Ethical Hacking & Penn Testing

CATALIN BOJA & ALIN ZAMFIROIU

Course

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

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: White/Grey/Black hat

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
- We are not responsible for the illegal use of these techniques and tools

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
  - **Fishing** – try to trick users using legit look like messages or websites to reveal information
  - **SQL Injections**

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 skils

- 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

Anonymity - Tools

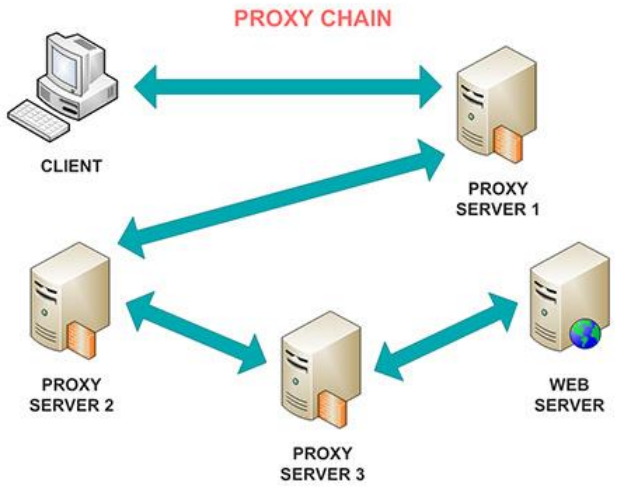
- VPN
- Browser
- File sharing and communication tools
- Recommended reading: https://privacytoolsio.github.io/privacytools.io/

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)

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***

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 - 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 – 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
- **Live CD OS**: Tails, Knoppix, Puppy Linux