

# Bezpečnost sít'ových aplikací

2019/2020

Př 10



# Penetrační testování, forenzní analýza

- Penetrační testování
  - Důvody a principy
  - Typy testování
  - Analýza / vyhodnocení výsledků
- Forenzní analýza
- Honeypot
  - Principy
  - Využití



# Důvody penetračních testů

- Cíl je být připraven == vědět dříve !!!
  - Chyba vzniká při změnách
    - Nastavení / Instalace – aktualizace SW
    - Provozu a hot-fixech
- Může provádět kdokoliv ?
  - Ano, ALE
    - Autor vždy vidí méně / jiné věci
    - Autor ví kam kliknout
    - Externista / kolega → lepší výsledek



# Typy penetračních testů

- Vnější
  - Nemám přístup do vnitřních systémů
- Vnitřní
  - S plným přístupem do vnitřních systémů
- Bezdrátové
  - Extra případ – vnitřních testů
  - Dnes stále aktuálnější



# Plánování penetračních testů

- Ohlášené / částečně ohlášené
  - Možnost přípravy
  - Možnost spolupráce s auditorem
  - Nemělo by se zasahovat
- Skryté / neohlášené
  - Nikdo není záměrně informován
  - Lepší výsledky o aktuálním stavu
  - Riziko/test zásahu admina/robota



# Strojové penetrační testy

- Strojové
  - Jednodušší a běžnější
  - Funguje na základě definovaných postupů
    - Můžeme se lépe připravit
    - Stroj nevychává ...
  - Dostupné nástroje
    - Nessus, W3af, sqlmap, rkhunter, OpenVas
    - Různá rozhraní
      - Konzole, WWW, GUI



# Strojové penetrační testování OpenVAS

Greenbone Security Assistant

Logged in as User **openvas** | Logout  
Tue Apr 22 07:43:09 2014 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration

Help

### Report Summary

Result of Task: **Immediate scan of IP 192.168.0.104** Task  
Order of results: by host  
Scan started: **Tue Apr 22 07:16:28 2014**  
Scan ended: Tue Apr 22 07:27:28 2014  
Scan status: Done

	High	Medium	Low	Log	False Pos	Total	Run Alert	Download
Full report:	0	2	0	16	0	18	<input type="button" value="v"/> <input type="button" value="▶"/>	<input type="button" value="PDF v"/> <input type="button" value="↓"/>
All filtered results:	0	2	0	0	0	2	<input type="button" value="v"/> <input type="button" value="▶"/>	<input type="button" value="PDF v"/> <input type="button" value="↓"/>
Filtered results 1 - 2:	0	2	0	0	0	2	<input type="button" value="v"/> <input type="button" value="▶"/>	<input type="button" value="PDF v"/> <input type="button" value="↓"/>

### Result Filtering

Sorting: [port ascending](#) | [port descending](#) | [threat ascending](#) | [threat descending](#)

Results per page:



# Strojové penetrační testování OpenVAS

## Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
<a href="#">192.168.0.104</a>	Apr 22, 07:16:39	Apr 22, 07:27:28	0	2	0	16	0
Total: 1			0	2	0	16	0

## Results per Host

### Host 192.168.0.104

Scanning of this host started at: 2014-04-22T07:16:39Z  
Number of results: 18

### Port Summary for Host 192.168.0.104

Service (Port)	Threat Level
otp (9390/tcp)	Medium
ssh (22/tcp)	Medium
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log

### Security Issues for Host 192.168.0.104

**Medium** (CVSS: 4.3) otp (9390/tcp)  
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

#### Summary:

This routine search for weak SSL ciphers offered by a service.

#### Vulnerability Insight:

These rules are applied for the evaluation of the cryptographic strength:

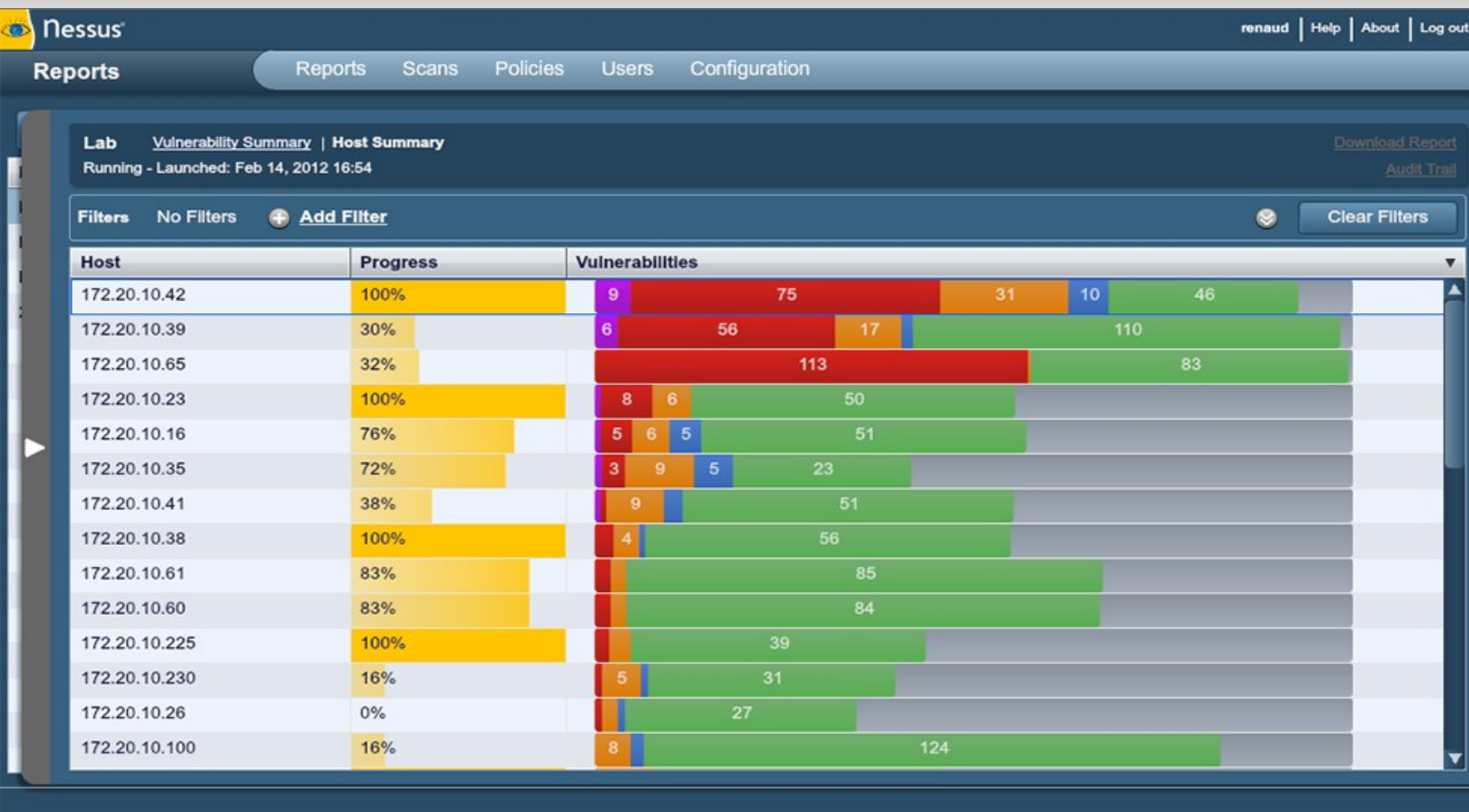
- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.



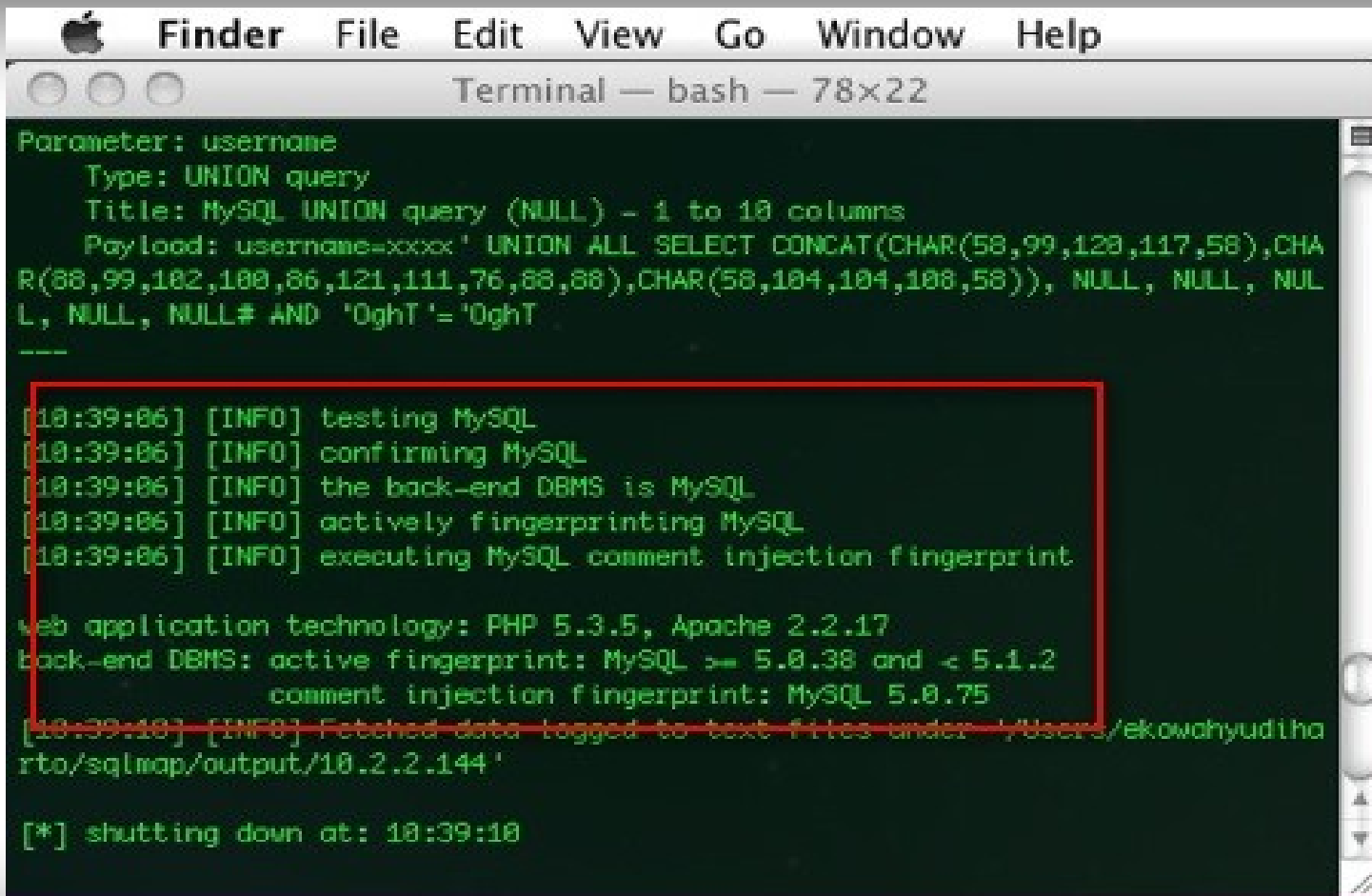


# Strojové penetrační testování

## Nessus



# Strojové penetrační testování sqlmap



```
Parameter: username
  Type: UNION query
  Title: MySQL UNION query (NULL) - 1 to 10 columns
  Payload: username=xxxx' UNION ALL SELECT CONCAT(CHAR(58,99,120,117,58),CHAR(88,99,102,100,86,121,111,76,88,88),CHAR(58,104,104,108,58)), NULL, NULL, NULL, NULL, NULL# AND 'OghT'='OghT
----

[10:39:06] [INFO] testing MySQL
[10:39:06] [INFO] confirming MySQL
[10:39:06] [INFO] the back-end DBMS is MySQL
[10:39:06] [INFO] actively fingerprinting MySQL
[10:39:06] [INFO] executing MySQL comment injection fingerprint

web application technology: PHP 5.3.5, Apache 2.2.17
back-end DBMS: active fingerprint: MySQL >= 5.0.38 and < 5.1.2
                comment injection fingerprint: MySQL 5.0.75
[10:39:10] [INFO] Fetched data logged to text files under '/Users/ekowachyudiha
rto/sqlmap/output/10.2.2.144'

[*] shutting down at: 10:39:10
```



# Ruční penetrační testování

- Zdlouhavější a nemusí pokrýt vše
  - Člověk může vynechat přehlednout
- Možnost on-line modifikovat postupy
- Využívá jednodušší nástroje
  - Ping, dig, nmap, curl, telnet,...
  - Lidskou invenci a pochopení dat
  - Složitější tvorba opakovatelných reportů



# Penetrační testy typické oblasti

- Chyby v nastavení sítí, FW a prostupů
- Backdoory známých aplikací
- DNS – možnost předstírat identitu
- WWW - DoS, DDoS, SQL Injection
- Mail – šíření spamu
- Obecně neautorizované přístupy
- ....



# Penetrační testy

- Důležitá je pravidelnost
- Testování nesmí omezovat provoz
- POZOR na tvorbu DDoS
- POZOR na poškození dat
- Konbinace s IDS
  - Pravidelná kontrola funkčnosti



# Výstup penetrační testů

- Klasicky zpráva auditora, kterou zákazník přebírá
- Výsledek musí být přehledný
  - Ideálně strojově zpracovatelný
  - Více formátů člověk / stroj, HTML / XML
- Ideální pravidelné opakování strojových testů



# Forenzní analýza

- Zajištění a konzervace dostupných stop
- Hlubokové zkoumání
  - Provedení útoků
  - Dopadů útoků
  - Tvorba ochranného plánu
- Slouží jako důkaz / potvrzení hypotéz



# Forenzní analýza

- Provádí po útoku na zakonzervovaném prostředí
  - Násobná binární kopie
- Opakování útoku / spuštění viru v izolovaném prostředí
  - Cílem je získat detailní znalosti o útoku
  - Zajistit možnost detekce
  - Zajistit možnost ochrany - patch





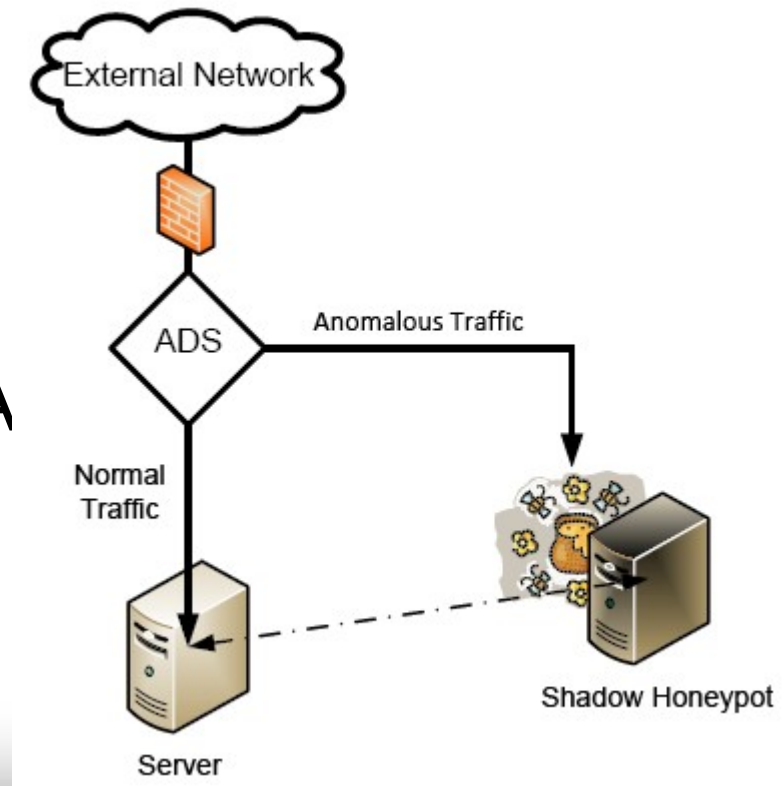
# Forenzní analýza typické cíle

- Zajištěné prostředí proti změnám
- Odhlední / obnova všech umyslně smazaných dat
- Odhalení / detekce skrytých dat a procesů
- Lámání šifrovaných částí dat / nástrojů
  - Pokud možno legální cestou - důkaz



# Honeypot

- Virtuální cesta / zdroj
- Nuhnost návnady
- Nemusí být reálné
- Nezasahujeme
- Doplněk pro For. A



# Honeypot

- Umožňuje v pro nás bezpečném prostředí zkoumat útočníka
- Nutná trpělivost + štěstí
- Velmi vhodné všechno monitorovat



# Obecně k testování

- Dává základní pocit bezpečí
- **NIKDY neodhalí vše**
- Vhodné kombinovat
  - Interní – plánovaný, pravidelný
  - Externí – skrytý, kontrola pravidelného
- **Nebrat jako útok na administrátora!**

