Ethical Hacking & Penn Testing

CATALIN BOJA & ALIN ZAMFIROIU

WWW.ISM.ASE.RO

Course

- What is and other info
- Anonymity
- Footprinting
- Password cracking
- Hacking using Social Engineering
- Network Sniffers
- Hacking a Web Site
- Hacking a Web Server
- Hacking a Wireless Network

Ethical Hacking Knowledge

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Disclaimer

- Don’t use these techniques and tools outside the laboratory environment
- Don’t use these techniques and tools and break any law in any country
- Don’t use these techniques and tools on services/computers/servers for which you don’t have permission to access
- We are not responsible for the illegal use of these techniques and tools

Disclaimer

The objectives of this course/presentation are:

- To increase the awareness regarding the digital trail that you leave
- To increase the awareness of your privacy on Internet
- To show you how the attacker perspective and tools
- To help you get an idea about tools and procedures used to hack

It’s NOT an objective of this presentation:

- To show you tools that you may use to conduct illegal activities

Ethical hacking

- What is ?
- Ethical – *conforming to accepted standards of conduct, ethical behavior* (Merriam-Webster dictionary)
- Hacking – make a system do what you want to do versus was was intended to do
- Types of hackers (https://en.wikipedia.org/wiki/Security_hacker):
  - White/Grey/Black hat
  - Script kiddie
  - Neophyte ("newbie", or "noob")
  - Hacktivist
  - Nation state

Key terms

- **Footprinting** – information gathering, pre-analysis (in digital and real world)
- **FUD** – Fully Undetectable for anti-virus
- **RAT** – Remote Administration Tools
- **Root kit** – tool installed on a OS that will help hide some processes (you will not see it in Task Manager)
- **Key loggers** – tools to steal and extract information
- **Reverse shells** – programs that will infect a device in order to open a command & control connection
- **Terminal** – command interface for Linux/Unix
- **Firewall** – controlling network inbound and outbound traffic (in Linux with IP table commands)

Key terms

- Attacks:
  - **DoS** – Denial of Service (make more requests than the server can manage; for ex. Apache server ~ 10000 requests by default); involves a single machine
  - **DDoS** – Distributed Denial of Service is a DoS conducted synchronous from multiple clients over the same target
  - **Phishing** – try to trick users using legit look like messages or websites to reveal information
  - **SQL Injections** – exploit SQL language to retrieve database information from the application interface

Key terms

- Tools:
  - **VPN** – Virtual Private Networks
  - **Proxy** – reroute traffic
  - **Tor** Browser/Network
  - **VPS** – Virtual Private Servers (ex. Make a internal SQL Server in a virtual machine)

Tools

- **Virtual Box**
  - https://www.virtualbox.org/
  - A virtualization environment to run a Linux virtual machine
- **Kali Linux**
  - https://www.kali.org/downloads/
  - A Linux distribution with a lot of useful tools
  - You need to install it in a virtual machine
- Any additional tools – most of them are Linux tools
- **Time** - this not works like in movies. It takes a lot of planning, effort, time and perseverance to get results

Necessary skills

- Always try to preserve your anonymity (avoid Windows OS, use VPNs, Proxys and Linux distributions)
- Always get open source tools and build them yourself or download them from verified sources
- Patience, perseverance and imagination – in some cases the needed information is not digital
- Curiosity – think out of the box and try thinks which may seem impossible to happen (like default passwords)

Anonymity - Tools

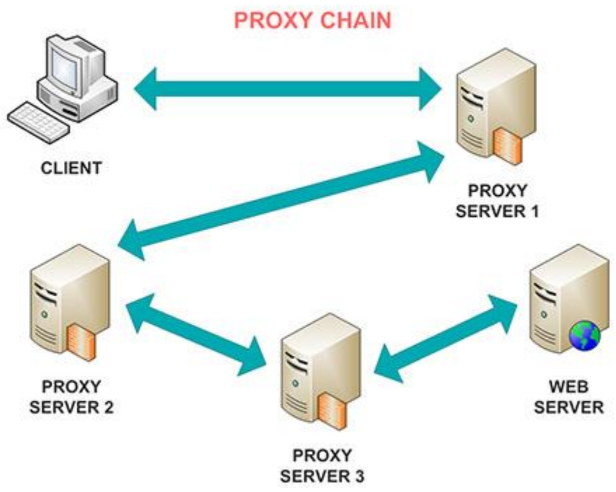
- VPN
- Browser
- File sharing and communication tools
- Recommended reading:
  - https://privacytoolsio.github.io/privacytools.io/

Anonymity - VPN

- Commercial services that have monthly/yearly costs
- Fast than proxy chains
- Encrypt data connection between you and the VPN server
- Some keeps logs, some not (don't expect to have "zero logs" policy)
- Some services may respond to government agencies requirements (see the Lavabit example)
- Check their service conditions (terms of use) - https://torrentfreak.com/vpn-services-keep-anonymous-2018/

Anonymity - Proxy

- Allow rerouting the network traffic through multiple Internet nodes (proxy)
- Is slow – efficient for small data transfers
- **Proxychains**
  - A Linux tool - configure it by editing */etc/proxychains.conf*
  - Supports HTTP, SOCKS4 and **SOCKS5** proxy servers
  - Types: dynamic/strict/random



https://proxyradar.com/kb/

Anonymity – Tor Network

- For anonymous browsing and network communications
- https://www.torproject.org/
- It’s a distributed, anonymous network in which multiple layer encryption is used to protect the connection data between intermediary nodes. Each relay sees only the information needed to reach the next node - https://www.torproject.org/about/overview.html.en
- For Linux you can install it with ***apt-get install tor*** or download it
- After download you can check the hash value with ***sha1sum***
- For Kali – update https://docs.kali.org/general-use/kali-linux-sources-list-repositories
- Check HiddenWiki for information

Anonymity - Proxy

1. Edit the proxychains config file - */etc/proxychains.conf*
2. Add the Tor proxy ***socks5 127.0.0.1 9050***
3. Check tor status with ***service tor status***
4. Start if needed ***service tor start*** or ***service tor restart***
5. Start the browser or any other app with proxychains
   1. ***proxychains firefox www.dnsleaktest.com***
   2. ***proxychains nmap***
6. Stop the service ***service tor stop***

Anonymity - Warrant canary

- a posted document stating that an organization has not received any secret subpoenas during a specific period of time
- Example:
  - https://www.vpnsecure.me/files/canary.txt
  - https://www.ivpn.net/resources/canary.txt

Anonymity - Browser

- Recommended: **Firefox**, Tor Browser, Brave
- **Browser fingerprint** - configuration, such as available fonts, browser type, and add-ons. If this combination of information is unique then you can be tracked - https://panopticlick.eff.org/
- **WebRTC** - is a new communication protocol that relies on JavaScript that can leak your actual IP address from behind your VPN - https://privacytoolsio.github.io/privacytools.io/webrtc.html

Anonymity - Browser

- Firefox settings (about:config) to disable WebRTC
  - media.peerconnection.enabled = false
  - media.peerconnection.turn.disable = true
  - media.peerconnection.use_document_iceservers = false
  - media.peerconnection.video.enabled = false
  - media.peerconnection.identity.timeout = 1
- Can’t disable it in Chrome

Anonymity - Browser

- privacy.trackingprotection.enabled = true
- geo.enabled = false
- browser.safebrowsing.phishing.enabled = false
- browser.safebrowsing.malware.enabled = false
- dom.event.clipboardevents.enabled = false
- webgl.disabled = true
- dom.battery.enabled = false
- browser.sessionstore.max_tabs_undo = 0

Anonymity - Browser

- network.cookie.cookieBehavior = 1 (Disable cookies, 0 = Accept all cookies by default, 1 = Only accept from the originating site (block third party cookies), 2 = Block all cookies by default
- network.cookie.lifetimePolicy = 2 (cookies are deleted at the end of the session, 0 = Accept cookies normally, 1 = Prompt for each cookie, 2 = Accept for current session only, 3 = Accept for N days
- browser.cache.offline.enable = false
- browser.send_pings = false
- webgl.disabled = true
- dom.battery.enabled = false
- browser.sessionstore.max_tabs_undo = 0

Anonymity - Browser

- Firefox Privacy Add-ons
  - uBlock Origin - https://addons.mozilla.org/firefox/addon/ublock-origin/
  - Self-Destructing Cookies - https://addons.mozilla.org/firefox/addon/self-destructing-cookies/
  - HTTPS Everywhere - https://www.eff.org/https-everywhere
  - Decentraleyes - https://addons.mozilla.org/firefox/addon/decentraleyes/

Anonymity – Canary Cookies & Tokens

- **Canary Cookies** - cookies generated by different websites and checked on cross domains
  - https://www.nfriedly.com/techblog/2010/08/how-facebook-sets-and-uses-cross-domain-cookies/
- **Canary Tokens** – hidden links that are triggered when you visit a link, open a document, run an application, read an email, etc.
  - http://canarytokens.org/generate

Anonymity - Email

- Use email services that provide message encryption (ProtonMail, mailbox.org and others)
- Use your own service: Mail-in-a-Box
- Test your privacy https://www.emailprivacytester.com/
- Use open source email clients: Thunderbird
- Email alternatives (decentralized and distributed systems): I2P-Bote, RetroShare, Bitmessage

Anonymity – Searching engines

- Don’t use Google or any search engine that records your searching activity and links to your profile
- https://duckduckgo.com/
- https://searx.me/
- https://www.qwant.com/
- https://www.startpage.com/
- Firefox add-on: Google search link fix

Anonymity - Communication

- Mobile: Signal
- Wire - https://app.wire.com/?connect
- Ricochet - https://ricochet.im/

Anonymity – Cloud storage

- Use services that encrypt the data on the client using local keys: Seafile, Nextcloud
- Self-hosted cloud server: Seafile, Pydio
- File sync software: SparkleShare, Syncany, Syncthing

Anonymity – DNS Leaking

- When you query a domain name like www.ism.ase.ro you send a request to a DNS server (set up by your ISP, proxy server, VPN server, etc);
- The DNS owners may log the information so they can associate queries for visited websites to a specific IP
- If you are connected to a VPN service the DNS leak may reveal information about the DNS servers you use – if they are related to your ISP then your real location is not protected by the VPN service (is not your real IP service but they have info on your real ISP)
- Use public Open DNS servers https://www.opendns.com/setupguide/ (208.67.222.222 · 208.67.220.220)
- Google DNS server is 8.8.8.8 or Cloudflare DNS server 1.1.1.1
- https://www.dnsleaktest.com/results.html

Anonymity – Live USB OS

- **Live CD OS**: Tails, Knoppix, Puppy Linux, Kali Light (https://docs.kali.org/downloading/kali-linux-live-usb-install)
- Tools
  - USB Stick - https://rufus.ie/
  - OS image file
  - Image Writer (for Windows) - https://launchpad.net/win32-image-writer
  - dd for Linux

Anonymity – MAC Changer

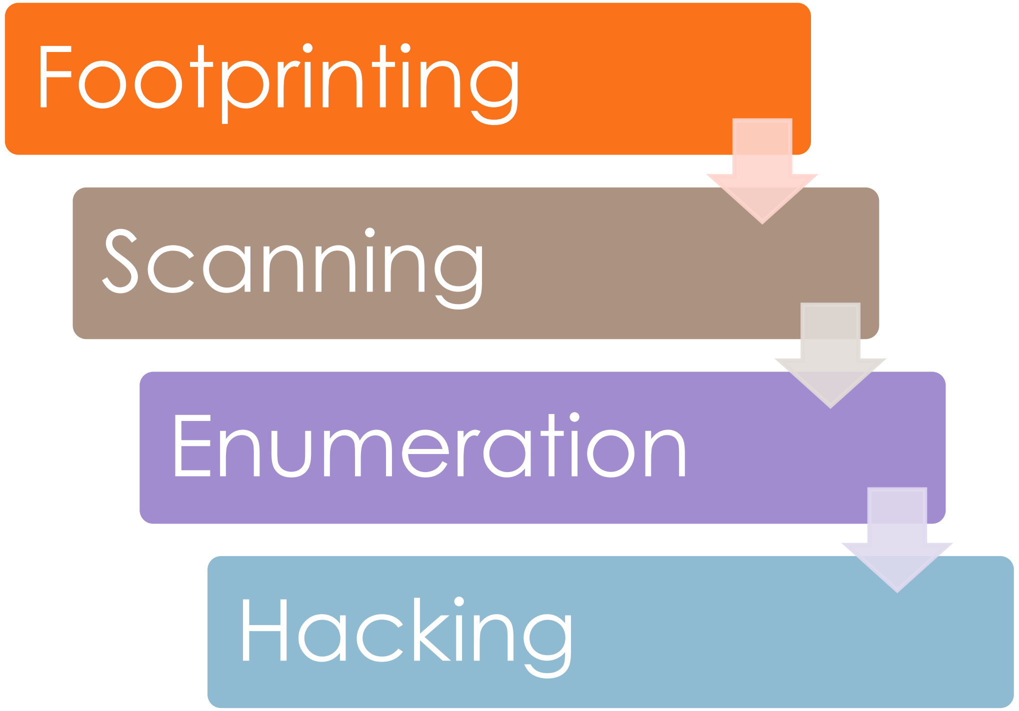
- MAC Address - https://en.wikipedia.org/wiki/MAC_address
- It will uniquely identify the network (Wired or Wi-Fi) board in the LAN
- The value is visible in our current LAN (until the next node)
- Important for Wi-Fi connections as the router will record it
- You can lookup for MAC vendors - https://macvendors.com/
- You can change it:
  - For Windows - https://www.groovypost.com/howto/change-mac-address-windows-10-why/
  - For Linux - https://linuxconfig.org/change-mac-address-with-macchanger-linux-command

Anonymity – Other

- **Password managers**: Master Password, KeePass
- **File encryption**: VeraCrypt, PeaZip, GnuPG
- **DNS**: DNSCrypt, OpenNIC
- **Digital Notebook**: Laverna, Turtl, Simplenote, Paperwork
- **Paste services**: Ghostbin, PrivateBin, Hastebin
- **Productivity tools**: Etherpad, Ethercalc, ProtectedText

Footprinting

- Gathering information on the target/company/organization without noise
- Prepares the scanning phase
- It's a stealthy operation
- It should gather as much information from mostly public information
- Active vs Passive activity



Footprinting

- Possible results
  - Organizational information
    - Employee accounts and email addresses
    - Company directories
    - Hidden and internal websites
    - Used Technology (OSs and versions)
    - Geo-location and phone numbers
  - Network map of resources (servers, websites, etc.) – domain names, topology
  - Potential obstacles
  - Accounts, services and persons of interest

Footprinting

- Collecting Location Information – geographic locations and surroundings
  - Google maps
  - Wikimapia
  - Bing maps
- Netcraft & Shodan
  - Determine IP blocks, Hostnames, Banner grabbing, Default passwords
- People Information
  - Pipl.com, Facebook, LinkedIn

Footprinting

- **People Information**
  - Sometimes is the weakest link in the security chain
  - Pipl.com, Facebook, LinkedIn
  - Personal & contact information
  - Personal context: friends, relatives, interests, events, hobbies, personal likes
  - Social engineering
  - Spoofing
  - Malware dissemination

Footprinting

- Jobsites and communities
  - Jobs announcements
  - Skills and technologies
- Financial Information
- Setting up alerts using Google
  - https://www.google.com/alerts

Google Hacking

- Use Google index to search for public information
- Queries can detailed using different tags
  - ext – extension
  - intext – containing text
  - http://www.googleguide.com/advanced_operators_reference.html
- **Google Hacking Database**
  - Predefined Google queries - Dorks
  - https://www.exploit-db.com/google-hacking-database

Website footprinting

- Website proxies
- Website mirroring
- Web spiders
- Web site monitoring
- Cached content
- Web archive

Website footprinting

Website proxies

- Tools: Burp Suite, FireBug (now Firefox Developer Tools)
- Information that can be collected:
  - OS and version
  - JavaScript libraries
  - JavaScript and HTML Code comments
  - Webserver info
  - Contact info
  - Cookies info

Website footprinting

Website mirroring

- Creates a local copy of the website
- Keeps the directory structure
- Tools
  - HTTrack
  - BlackWidow

Website footprinting

Web spiders / miners

- Tools used to extract specific information
- Tools
  - Web data extractor
  - Web Data Miner
  - Visual Scraper
- Web site monitoring
  - Monitors a website for changes
  - www.followthatpage.com
- Web Archive – Way Back Machine

Website footprinting

Useful resources

- Bwapp - http://www.itsecgames.com/
- Hack this site - https://www.hackthissite.org/pages/index/index.php

Scanning & Enumeration

- In-depth analysis of interesting targets found on previous phase
- More invasive
- More specific analysis of the most vulnerable targets