REFERENCE

1. SSL/TLS Deployment Best Practices
2. HeartBleed
3. POODLE attack on TLS
4. POODLE attack on SSL3

Tools

1. Qualys SSL Labs – SSL Server Test

OWASP WebGoat

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security

Objective

Agenda

Study

1. Using OWASP Top Ten Project (see REFERENCE)study top 10 web vulnerabilities

Exercises

1. Install and launch WebGoat (see REFERENCE)
2. Launch ZAP security scanner, configure it as a local proxy-server. NOTE: Please, use different port numbers for ZAP and WebGoat.
3. Launch Mantra, set it to use ZAP as proxy-server (Top left → Tools → Settings)
4. Follow WebGoat LESSONS

REFERENCE

1. OWASP WebGoat Project
2. OWASP Top Ten Project

Tools

1. WebGoat
2. OWASP Mantra
3. OWASP ZAP
4. (OPTIONAL)Telerik Fiddler