



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 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 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

Anonymity - Tools

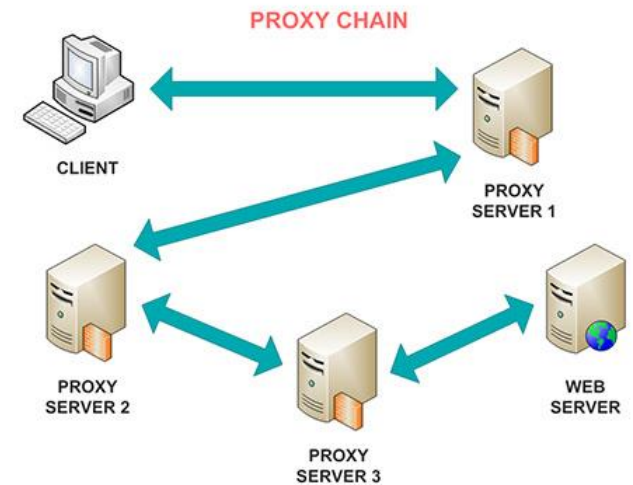
- ▶ VPN
- ▶ Browser
- ▶ File sharing and communication tools
- ▶ Recommended reading: <https://privacytoolsio.github.io/privacytools.io/>

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 for 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://panopticklick.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



Password cracking

ALIN ZAMFIROIU

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 and instruments

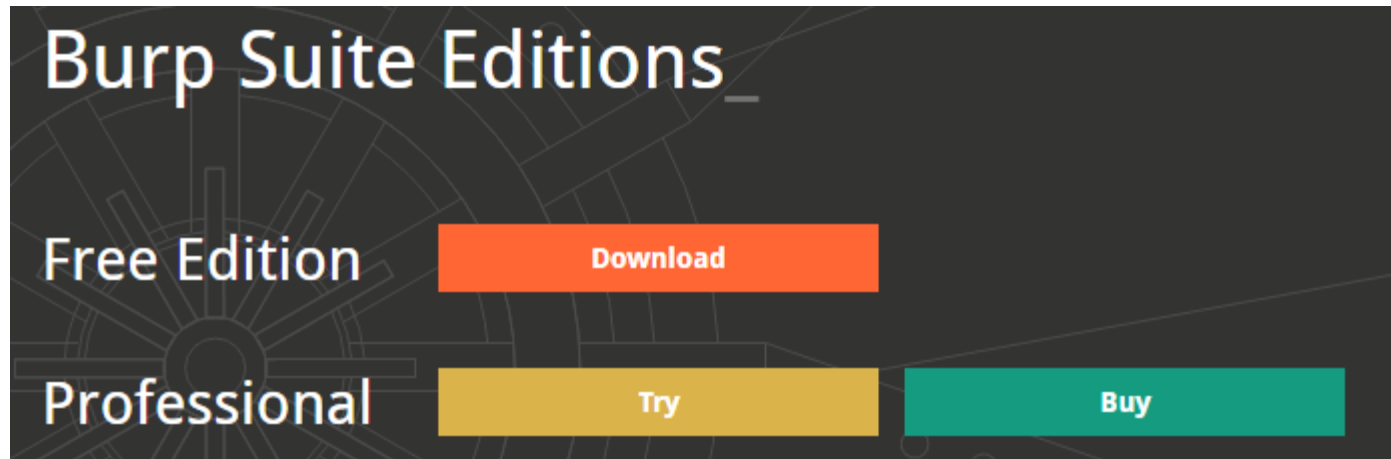
- ▶ The most used software tools to crack user passwords are:
 - ▶ Brutus
 - ▶ Cain and abel
 - ▶ RainbowCrack
 - ▶ John the Ripper
 - ▶ Wfuzz
 - ▶ AirCrack NG
 - ▶ THC Hydra
 - ▶ Medusa
 - ▶ Burp Suite

Real scenarios

- ▶ **Burp Suite + Firefox**

Burp Suite

- ▶ Download the BurpSuite

The image shows a screenshot of the Burp Suite Editions selection screen. It has a dark background with a faint, light-colored spider web pattern. The title "Burp Suite Editions" is at the top left in a white sans-serif font. Below the title, there are two rows of options. The first row is for the "Free Edition", with the text in white and an orange "Download" button to its right. The second row is for the "Professional" edition, with the text in white and two buttons to its right: a yellow "Try" button and a teal "Buy" button.

Burp Suite Editions

Free Edition	Download	
Professional	Try	Buy

Burp Suite

Burp Suite Free Edition v1.7.21 Latest Stable


Released 07 April 2017 | [v1.7.21 Release notes](#)

Download

 **Download for Windows (64-bit)**

[View Checksums](#)



Download

 **Download plain JAR file**

[View Checksums](#)



Download

Other Platforms

 **Download for Linux**


[View Checksums](#)


Download

 **Download for Mac OSX**

[View Checksums](#)


Download

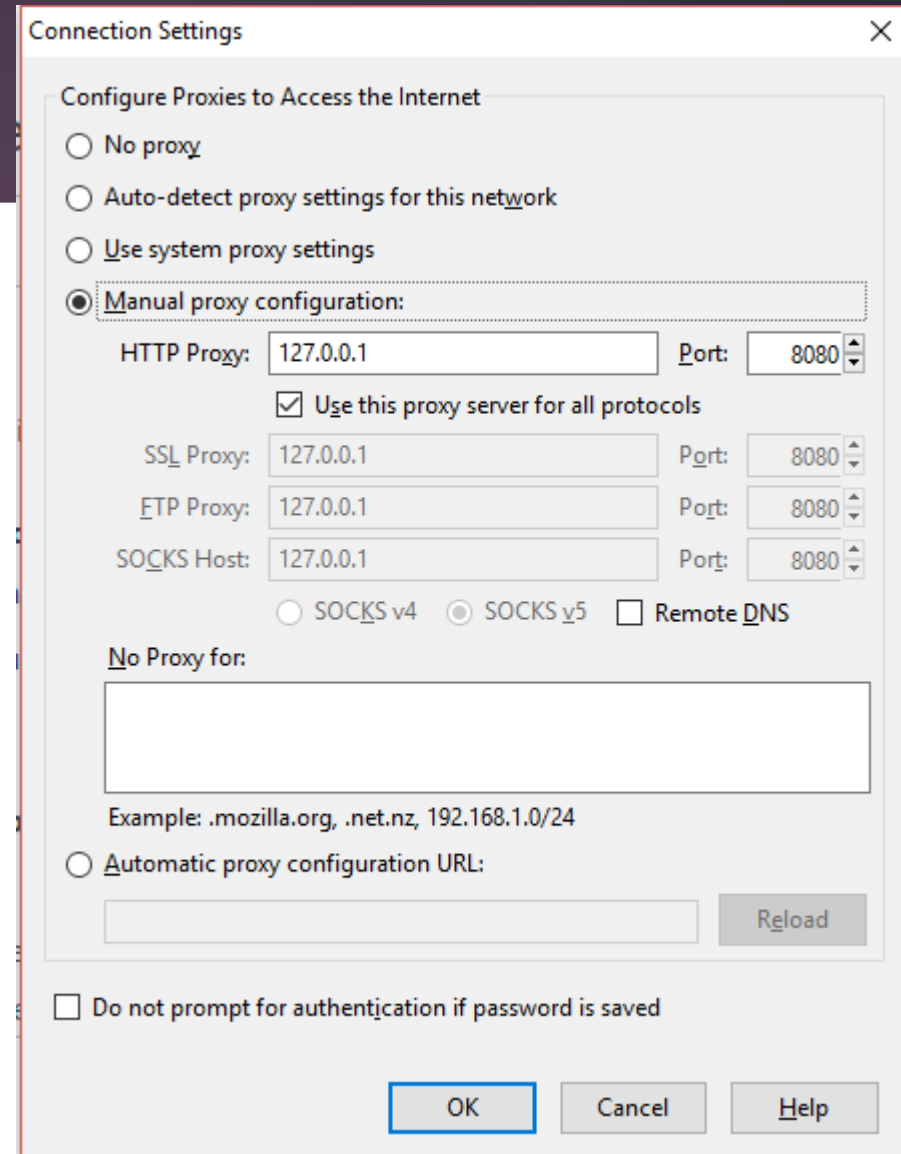
 **Download for Windows (32-bit)**

[View Checksums](#)


Download

Burp Suite

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



The screenshot shows the 'Connection Settings' dialog box in Burp Suite. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to 127.0.0.1 on port 8080. The checkbox 'Use this proxy server for all protocols' is checked. The SSL Proxy, FTP Proxy, and SOCKS Host are also set to 127.0.0.1 on port 8080. The SOCKS version is set to v5. The 'No Proxy for:' field is empty. The 'Automatic proxy configuration URL' is also empty. The 'Do not prompt for authentication if password is saved' checkbox is unchecked. The OK button is highlighted.

Connection Settings

Configure Proxies to Access the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

☒ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

☐ SOCKS v4 ☒ SOCKS v5 ☐ Remote DNS

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL:

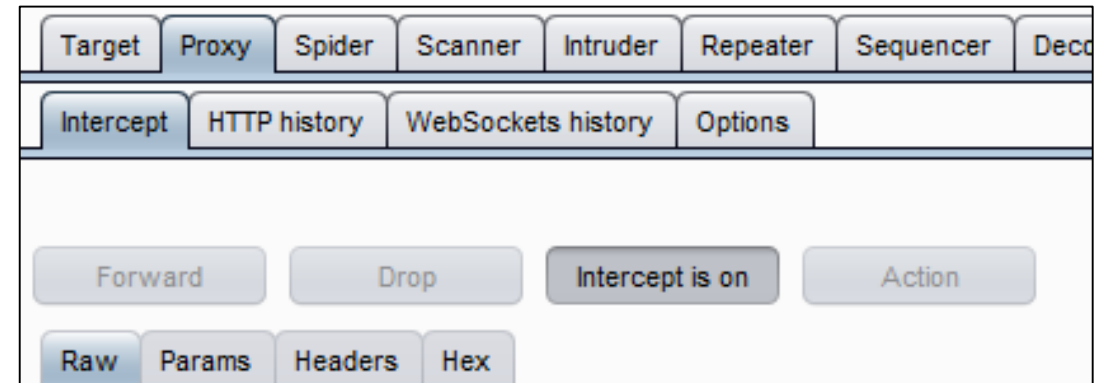
Reload

☐ Do not prompt for authentication if password is saved

OK Cancel Help

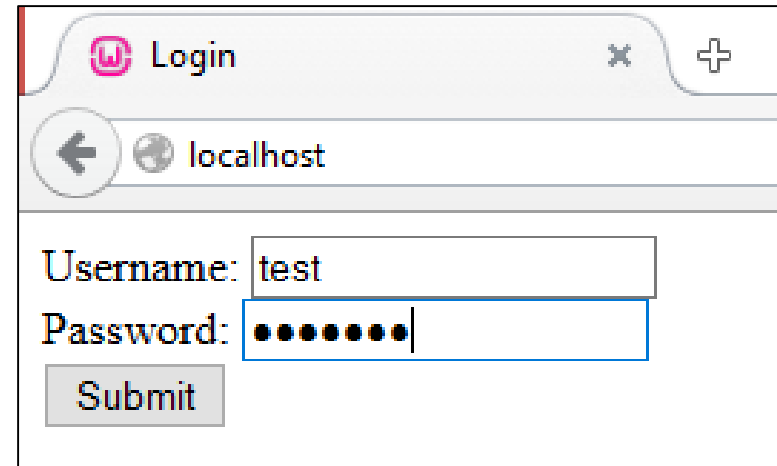
Burp Suite

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



Burp Suite

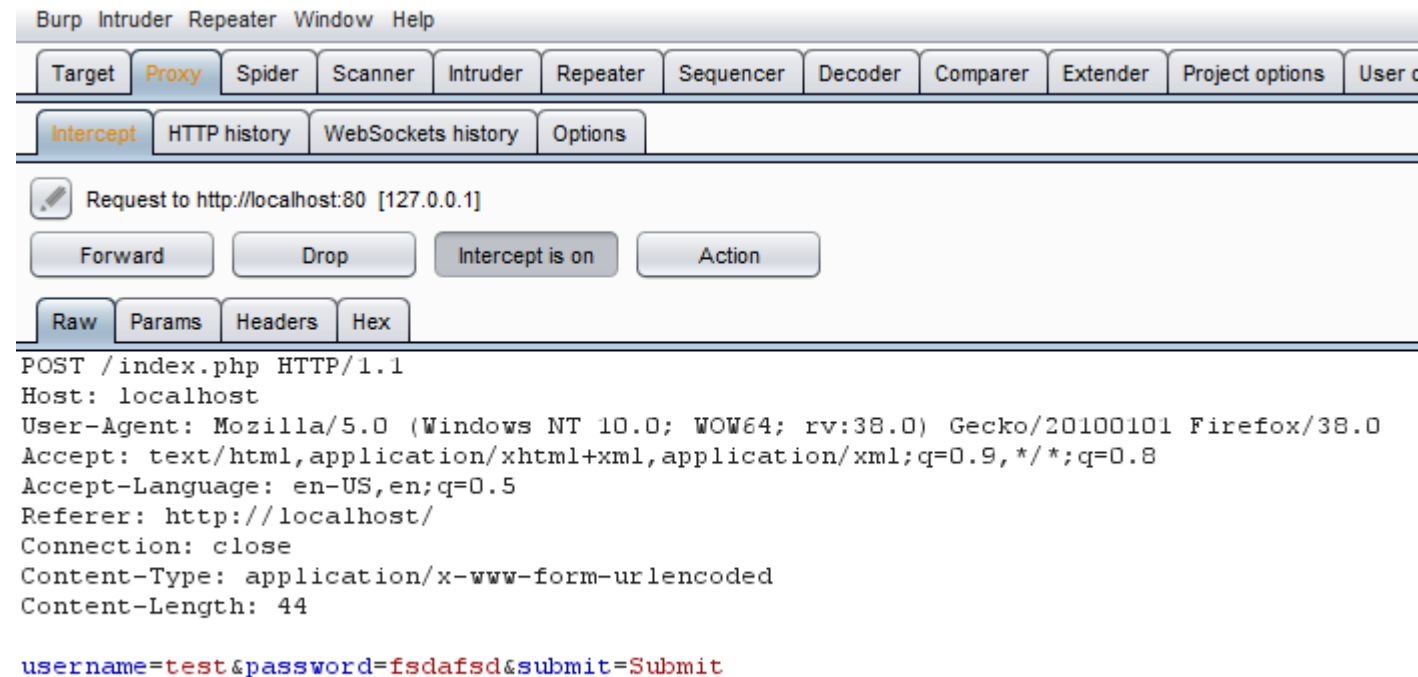
- ▶ Now we have to request the web site with a test user a test password.



A screenshot of a web browser window. The title bar shows a tab labeled "Login" with a pink icon. The address bar shows a back button, a globe icon, and the text "localhost". The main content area contains a login form with two input fields: "Username:" containing the text "test" and "Password:" containing ten black dots. Below the password field is a "Submit" button.

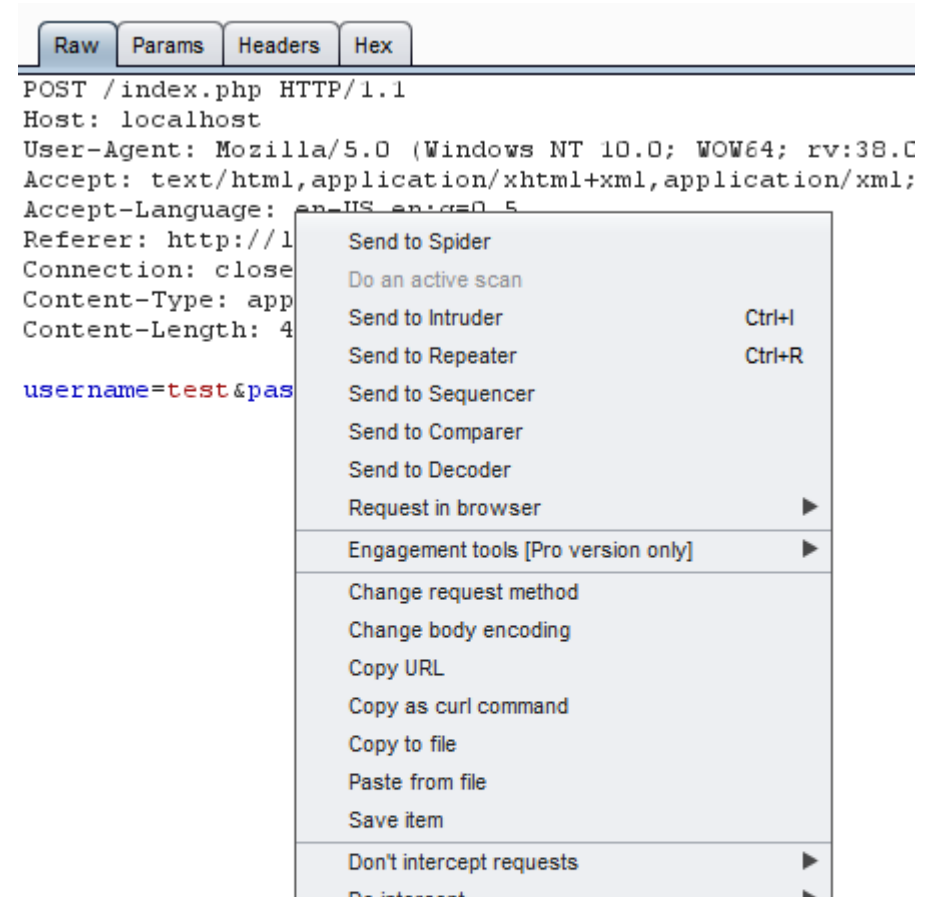
Burp Suite

- ▶ 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 or 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

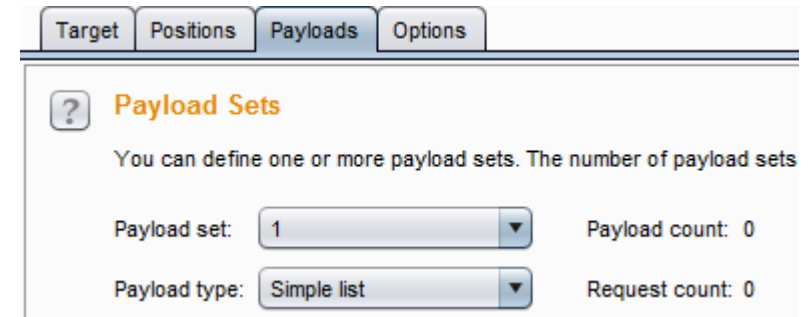
Attack type: Cluster bomb

```
POST /index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=$test&password=$fsdafsd&submit=Submit
```


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
 - ▶ Extension-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

? Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	test
Load ...	admin
Remove	user
Clear	usertest

Add

Add from list ... [Pro version only]

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**.

Results Target Positions Payloads Options							
Filter: Showing all items							
Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	211	
1	test	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
2	admin	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
3	user	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
4	usertest	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
5	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
6	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
7	user	password	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
8	usertest	password	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
9	test	test	200	<input type="checkbox"/>	<input type="checkbox"/>	404	
10	admin	test	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
11	user	test	200	<input type="checkbox"/>	<input type="checkbox"/>	211	
12	usertest	test	200	<input type="checkbox"/>	<input type="checkbox"/>	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

i shall use strong passwords.

i shall use strong passwords.

i shall use strong passwords.

i shall use strong passwords.

! 5ha!! u53 \$4r0ng-p@5sw0rdz!

x	0	x
0	x	x
0	0	x

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

I changed
my password
to "incorrect"
so whenever
I forget what it is,
the computer will say
"your password is
incorrect."

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.
- ▶ <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>

Password cracking





Social Engineering

ALIN ZAMFIROIU

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

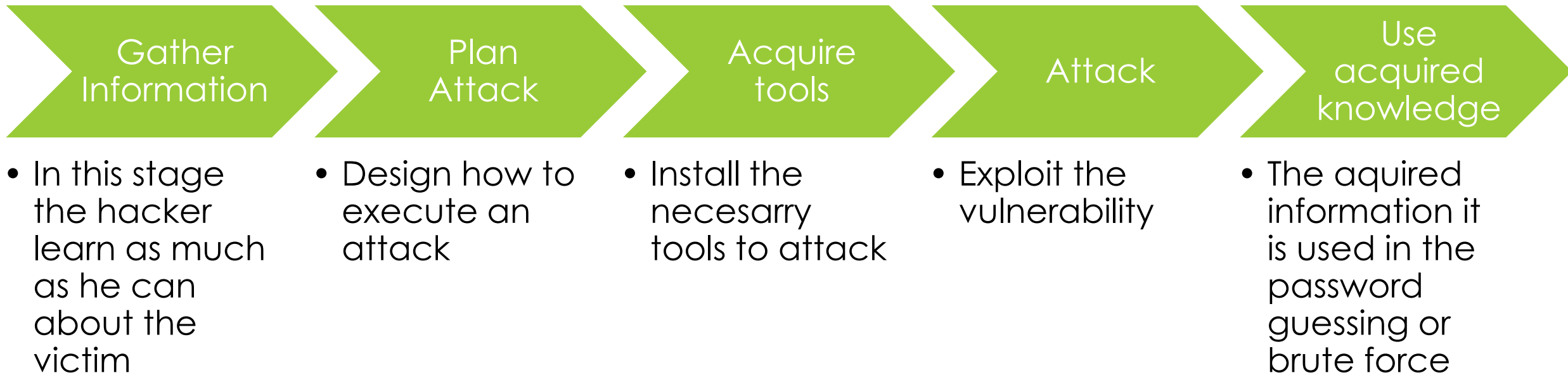
What is Social Engineering

- ▶ 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!

What is Social Engineering

- ▶ *The most used social engineering attacks are made by using the phone (**vishing**).*
- ▶ <https://www.youtube.com/watch?v=lc7scxvKQOo&t=19s>
- ▶ Other examples

The process



Techniques

- ▶ Familiarity exploit
- ▶ Intimidating circumstances
- ▶ Phishing and vishing
- ▶ Tailgating
- ▶ Exploiting human curiosity
- ▶ Exploiting human greed

Techniques

- ▶ **Pretexting** – to be another person
- ▶ **Baiting** – CDs, USB memory, etc.
- ▶ **Quid pro quo** – questionnaire.

Real scenarios

► PayPal Account

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



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 scenarios

- ▶ Email address

● **PayPal** <donotreply@resolution-center.com>

- ▶ The redirect link

www.btw-marketing.de/securelink.la.php



Tools and instruments

- ▶ **Kali SET**
- ▶ **Ghost Phisher**
- ▶ **Maltego**

Countermeasures

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

References

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

Social Engineering





Hacking a WebSite

ALIN ZAMFIROIU

Top Ten OWASP

- ▶ **A1** - Injection
- ▶ **A2** - Cross-Site Scripting (XSS)
- ▶ **A3** - Broken Authentication and Session Management
- ▶ **A4** - Insecure Direct Object References
- ▶ **A5** - Cross-Site Request Forgery (CSRF)
- ▶ **A6** - Security Misconfiguration
- ▶ **A7** - Insecure Cryptographic Storage
- ▶ **A8** - Failure to Restrict URL Access
- ▶ **A9** - Insufficient Transport Layer Protection
- ▶ **A10**- Unvalidated Redirects and Forwards

A1 - Injection

- ▶ 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.

A2 - Cross-Site Scripting (XSS)

- ▶ 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.

A3 - Broken Authentication and Session Management

- ▶ Application 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.

A4 - Insecure Direct Object References

- ▶ A direct reference to an object occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key.
- ▶ Without an access control check or without any other form of protection, attackers can manipulate these references to access unauthorized data.

A5 - Cross-Site Request Forgery (CSRF)

- ▶ A CSRF attack forces a victim's browser to send an HTTP request logged counterfeit, including the victim's session cookie authentication and other information automatically included to a vulnerable web application.
- ▶ This allows the attacker to force the victim's browser to generate requests the vulnerable application it believes are legitimate request from victim.

A6 - Security Misconfiguration

- ▶ 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 secure default configurations. This involves keeping up-to-date for all applications and code libraries used by them.

A7 - Insecure Cryptographic Storage

- ▶ Many web applications do not properly protect sensitive data such as credit cards, ID's, authentication credentials, using encryption or hashing good mechanisms.
- ▶ Attackers may steal or modify such weakly protected data so as to determine identity theft, credit card fraud, or other criminal acts.

A8 - Failure to Restrict URL Access

- ▶ Most web applications check URL access rights before play protected links and buttons.
- ▶ However, applications have to perform the same type of checks each time these pages are accessed, or attackers will be able to forge URLs to access these pages.

A9 - Insufficient Transport Layer Protection

- ▶ Applications frequently fail to authenticate, encrypt or protect the confidentiality and integrity of sensitive network traffic.
- ▶ You could not protect and encrypt traffic using weak algorithms, use expired certificates are valid or not, or do not use them properly.

A10- Unvalidated Redirects and Forwards

- ▶ Web applications frequently redirect the users to other pages mode and sites and using data not reliable to determine the landing page.
- ▶ Without concrete validation, attackers can redirect victims to phishing or malware pages, or use the redirects to access unauthorized pages.

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.

Tools for pentesting

- ▶ Nmap
- ▶ Metasploit penetration testing software
- ▶ John the Ripper
- ▶ THC Hydra
- ▶ OWASP Zed
- ▶ Wireshark
- ▶ Aircraft-ng
- ▶ Cain and Abel
- ▶ Nikto website vulnerability scanner

Hacking a WebSite



Audit IT Master Securitatea Informatică

ASE Bucuresti, 8 aprilie 2017

ing. Florin-Mihai Iliescu, CISA, CISSP
Infologica

Tematică (1)

- **Procesul de audit:** definirea cerințelor de documentare a funcției de audit, a scopului, a rolului și responsabilităților; planificarea angajamentului pentru a adresa obiectivele auditului, pentru respectarea standardelor profesionale, evaluarea aspectelor specifice, documentarea și raportarea cerințelor.
- **Standarde și proceduri:** ITAF - A Professional Practices Framework for IS Audit/ Assurance.
- **Definirea planului de audit:** revizuirea afirmațiilor ce fac obiectul evaluării; selectarea criteriilor pe baza cărora subiectul va fi evaluat, pentru a fi obiective, complete, relevante, măsurabile, general recunoscute și pe înțelesul tuturor celor cărora le este destinat raportul de audit.

Tematică (2)

- **Cerințe de audit specifice instituțiilor financiar-bancare:**
Internet Banking, Sistemul Electronic de Plăți.
- **Colectarea dovezilor și documentarea testelor:**
considerarea lipsei unor controale în planificarea auditului, în determinarea naturii, momentului și complexității procedurilor de audit, obținerea unui număr suficient de dovezi, adecvate pentru a trage concluziile rezonabile.
- **Redactarea raportului de audit:** documentarea și comunicarea oricăror acte ilegale sau încălcări ale reglementărilor; raportarea rezultatelor angajamentului; monitorizarea activităților relevante pentru a concluziona dacă au fost întreprinse acțiuni pentru a adresa constatările și recomandările de audit.

Managementul funcției de audit

Auditul poate fi efectuat de personal din interiorul organizației, sau de personal extern.

- Formalizarea funcției de audit:
 - "Audit Charter": autoritatea, scopul și responsabilitatea funcției de audit trebuie stabilite și aprobate de conducere în cazul auditului intern.
 - "Statement of Work": scopul și obiectivele auditului trebuie agreate prin contract sau într-o declarație de angajament.
- Competența auditorilor de sisteme informatice
 - Cunoștințele și abilitățile necesare
 - Educație profesională continuă
 - Plan de instruire anual
 - Instrumente, metodologii, planuri de lucru

Planificarea Auditului (1)

- Pe termen scurt:
 - Probleme ce trebuie adresate în cursul anului;
- Pe termen lung:
 - Schimbarea strategiei IT;
- Procesele afacerii:
 - Evaluarea calitativă și cantitativă a riscului;
 - Factori de risc, frecvența și impactul scenariilor de risc;
 - Riscul global pentru fiecare proces de afacere;
 - Mediul evaluat, sisteme informatice, tehnologii.

Planificarea Auditului (2)

- ✓ Misiunea și obiectivele afacerii
 - ✓ Cerințele de securitate și procesare
 - ✓ Schimbările survenite în activitate
 - ✓ Revizuirea auditurilor precedente
 - ✓ Structura de organizare
 - ✓ Politici și proceduri
 - ✓ Analiza de risc
 - ✓ Stabilirea scopului și a obiectivelor
 - ✓ Dezvoltarea abordării și strategiei de audit
 - ✓ Desemnarea personalului
- Planul de audit trebuie să permită atingerea obiectivelor și să respecte standardele profesionale.
 - Auditorul IT trebuie să cunoască arhitectura sistemului informatic, tehnologiile folosite, precum și tendințele de dezvoltare viitoare ale organizației.
 - Înțelegerea afacerii / activității auditate.

Codul de etică profesională

- ISACA Code of Professional Ethics
 - Susținerea și încurajarea respectării standardelor, procedurilor și a controalelor.
 - Obiectivitate, responsabilitate și profesionalism, în conformitate cu standardele profesionale și cele mai bune practici.
 - Onorează interesele clientului, cu onestitate și în conformitate cu legea, menținând standarde înalte de conduită și caracter, fără a se angaja în activități care să discrediteze profesia.
 - Păstrează confidențialitatea informațiilor, nu le folosește în interes personal și nu le divulgă către persoane nepotrivite.
 - Își menține competențele și nu se angajează decât în activități pe care le poate îndeplini cu profesionalism.
 - Informează părțile adecvate privind rezultatele și le aduce la cunoștință toate aspectele semnificative.
 - Susține educarea profesională a beneficiarilor pentru a-și îmbunătăți înțelegerea despre securitate și controlul sistemelor informatice.

Standardele de audit

- **Standarde**: definesc cerințele obligatorii pentru auditul sistemelor informatice și pentru raportare;
- **Ghiduri**: îndrumări pentru aplicarea standardelor de audit; implementarea standardelor se face prin prisma judecății profesionale a auditorului;
- **Instrumente și tehnici**: informații despre cum se pot îndeplini cerințele standardului fără să stabilească cerințe obligatorii.

- ITAF (Information Technology Assurance Framework): A Professional Practices Framework for IS Audit/Assurance, 3rd Edition
 - Model de referință comprehensiv care stabilește standardele, definește termenii și conceptele specifice auditării sistemelor informatice, oferă instrumente și tehnici de evaluare a sistemelor informatice.
- Standardele ITAF sunt structurate astfel:
 - General standards (1000 series);
 - Performance standards (1200 series);
 - Reporting standards (1400 series).

Standardele ITAF (1)

- **1001 Audit Charter** - definirea cerințelor de documentare a funcției de audit, a scopului, a rolului și responsabilităților.
- **1002 Organisational Independence** - independența funcției de audit față de zona și activitățile auditate.
- **1003 Professional Independence** - independența și obiectivitate în toate aspectele care au legătură cu auditul.
- **1004 Reasonable Expectation** - finalizarea angajamentului în conformitate cu standardele de audit, folosirea altor standarde sau reglementări aplicabile dacă sunt necesare pentru tragerea concluziilor.

Standardele ITAF (2)

- **1005 Due Professional Care** - respectarea standardelor profesionale de audit aplicabile, în planificarea, efectuarea și raportarea rezultatelor angajamentului.
- **1006 Proficiency** - deținerea competențelor necesare pentru realizarea auditului.
- **1007 Assertions** - revizuirea afirmațiilor ce fac obiectul evaluării pentru a determina dacă pot fi auditate.
- **1008 Criteria** - selectarea criteriilor pe baza cărora subiectul va fi evaluat, pentru a fi obiective, complete, relevante, măsurabile, general recunoscute și pe înțelesul tuturor celor cărora le este destinat raportul de audit.

Standardele ITAF (3)

- **1201 Engagement Planning** - planificarea angajamentului pentru a adresa obiectivele auditului, pentru respectarea standardelor profesionale, evaluarea aspectelor specifice, documentarea și raportarea cerințelor.
- **1202 Risk Assessment in Planning** - prioritatea și alocarea resurselor de audit trebuie să se bazeze pe o analiză a riscurilor.
- **1203 Performance and Supervision** - respectarea planului stabilit pentru evaluarea afirmațiilor auditate, deținerea cunoștințelor tehnice pentru realizarea activităților, documentarea procesului de audit, a dovezilor care susțin constatările și concluziile.
- **1204 Materiality** - considerarea lipsei unor controale în planificarea auditului, în determinarea naturii, momentului și complexității procedurilor de audit.

Standardele ITAF (4)

- **1205 Evidence** - obținerea unui număr suficient de dovezi, adecvate pentru a trage concluziile rezonabile.
- **1206 Using the Work of Other Experts** - condițiile în care se pot folosi rezultatele altor experți în cadrul angajamentului.
- **1207 Irregularity and Illegal Acts** - documentarea și comunicarea oricăror acte ilegale sau încălcări ale reglementărilor.
- **1401 Reporting** - raportarea rezultatelor angajamentului.
- **1402 Follow-up Activities** - monitorizarea activităților relevante pentru a concluziona dacă au fost întreprinse acțiuni pentru a adresa constatările și recomandările de audit.

1001 Audit Charter

- Cerințe:
 - 1001.1 Scopul, responsabilitățile, autoritatea și răspunderea funcției de audit trebuie să fie documentate;
 - 1001.2 Statutul funcției de audit trebuie agreat și aprobat de către nivelul de management corespunzător.
- Aspecte cheie:
 - Autoritatea, scopul, responsabilitățile și limitările funcției de audit;
 - Independența și răspunderea auditorului;
 - Rolurile și responsabilitățile celui auditat pe parcursul angajamentului;
 - Revizuirea, actualizarea și comunicarea formală a statului funcției de audit.
- Ghid:
 - 2001 Audit Charter

1002 Organisational Independence

- Cerințe:
 - 1002.1 Funcția de audit trebuie să fie independentă de zona sau activitatea evaluată pentru a permite îndeplinirea cu obiectivitate a angajamentului.
- Aspecte cheie:
 - Raportarea către un nivel de management care să permită independență și desfășurarea activităților fără interferențe.
 - Consemnarea piedicilor care afectează independența;
 - Evitarea implicării în inițiative IT nelegate de audit, pentru că ar putea afecta independența pe viitor.
- Definiții:
 - Impairment (deteriorare) – Un aspect care diminuează capacitatea de a îndeplini obiectivele de audit. Poate viza: conflict personal de interese, restricționarea accesului la înregistrări, persoane, echipamente, locații, limitarea resurselor (finanțare sau subdimensionare).
- Ghid:
 - 2002 Organisational Independence

1003 Professional Independence

- Cerințe:
 - 1003.1 Independență și obiectivitate, atât în atitudine cât și comportament în toate aspectele legate de misiunile de audit și asigurare.
- Aspecte cheie:
 - Executarea auditului imparțial și fără influențe în formularea concluziilor.
 - Consemnarea piedicilor care afectează independența;
 - Menținerea în permanență a independenței, evaluarea periodică a caracterului independent.
 - Evitarea implicării în inițiative IT nelegate de audit, pentru că ar putea afecta independența pe viitor.
- Definiții:
 - Independence în appearance (atitudine independentă) – evitarea acțiunilor sau circumstanțelor care ar putea pune la îndoială integritatea, obiectivitatea și profesionalismul exercitate în efectuarea auditului.
 - Independence of mind (lipsa prejudecăților) – menținerea unei atitudini care să permită exprimarea unei concluzii fără a fi afectată judecată profesională și menținerea integrității, obiectivității și scepticismului.
- Ghid:
 - 2003 Professional Independence

2003 Professional Independence

- Amenințări:
 - **Self-interest** (Interes propriu) – existența unui interes financiar sau de altă natură ce poate influența judecata sau comportamentul profesional
 - **Self-review** (Auto-revizuirea) – evaluarea inadecvată a propriilor rezultate sau a judecății profesionale al altui membru din funcția de audit.
 - **Advocacy** (Avocatură) – promovarea funcției de audit pentru a influența obiectivitatea.
 - **Familiarity** (Familiaritate) – relația lungă / apropiată cu auditatul, înțelegător cu interesele sale, sau acceptarea superficială a rezultatelor auditului.
 - **Intimidation** (Intimidare) – descurajarea unui comportament integru și obiectiv
 - **Bias** (Prejudecată) – poziție subiectivă ca urmare a unor convingeri politice, ideologice, sociale, sau de altă natură
 - **Management participation** (Implicarea managementului) – efectuarea auditului de persoane care au rol sau funcții de management în organizația auditată.

1004 Reasonable Expectation

- Cerințe:
 - 1004.1 Așteptările auditorilor trebuie să fie rezonabile în ceea ce privește îndeplinirea angajamentului în conformitate cu standardele de audit, iar acolo unde este necesar alte standarde profesionale sau tehnice, sau reglementări aplicabile pot fi necesare pentru exprimare opiniei.
 - 1004.2 Așteptări rezonabile în ceea ce privește scopul angajamentului în vederea formulării unei concluzii asupra subiectului auditat și tratarea oricăror restricții.
 - 1004.3 Așteptări rezonabile cu privire la înțelegerea de către management a obligațiilor și responsabilităților sale ce privesc furnizarea informațiilor relevante și în timp util necesare pentru angajament.
- Aspecte cheie:
 - Acceptarea angajamentului doar dacă poate fi onorat cu succes respectând standardele profesionale.
 - Efectuarea auditului doar dacă evaluarea se poate face în raport cu criterii relevante.
 - Revizuirea scopului pentru a determina dacă este clar documentat și permite exprimarea unei concluzii asupra subiectului evaluat.
 - Identificarea piedicilor care pot afecta efectuarea angajamentului, inclusiv accesul la informații relevante în timp util.
- Definiții:
 - Opinia auditorului – o declarație formală care descrie scopul auditului, procedurile folosite în realizarea raportului, îndeplinirea sau nu a criteriilor de audit.
- Ghid:
 - 2004 Reasonable Expectation

1005 Due Professional Care

- Cerințe:
 - 1005.1 Auditorii de sisteme informatice trebuie să exercite profesionalism, incluzând și respectarea standardelor profesionale de audit, în planificarea, efectuarea și raportarea rezultatelor angajamentului.
- Aspecte cheie:
 - Demonstrarea competențelor și a unui nivel suficient de înțelegere care să permită atingerea obiectivelor de audit.
 - Menținerea unui scepticism profesional.
 - Menținerea competențelor profesionale, fiind la curent și respectând standardele.
 - Comunicarea rolurilor și responsabilităților în cadrul echipei de audit.
 - Tratarea tuturor rezervelor ce privesc respectarea standardelor în cadrul angajamentului.
 - Protejarea informațiilor obținute în timpul auditului.
 - Obținerea unui nivel rezonabil de asigurări, nivelul de teste variind în funcție de tipul angajamentului.
- Definiții:
 - Scepticism profesional – atitudine interogativă și evaluarea critică a probelor de audit.
- Ghid:
 - 2005 Due Professional Care

1006 Proficiency

- Cerințe:
 - 1006.1 Deținerea competențelor adecvate.
 - 1006.2 Cunoștințe adecvate asupra subiectului evaluat.
 - 1006.3 Menținerea competențelor profesionale prin educare profesională continuă și instruire.
- Aspecte cheie:
 - Demonstrarea unui nivel suficient de competențe înainte de începerea angajamentului.
 - Evaluarea mijloacelor alternative de a dispune de competențele necesare, incluzând subcontractarea, externalizarea, amânarea angajamentului.
- Definiții:
 - Competence (competență) – abilitatea de a efectua o activitate cu succes.
 - Proficiency (experiență) – deținerea experienței și calificării.
- Ghid:
 - 2006 Proficiency

1007 Assertions

- Cerințe:
 - 1007.1 Auditorii SI trebuie să revizuiască afirmațiile în raport cu care subiectul va fi evaluat pentru a determina dacă acestea pot fi auditate și sunt suficiente, valide și relevante.
- Aspecte cheie:
 - Evaluarea criteriilor de evaluare pentru a asigura susținerea afirmațiilor.
 - Determinarea faptului că afirmațiile pot fi auditate și susținute prin informații valide.
 - Validarea afirmațiilor în raport cu standarde sau declarații oficiale pentru a asigura că răspund așteptărilor beneficiarilor.
 - Formularea unei concluzii pentru fiecare din afirmații pe baza constatărilor fiecărui criteriu și a judecății profesionale.
- Definiții:
 - Assertion (afirmație, aserțiune) – orice declarație formală despre subiect făcută de management.

1008 Criteria

- Cerințe:
 - 1008.1 Selectarea criteriilor în raport cu care este evaluat subiectul, de o manieră completă, obiectivă, relevantă, măsurabilă, inteligibile, universal acceptate, oficiale, accesibile tuturor destinatarilor raportului.
 - 1008.2 Auditorii trebuie să țină cont de originea criteriilor și să se concentreze pe indicatorii publicați de entități oficiale relevante înainte de a lua în calcul criterii mai puțin cunoscute.
- Aspecte cheie:
 - Alegere atentă a criteriilor de evaluare și capacitatea de a justifica selecția făcută.
 - Folosirea judecății profesionale pentru a se asigura că aplicarea criteriilor permite exprimarea unei opinii corecte.
 - Oferirea oricăror informații suplimentare necesare formulării unui raport corect, obiectiv și inteligibil.
- Definiții:
 - Criteria (criterii) – standarde, referințe folosite pentru a măsura și prezenta subiectul și în raport cu care auditorul SI realizează evaluare.
- Ghid:
 - 2008 Criteria

1201 Engagement Planning

- Cerințe:
 - 1201.1 Planificarea fiecărui audit de sisteme informatice pentru a adresa:
 - Obiectivele, scopul, durata și cerințele;
 - Respectarea legilor în vigoare și a standardelor profesionale de audit;
 - Utilizarea unei abordări bazate pe analiza riscurilor;
 - Evaluarea aspectelor specifice;
 - Cerințele de documentare și raportare.
 - 1002.2 Documentarea unui plan de proiect care descrie:
 - felul angajamentului, obiectivele, durata și resursele necesare
 - durata și extindere procedurilor de audit pentru a finaliza angajamentul.

1202 Risk Assessment in Planning

- Cerințe:
 - 1202.1 Funcția de audit și asigurare a sistemelor informatice trebuie să utilizeze o metodologie și abordare corespunzătoare bazată pe evaluarea riscurilor pentru dezvoltarea planului de audit al sistemului informatic care să stabilească prioritățile pentru alocarea eficace a resurselor de audit al sistemelor informatice.
 - 1202.2 Experții în audit și în evaluarea a sistemelor informatice trebuie să identifice și să evalueze riscurile relevante atunci când sunt planificate angajamentele individuale.

1203 Performance and Supervision

- Cerințe:
 - 1203.1 Auditorii SI își desfășoară activitatea în conformitate cu planul de audit al sistemelor informatice aprobat ce trebuie să acopere riscul identificat și respectarea termenelor agreate.
 - 1203.2 Auditorii SI asigură supravegherea personalului de audit pentru care au responsabilitatea de supraveghere, pentru a realiza obiectivele de audit și a respecta standardele profesionale de audit aplicabile.
 - 1203.3 Auditorii SI acceptă doar atribuțiile pentru care au cunoștințe și abilitați, sau pentru care sunt așteptări rezonabile fie pentru dobândirea competențelor în timpul angajamentului sau realizarea obiectivelor sub supraveghere.
 - 1203.4 Auditorii SI trebuie să obțină dovezi suficiente și adecvate pentru îndeplinirea obiectivelor de audit. Constatările de audit și concluziile sunt susținute de analiza și interpretarea corespunzătoare a dovezilor.
 - 1204.5 Auditorii SI trebuie să documenteze procesul de audit, descriind activitatea și dovezile de audit și care susțin constatările și concluziile.
 - 1203.6 Auditorii SI trebuie să identifice și să tragă concluzii asupra aspectelor constatate.

1204 Materiality

- Cerințe:
 - 1204.1 Auditorii SI trebuie să țină cont de eventualele puncte slabe sau absența controalelor în timpul planificării unui angajament și că lipsa lor ar putea duce la o deficiență materială.
 - 1204.2 Auditorii SI trebuie să ia în considerare materialitatea precum și relația sa cu riscul de audit în timp ce se determină natura, termenele și acoperirea procedurilor de audit.
 - 1204.3 Auditorii SI trebuie să ia în considerare efectul cumulativ al deficiențelor minore de control sau a punctelor slabe și dacă absența controalelor se traduce printr-o deficiență semnificativă sau o slăbiciune materială.
 - 1204.4 Auditorii SI trebuie să prezinte în raport următoarele:
 - Absența sau ineficacitatea controalelor;
 - Importanța deficiențelor controalelor;
 - Probabilitatea ca aceste puncte slabe să rezulte într-o deficiență semnificativă sau slăbiciune materială.

1205 Evidence

- Cerințe:
 - 1205.1 Auditorii SI trebuie să obțină suficiente dovezi corespunzătoare pentru a putea trage concluzii rezonabile pe care să se bazeze rezultatele angajamentului.
 - 1205.2 Auditorii SI vor evalua dacă dovezilor obținute sunt suficiente pentru susținerea concluziilor și îndeplinirea obiectivelor angajamentului.

1206 Using the Work of Other Experts

- Cerințe:
 - 1206.1 Auditorii SI trebuie să ia în considerare utilizarea activității altor experți, atunci când este cazul.
 - 1206.2 Auditorii SI evaluează și aprobă caracterul adecvat al calificărilor profesionale ale celorlalți experți, competențele, experiența relevantă, resursele, independența și calitatea proceselor de control, înainte de angajament.
 - 1206.3 Auditorii SI revizuiesc și evaluează activitatea altor experți ca parte a angajamentului, și documentează concluzia privind gradul de utilizare a muncii acestora.
 - 1206.4 Auditorii SI stabilesc dacă activitatea altor experți, care nu fac parte din echipa de audit este corespunzătoare și completă pentru a concluziona cu privire la obiectivele de angajament actuale, și documentează clar concluzia.
 - 1206.5 Auditorii SI trebuie să stabilească dacă activitatea celorlalți experți va fi considerată și asimilată direct sau menționată separat în raport.
 - 1206.6 Auditorii SI aplică proceduri adiționale de testare pentru a obține suficiente dovezi suplimentare în condițiile în care activitatea altor experți nu furnizează dovezi suficiente și adecvate.
 - 1206.7 Auditorii SI furnizează o concluzie sau o opinie de audit adecvată, și include orice limitare a scopului în cazul în care dovezile solicitate nu sunt obținute prin proceduri de testare suplimentare.

1207 Irregularity and Illegal Acts

- Cerințe:
 - 1207.1 Auditorii SI trebuie să ia în considerare riscul de nereguli și încălcări a prevederilor legale în timpul angajamentului.
 - 1207.2 Auditorii SI trebuie să mențină o atitudine sceptică profesională în timpul angajamentului.
 - 1207.3 Auditorii SI trebuie să documenteze și să comunice orice nereguli materiale sau orice act ilegal autorității corespunzătoare în timp util.

- Cerințe:
 - 1401.1 Auditorii SI furnizează un raport pentru a comunica rezultatele la încheierea angajamentului conținând:
 - Identificarea organizației, destinatarii vizați și orice restricție cu privire la conținut și a distribuției;
 - Domeniul de aplicare, obiectivele de angajament, perioada vizată precum și felul, calendarul și amploarea lucrărilor efectuate;
 - Constatările, concluziile și recomandările;
 - Orice calificări sau limitări a scopului pe care auditorul SI o are în ceea ce privește angajamentul;
 - Semnătura, data și distribuirea în conformitate cu condițiile statutului sau a scrisorii de angajament.
 - 1401.2 Auditorii SI trebuie să asigure suficiente dovezi care să susțină constatările din raportul de audit.

1402 Follow-up Activities

- Cerințe:
 - 1402.1 Auditorii SI monitorizează informațiile relevante pentru a concluziona dacă conducerea a planificat/a luat în considerare măsuri în timp util pentru a adresa constatările auditului raportate și recomandările.

- Analiza de risc este parte a planificării auditului și ajută la identificarea riscurilor și vulnerabilităților astfel încât auditorul SI să determine măsurile necesare reducerii acestor riscuri:
 - **Riscurile generale ale afacerii** – Înțelegerea naturii și scopului afacerii, a mediului în care operează.
 - **Riscurile legate de utilizarea tehnologiei** – Dependența proceselor de tehnologie pentru a produce rezultate, impactul IT-ului asupra obiectivelor afacerii.
 - **Măsuri relevante de control.**
- Evaluarea eficacității procesului de management al riscului utilizat de organizație

- Măsuri de reducere a riscurilor: politici, proceduri, practici, mod de organizare. Este responsabilitatea managementului să stabilească o cultură care să faciliteze un sistem de control intern eficient și eficace și pentru monitorizarea continuă a eficacității acestui sistem de control intern din care face parte fiecare persoană din organizație.
- Clasificarea controalelor:
 - Preventive
 - Detective
 - Corrective
- COBIT 5

Controale Generale

- Sunt stabilite de management pentru întreaga organizație pentru a atinge obiective specifice.
- Controale generale pot fi:
 - controale financiare care să vizeze operațiunile contabile;
 - controale operaționale care privesc activitatea zilnică;
 - controale administrative care susțin controalele operaționale în respectarea politicilor stabilite de management;
 - politica de organizare a securității și proceduri de utilizare adecvată a resurselor;
 - politici de înregistrare a operațiunilor, păstrare a înregistrărilor;
 - accesul în locație, în centrele de date, la resursele IT.

COBIT 5 - Domenii

- Guvernanță:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - EDM02 Ensure Benefits Delivery
 - EDM03 Ensure Risk Optimisation
 - EDM04 Ensure Resource Optimisation
 - EDM05 Ensure Stakeholder Transparency
- Management:
 - Align, Plan and Organise (APO)
 - Build, Acquire and Implement (BAI)
 - Deliver, Service and Support (DSS)
 - Monitor, Evaluate and Assess (MEA)

COBIT 5 - Align, Plan and Organise

- Guvernanță:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - EDM02 Ensure Benefits Delivery
 - EDM03 Ensure Risk Optimisation
 - EDM04 Ensure Resource Optimisation
 - EDM05 Ensure Stakeholder Transparency
- Management:
 - Align, Plan and Organise (APO)
 - Build, Acquire and Implement (BAI)
 - Deliver, Service and Support (DSS)
 - Monitor, Evaluate and Assess (MEA)

COBIT 5 - Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

COBIT 5 - Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

COBIT 5 - Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

COBIT 5 - Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Capability Maturity Model (CMM)

- Level 1 - Initial (Chaotic)
 - undocumented and in a state of dynamic change, driven in an ad hoc, uncontrolled and reactive manner.
- Level 2 - Repeatable
 - repeatable, possibly with consistent results, unlikely to be rigorous
- Level 3 - Defined
 - defined and documented, subject to some degree of improvement over time.
- Level 4 - Managed
 - metrics, management can effectively control, can identify ways to adjust and adapt
- Level 5 - Optimizing
 - focus is on continually improving process performance.

Abordarea auditului bazată pe risc

- Natura și profunzimea testelor efectuate are la bază analiza prealabilă a riscurilor:
 - Teste de conformitate;
 - Teste de detaliu.
- Riscul de audit este influențat de:
 - Riscul Inerent
 - Riscul de Control
 - Riscul de Detecție

Abordarea auditului bazată pe risc (1)

- Strângerea informațiilor preliminare și planificare
 - Cunoștințe despre afacere și industrie;
 - Rezultatele auditurilor precedente;
 - Informații financiare recente;
 - Reglementări, cerințe legislative;
 - Evaluare riscurilor inerente.



-
- Control
- Policies
- Goals
- Reliability
- Function
- Selection
- Activities
- Integrated
- Procedures
- Effectiveness
- Programmed
- Implementation
- Administration
- Improvement
- Organization
- Maintenance
- Amendment
- Revised
- Compliance
- System
- Testing
- Regular
- Output
- Related
- Comply
- Results
- Checks
- Design
- Duties
- Objectives
- Computerized
- Ess
- Des
- R
- C
- M

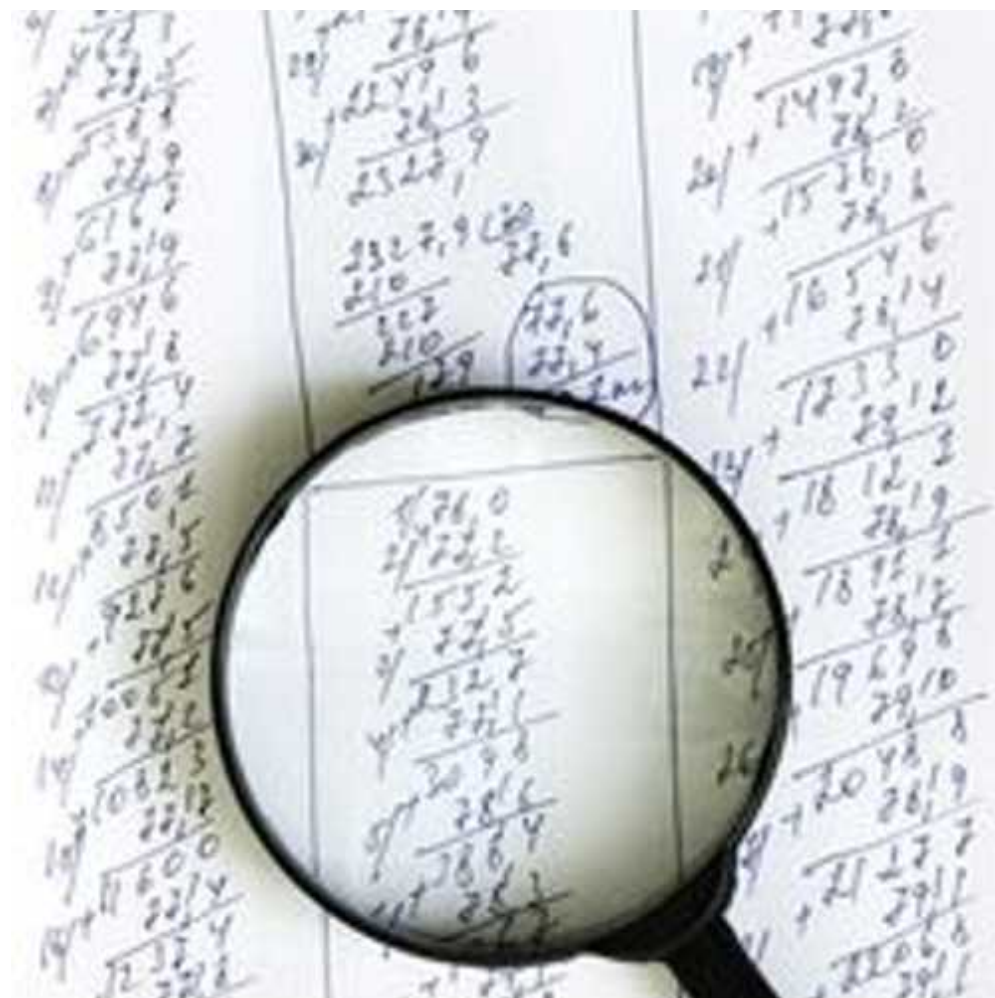
Abordarea auditului bazată pe risc (3)

- Efectuarea testelor de conformitate
 - Identificarea controalelor cheie ce vor fi testate;
 - Testarea eficacității controalelor, prevenirea riscului, aderarea la politicile și procedurile organizației.



Abordarea auditului bazată pe risc (4)

- Efectuarea testelor de detaliu (substantive):
 - Proceduri analitice;
 - Alegerea populației;
 - Dimensionare eșantion analizat;
 - Rata așteptată de eroare;
 - Rata detectată de eroare.



Abordarea auditului bazată pe risc (5)

- Finalizarea auditului:
 - Sumar al constatărilor, perioada evaluată, criteriile folosite pentru evaluare;
 - Formularea recomandărilor;
 - Documentarea raportului de audit;
 - Plan de remediere agreeat de conducere.



- Eșantionare statistică:
 - Metodă obiectivă pentru determinarea dimensiunii eșantionului și a criteriilor de selecție;
- Eșantionare nestatistică:
 - Numărul de articole analizate, dimensiunea eșantionului sunt alese de auditor în baza judecății profesionale.

Tehnici de audit asistate de calculator

- CAAT (Computer-Assised Audit Techniques)
 - Colectarea informațiilor disponibile în format electronic;
 - Oferă posibilitatea auditorului de a colecta singur informațiile necesare;
- Generalized Audit Software (GAS)
 - Software capabil să citească date direct din diverse tipuri de baze de date sau fișiere text;
 - Oferă facilități de calcul, analiză statistică, verificare secvențe / duplicate.
- Tehnici de audit online continuu.

Materialitatea constatărilor

- Mică:
 - problema nu are un impact asupra obiectivelor de audit, dar cumulată cu alți factori de risc poate avea urmări negative.
- Medie:
 - problema nu are impact direct, dar nerezolvarea ei în timp poate duce la apariția unor incidente ce pot afecta obiectivele de audit.
- Mare:
 - problema are impact direct, și trebuie rezolvată pentru a îndeplini obiectivele de audit.

Comunicarea rezultatelor auditului



- Faptele prezentate în raport sunt corecte;
- Recomandările sunt realiste, fezabile;
- Negocierea, găsirea unor alternative pentru remedierea problemelor;
- Termene pentru remedierea problemelor;
- Limitarea rolului de auditor de cel al consultantului în acordarea de asistență în rezolvarea problemelor.

Documentația de audit



- Planificarea și pregătirea scopului și a obiectivelor de audit;
- Descrierea domeniului auditat;
- Programul de audit (plan de teste);
- Pașii efectuați și dovezile colectate;
- Utilizarea serviciilor altor auditori și experți;
- Constatări, concluzii și recomandări;
- Relația între documentația de audit, dovezi și datarea acestora.

Certificarea Auditorilor SI

- Certified Information Systems Auditor (CISA)
 - Task Statements
 - Knowledge Statements
- <http://www.isaca.org/Certification>
- Domain 1—The Process of Auditing Information Systems (21%)
- Domain 2—Governance and Management of IT (16%)
- Domain 3—Information Systems Acquisition, Development and Implementation (18%)
- Domain 4—Information Systems Operations, Maintenance and Service Management (20%)
- Domain 5—Protection of Information Assets (25%)



Auditarea Sistemelor de Internet Banking

- ORDIN MCTI (actual MCSI) nr. 389 din 27 iunie 2007
 - a) confidențialitatea și integritatea comunicațiilor;
 - b) confidențialitatea și nonrepudierea tranzacțiilor;
 - c) confidențialitatea și integritatea datelor;
 - d) autenticitatea părților care participă la tranzacții;
 - e) protecția datelor cu caracter personal;
 - f) păstrarea secretului bancar;
 - g) trasabilitatea tranzacțiilor;
 - h) continuitatea serviciilor oferite clienților;
 - i) împiedicarea, detectarea și monitorizarea accesului neautorizat în sistem;
 - j) restaurarea informațiilor gestionate de sistem în cazul unor calamități naturale și evenimente imprevizibile;
 - k) gestionarea și administrarea sistemului informatic;
 - l) orice alte activități sau măsuri tehnice întreprinse pentru exploatarea în siguranță a sistemului.

Riscuri asociate Internet Banking (1)

- a) confidențialitatea și integritatea comunicațiilor
 - Interceptarea comunicației și compromiterea informațiilor tranzacționate.
 - Interceptarea comunicației și modificarea parametrilor tranzacției.

Riscuri asociate Internet Banking (2)

- b) confidențialitatea și nonrepudierea tranzacțiilor
 - Interceptarea tranzacției și modificarea parametrilor tranzacției.
 - Nerecunoașterea tranzacției de către client.
 - Accesul unor persoane neautorizate la tranzacțiile efectuate de clienți.

Riscuri asociate Internet Banking (3)

- c) confidențialitatea și integritatea datelor
 - Accesul neautorizat la datele stocate în aplicație, baza de date, fișiere.
 - Modificarea neautorizată a datelor.

Riscuri asociate Internet Banking (4)

- d) autenticitatea părților care participă la tranzacții
 - Clonarea serverului de aplicație și efectuarea unor atacuri de Phishing.
 - Atribuirea accesului unei persoane neautorizate în vederea comiterii unor fraude.

Riscuri asociate Internet Banking (5)

- e) protecția datelor cu caracter personal
 - Nerespectarea prevederilor legale cu privire la protecția datelor cu caracter personal.

Riscuri asociate Internet Banking (6)

- f) păstrarea secretului bancar
 - Accesul administratorilor la datele operaționale, încălcând obligația de asigurare a secretului bancar.

Riscuri asociate Internet Banking (7)

- g) trasabilitatea tranzacțiilor
 - Imposibilitatea identificării autorului unei tranzacții;
 - Lipsa detaliilor privind efectuarea unei tranzacții;
 - Modificarea înregistrărilor cu detaliile unei tranzacții.

Riscuri asociate Internet Banking (8)

- h) continuitatea serviciilor oferite clienților
 - Întreruperea serviciului oferit clienților ca urmare a unor erori de aplicație.
 - Întreruperea serviciului oferit clienților ca urmare a unor defecțiuni hardware.
 - Întreruperea serviciului oferit clienților ca urmare a unor incidente neprevăzute majore (dezastre naturale, atacuri informatice, sabotaj, etc.)
 - Întreruperea serviciului ca urmare a modificării componentelor HW sau SW, fără o testare și autorizare corespunzătoare.
 - Întreruperea serviciului, sau funcționarea greoaie ca urmare a supraîncărcării serverelor sau a neoptimizării bazei de date sau aplicației.

Riscuri asociate Internet Banking (9)

- i) împiedicarea, detectarea și monitorizarea accesului
 - Posibilitatea ocolirii mecanismului de autorizare a accesului la date.
 - Lipsa unor mecanisme de a detecta acțiunile neautorizate și de a limita efectele acestora.
 - Lipsa unui proces de analiză a accesului în vederea identificării la timp a tentativelor de acces / a accesului neautorizat.

Riscuri asociate Internet Banking (10)

- j) restaurarea informațiilor gestionate de sistem
 - Pierderea datelor ca urmare a salvării defectuoase sau a compromiterii mediului de stocare a acestora.
 - Incapacitatea de a restaura datele salvate ca urmare a necunoașterii procedurii de restaurare sau a lipsei mijloacelor tehnice.

Riscuri asociate Internet Banking (11)

- k) gestionarea și administrarea sistemului informatic
 - Administrarea defectuoasă datorată nestabilirii clare a responsabilităților.
 - Administrarea eronată ca urmare a necunoașterii procedurilor de gestiune a sistemului informatic.
 - Nerespectarea prevederilor cu privire la documentarea planului de securitate.

- Studiu de caz al ABN-AMRO și Dutch Cybercrime Police Agency (Poliție)
- Infractorii au obținut 750% ROI.
- Au cumpărat și îmbunătățit un toolkit gratuit bazat pe Zeus, au angajat o rețea botnet pentru a trimite spam, au închiriat un centru de comandă, și apoi au folosit calculatoare PC din botnet pentru a stabili sesiuni către Internet banking.
- Au angajat traducători calificați pentru a traduce paginile de eroare ale băncii, au angajat cărauși pentru transferul banilor în Ucraina și Rusia.
- În cele 23 de tranzacții frauduloase au obținut un ROI de 750%, (cheltuielula angajată fiind 13.550 €, iar fraudă totală ajungând la 116.000 €)

Vectori de atac

- Acces neautorizat:
utilizator / parolă
- Sniffing
- Acțiuni neautorizate:
 - Malware
 - Vulnerabilitate →
Exploit
- Social Engineering
(Kits)



- Referințe

- CISA Review Manual
- ITAFTM: A Professional Practices Framework for IS Audit/ Assurance, 3 rd Edition
- Ordinul MCTI nr. 389 / 2007

- Contact

- Florin-Mihai Iliescu
- office@infologica.ro
- 0723233317 / 021-4114548
- www.infologica.ro