



UpGreat  
we know-how to do IT

Wsparcie dla biznesu



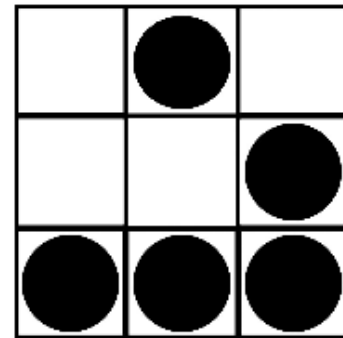


## WARSZTAT (ETHICAL) HACKERA

- Czym są testy penetracyjne
- Metodyki przeprowadzania testów
- Narzędzia wykorzystywane w testach
- Laboratorium – popularne ataki
- Z życia wzięte – wyniki testów penetracyjnych
- Jak podnieść poziom bezpieczeństwa

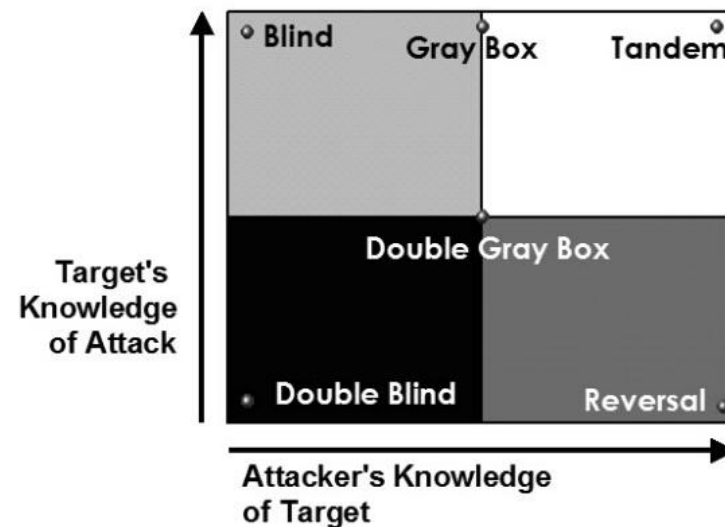
## TESTY PENETRACYJNE - TERMINOLOGIA

- **Ethical hacker / pentester**  
Osoba wykorzystująca techniki, wiedzę i narzędzia hackerów do przeprowadzania kontrolowanych testów / ataków
- **Czy hacker jest zły?**  
Nie, ale pojęcie to zostało nacechowane pejoratywnie przez media. W języku potocznym przyjęło się, iż hacker ma zawsze złe intencje.
- **White hat, black hat**  
W terminologii związanej z tematyką bezpieczeństwa używa się powyższych określeń dla odróżnienia hackerów „złych” od „dobrych”

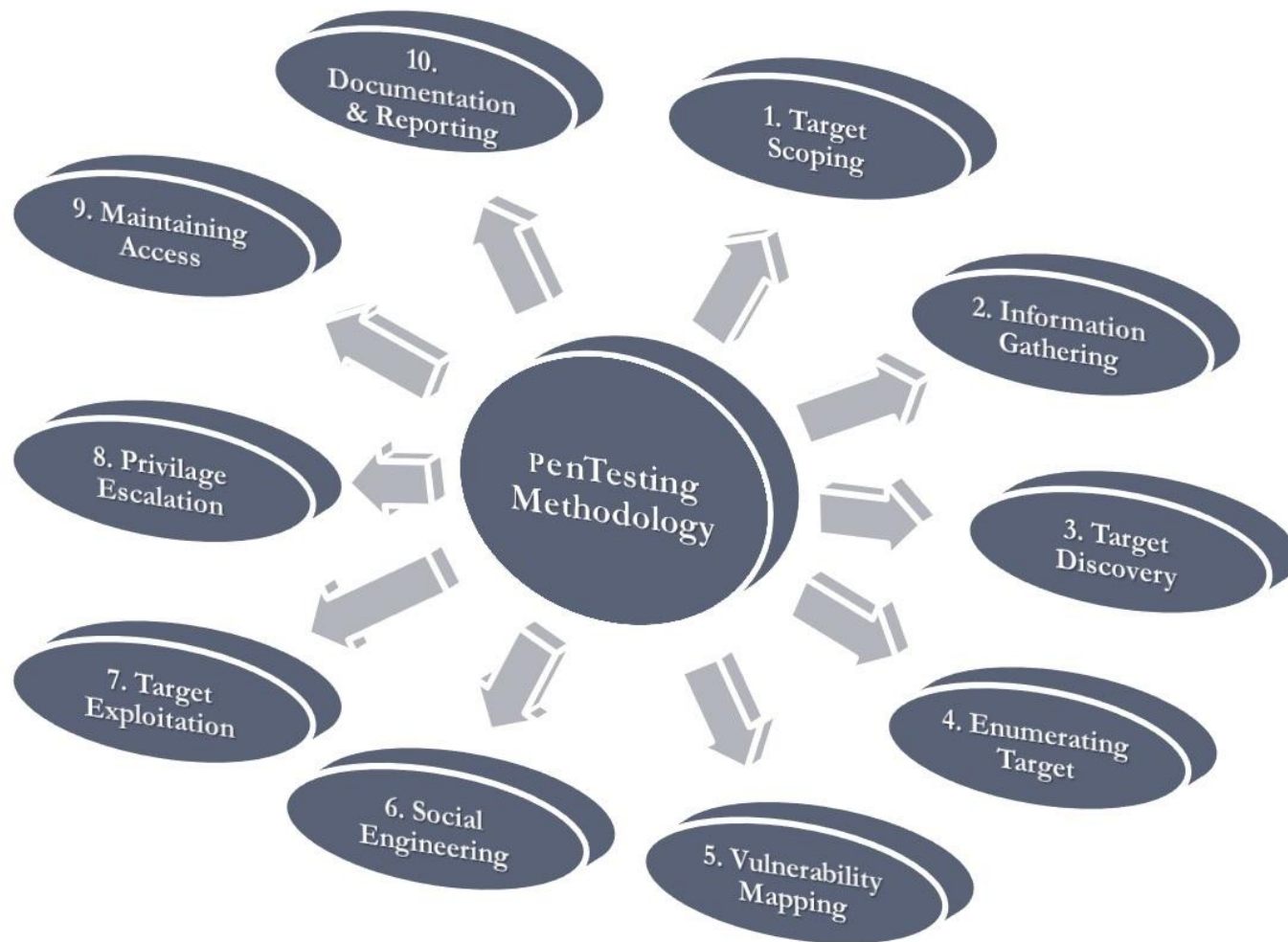


## METODYKI TESTÓW PENETRACYJNYCH

- OWASP Web Application Penetration Testing (Testing Guide)
- PTES Penetration Test Execution Standard
- Open Source Security Testing Methodology Manual (OSSTMM)
- EC-Council Licensed Penetration Tester methodology (LPT)
- NIST PUB 800-115

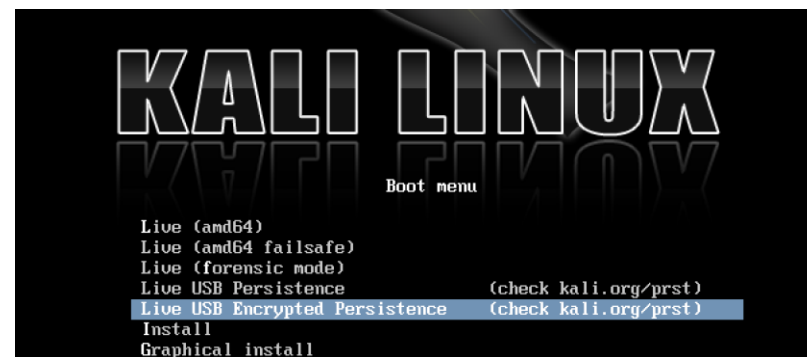
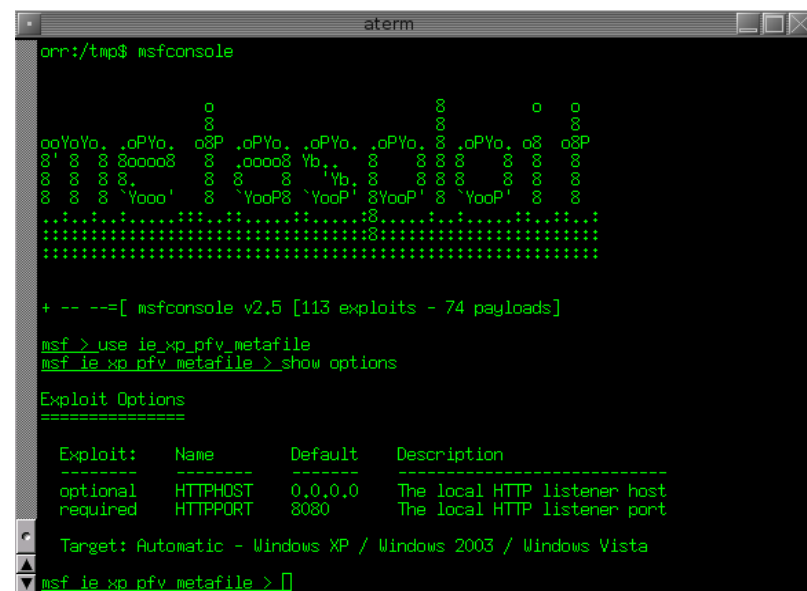


## FAZY TESTÓW PENETRACYJNYCH



## NARZĘDZIA (ETHICAL) HACKERA

- Rekonesans  
Google, RIPE, DNS, theHarvester
- Skanowanie portów i podatności  
Nmap, Nessus, Open-VAS, LanGuard  
sqlmap, wpscan
- Przechwytywanie ruchu  
Wireshark, airodump, burp suite
- Generowanie, wstrzykiwanie ruchu  
Scapy, hping, aireplay-ng, burp suite
- Exploits, Social engineering, C&C  
Metasploit, SET
- Łamanie haseł  
hydra, ncrack, hashcat, crunch

The image shows a terminal window titled 'aterm' running the Metasploit Framework (msfconsole). The prompt is 'orr:/tmp\$ msfconsole'. The user has entered the command 'use ie\_xp\_pf\_v\_metatile' and 'show options'. The output shows the 'Exploit Options' for the 'ie\_xp\_pf\_v\_metatile' exploit.

```

+ -- ==[ msfconsole v2.5 [113 exploits - 74 payloads]

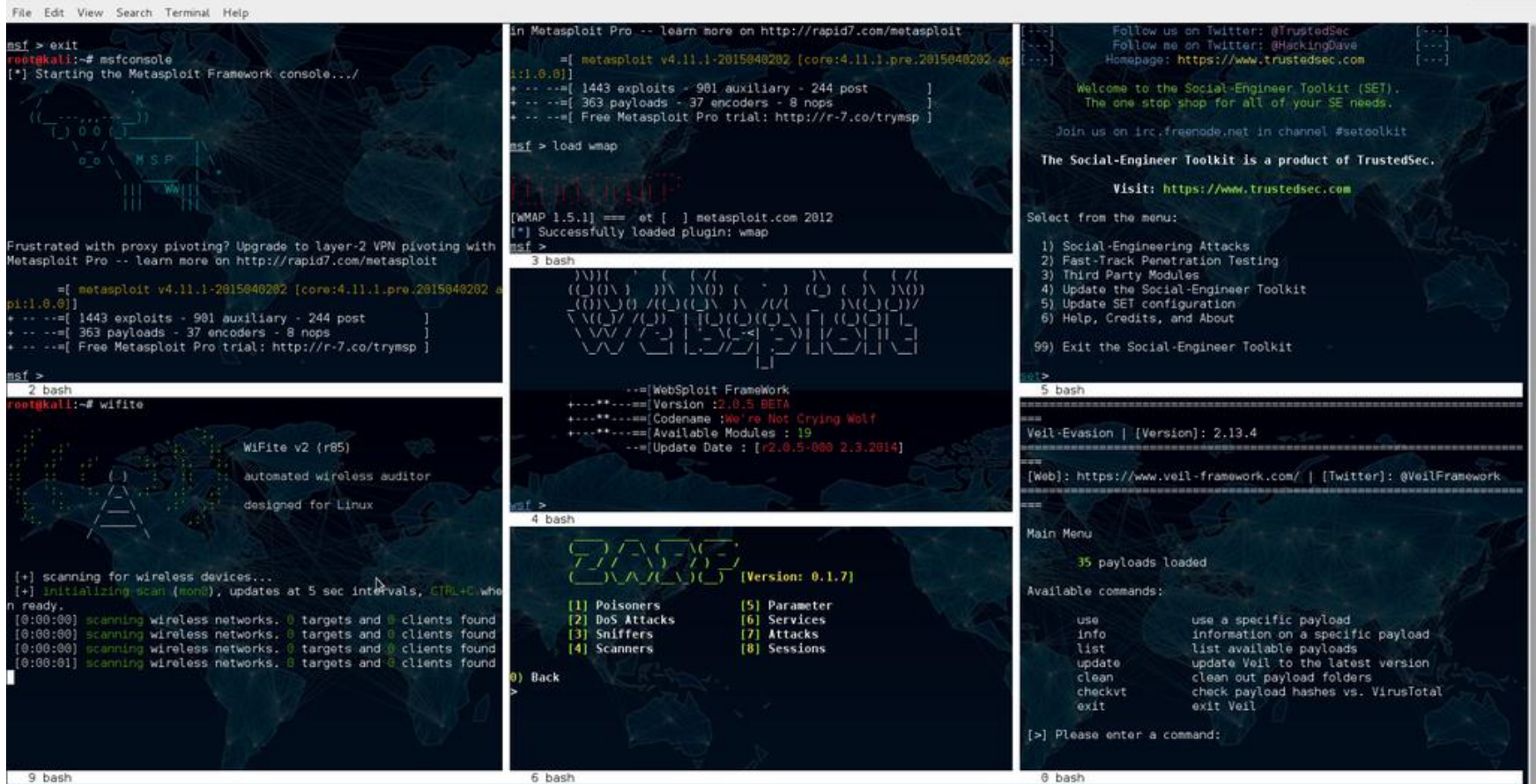
msf > use ie_xp_pf_v_metatile
msf ie_xp_pf_v_metatile > show options

Exploit Options
=====
Exploit:  Name      Default  Description
-----  -
optional HTTPHOST  0.0.0.0  The local HTTP listener host
required HTTPPORT  8080    The local HTTP listener port

Target: Automatic - Windows XP / Windows 2003 / Windows Vista

msf ie_xp_pf_v_metatile >
  
```

# NARZĘDZIA (ETHICAL) HACKERA



The image displays a grid of terminal windows showcasing several ethical hacking tools:

- Metasploit Pro:** Shows the framework's version (v4.11.1-2015040202), statistics (1443 exploits, 901 auxiliary, 244 post, 363 payloads, 37 encoders, 8 nops), and the loading of the wmap plugin.
- WiFiMap:** A network mapping tool for wireless networks, version 1.5.1.
- WiFiFite:** An automated wireless auditor, version v2 (r85), designed for Linux.
- WebSploit Framework:** Version 2.0.5 BETA, with a codename 'We're Not Crying Wolf' and 19 available modules.
- Veil Framework:** Version 2.13.4, featuring 35 payloads and a menu of commands like 'use', 'info', 'list', 'update', 'clean', 'checkvt', and 'exit'.

## JAKIEGO SPRZĘTU POTRZEBUJEMY?

- Karta WIFI**  
 Odpowiedni chipset i sterownik wspierające wstrzykiwanie.  
 Zewnętrzna antena o lepszym zasięgu.
- Wydajne GPU/CPU**  
 Ewentualnie dostęp do wydajnego środowiska chmurowego

```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1		11	WPA2	63db	no	
2		11	WPA2	55db	no	clients
3		11	WPA2	29db	no	client

```
[0:00:49] scanning wireless networks. 3 targets and 7 clients found
```

```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1		11	WPA2	59db	no	client
2		11	WPA2	28db	no	
3		8	WPA2	27db	no	
4		1	WPA	26db	no	client
5		1	WPA2	25db	no	
6		1	WPA2	25db	no	
7		1	WPA	23db	no	
8		3	WPA2	21db	no	
9		3	WPA2	20db	no	
10		6	WPA2	19db	no	
11		1	WPA2	19db	no	
12		7	WPA2	19db	no	clients
13		2	WPA2	19db	no	
14		11	WPA2	18db	no	
15		11	WPA2	18db	no	
16		11	WPA2	18db	no	
17		1	WPA2	17db	no	
18		11	WPA2	16db	no	
19		11	WPA2	16db	no	
20		11	WPA2	16db	no	
21		11	WPA2	16db	no	
22		11	WPA2	15db	no	
23		11	WPA2	14db	no	
24		2	WPA2	11db	no	

```
[0:01:09] scanning wireless networks. 24 targets and 5 clients found
```



## LABORATORIUM

- Atak MITM przez zatrucie ARP  
Cain&Abel oraz APR – arp poison routing
- Atak na WLAN WEP x 2  
Aircrack-ng, wifite
- Atak na WLAN WPA2  
Aircrack-ng, metody słownikowe
- Wektor ataku socjotechnicznego  
Metasploit Framework, file wrapping



## WYNIKI TESTÓW

- **Tajne - umowa o poufności**  
Zabezpieczone kryptologicznie,  
dane przesyłane dwoma kanałami  
komunikacji
- **Raport**  
Zestawienie znalezionych podatności,  
luk oraz zagrożeń
- **Analiza ryzyka**  
Ocena zagrożeń wynikających ze  
znalezionych podatności
- **Propozycje usprawnień**  
Opis rozwiązań pozwalających wyeliminować  
lub zminimalizować znalezione zagrożenia.



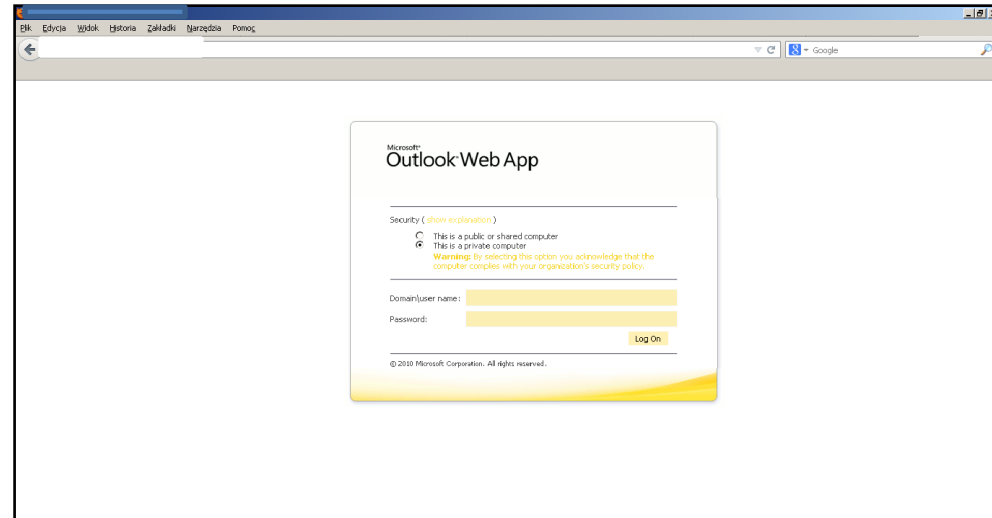
## WYNIKI TESTÓW – REKONESANS INFORMACYJNY

- Duża ilość danych osobowych przydatnych w atakach socjotechnicznych
- Zdjęcia, nazwiska, stanowiska pracy, numery telefonów, adresy e-mail
- Również członkowie zarządu, główna księgowa kadrowa, dyrektor IT
- Duże ryzyko wykorzystania danych w ataku socjotechnicznym



## WYNIKI TESTÓW - PHISING

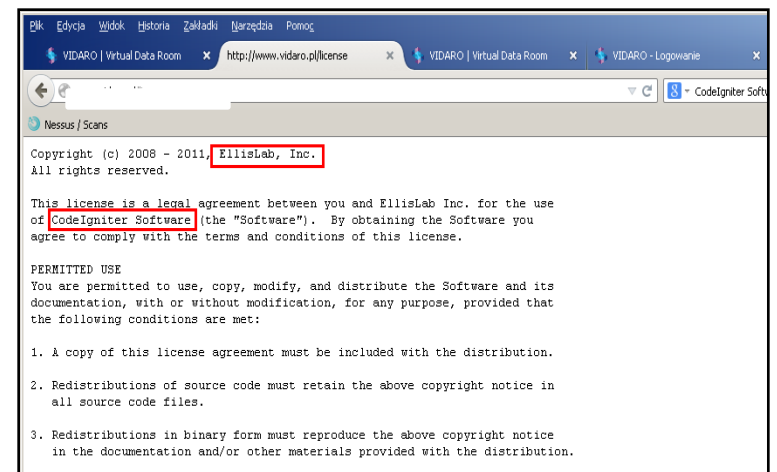
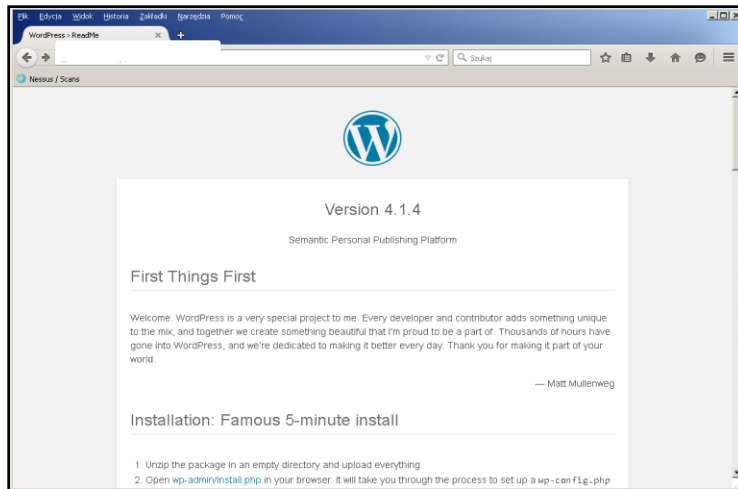
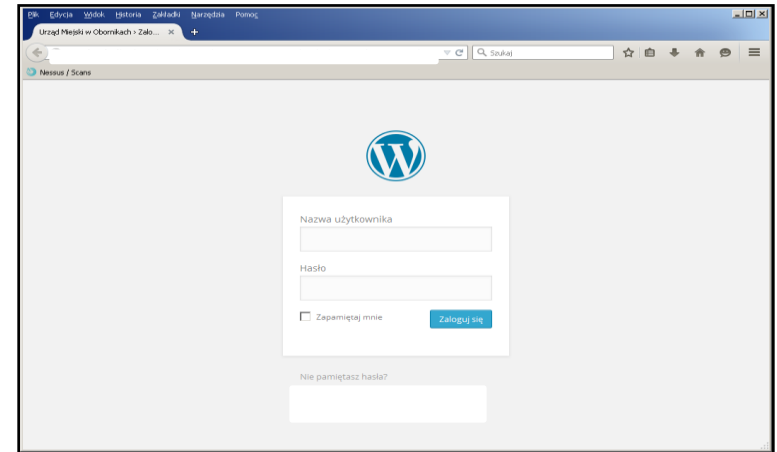
- Fałszywy serwis OWA pod nietypowym adresem URL z obcej domeny
- Wysłana prośba do użytkowników o weryfikację działania umotywowana wymianą serwera
- Skuteczność 50%



2013-05-28 13:14:02 10.20.30.40 **username=XXXXXXXX&password=XXXXXXXX&SubmitCreds=Log+On**

2013-05-28 13:46:29 10.20.30.40 **username=XXXXXXXX&password=XXXXXXXX&SubmitCreds=Log+On**

# WYNIKI TESTÓW – OWASP TOP 10



## WYNIKI TESTÓW - SKANOWANIE

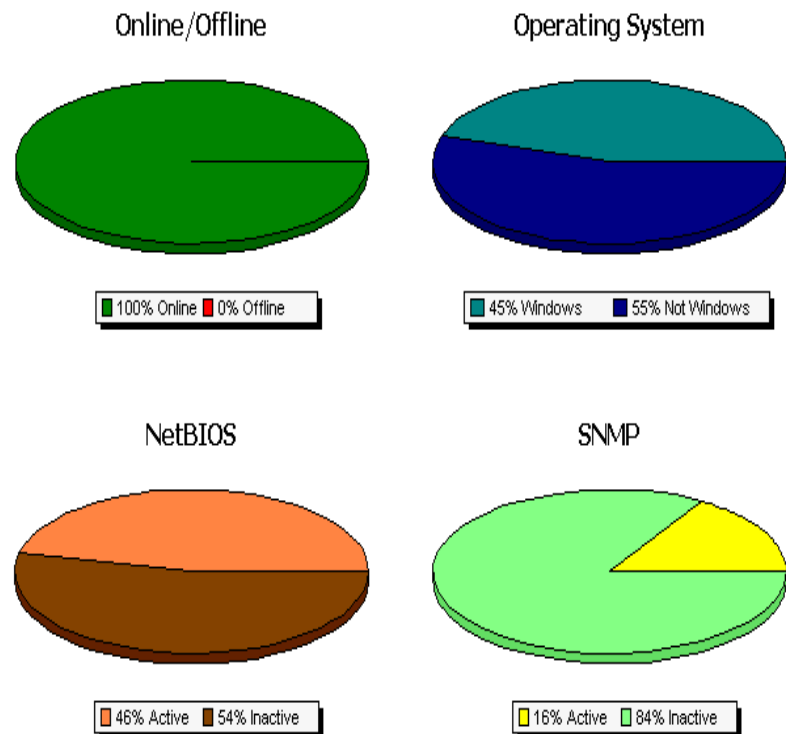
- Skanowanie nmap
- Ponad 20 otwartych portów TCP/UDP

Scanning xxxxxxxx.v-isp.energis.pl (xx.xx.xx.xx)

Discovered open port 993/tcp on xx.xx.xx.xx  
 Discovered open port 3389/tcp on xx.xx.xx.xx  
 Discovered open port 587/tcp on xx.xx.xx.xx  
 Discovered open port 25/tcp on xx.xx.xx.xx  
 Discovered open port 443/tcp on xx.xx.xx.xx  
 Discovered open port 143/tcp on xx.xx.xx.xx  
 Discovered open port 80/tcp on xx.xx.xx.xx  
 Discovered open port 1025/tcp on xx.xx.xx.xx  
 Discovered open port 445/tcp on xx.xx.xx.xx  
 Discovered open port 135/tcp on xx.xx.xx.xx  
 Discovered open port 139/tcp on xx.xx.xx.xx  
 Discovered open port 1026/tcp on xx.xx.xx.xx  
 Discovered open port 5666/tcp on xx.xx.xx.xx  
 Discovered open port 593/tcp on xx.xx.xx.xx  
 Discovered open port 6004/tcp on xx.xx.xx.xx  
 Discovered open port 7070/tcp on xx.xx.xx.xx  
 Discovered open port 1027/tcp on xx.xx.xx.xx

Exportation Date	14/08/2012 11:44
Total IP Addresses in list	964
Total IP Addresses ONLINE	964
Total IP Addresses OFFLINE	0

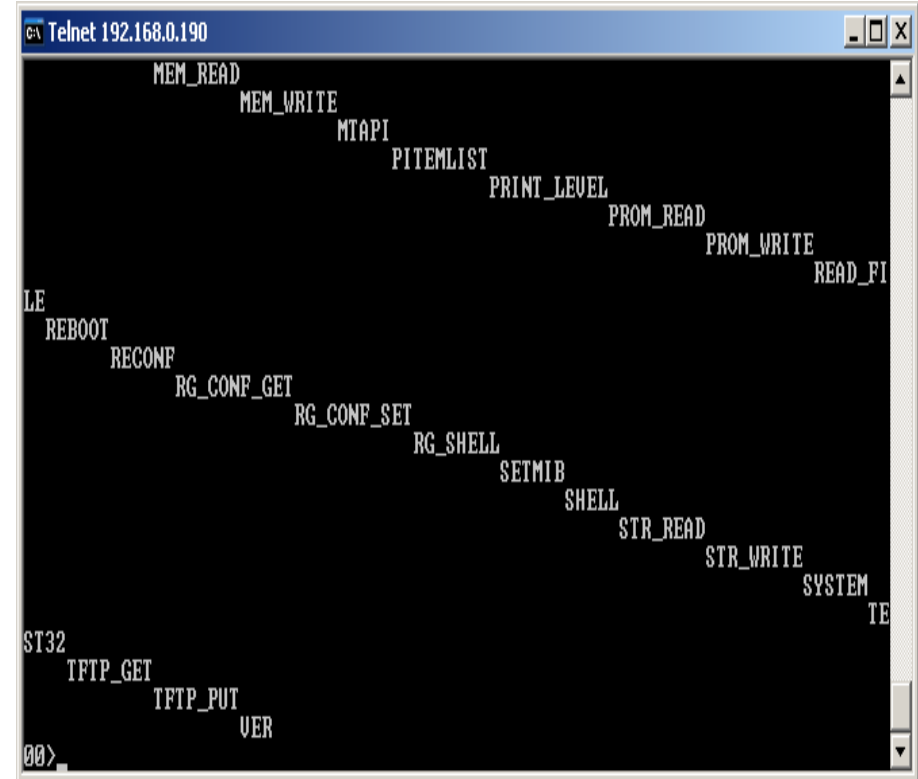
Scan Ranges	
FROM IP	TO IP
192.168.0.1	192.168.255.254



## WYNIKI TESTÓW – OTWARTE PORTY

- AP WAP610N
- Otwarty port 1111
- telnet xx.xx.xx.xx 1111

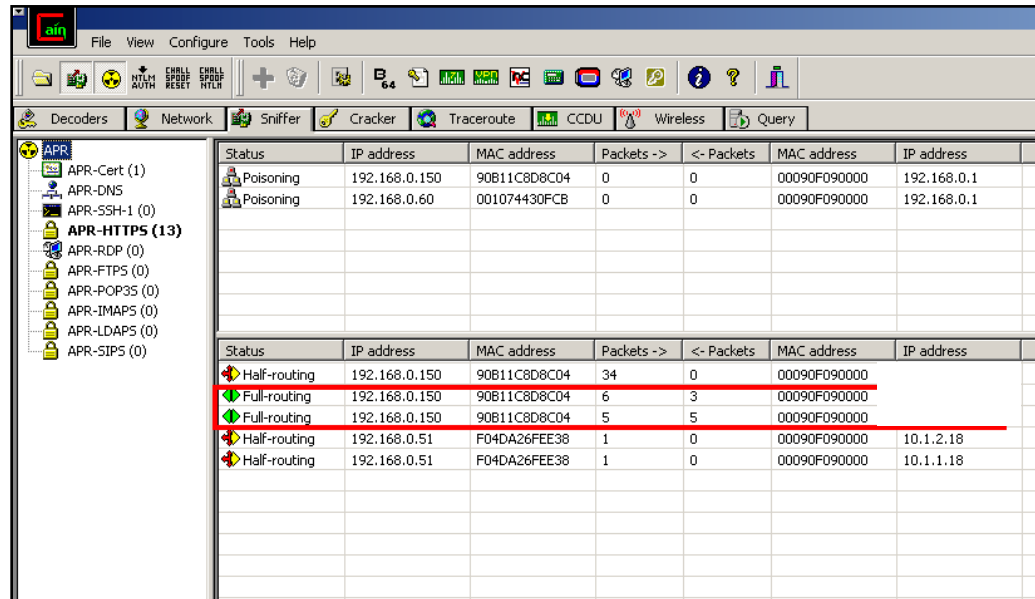
```
> system cat /etc/shadow
root:$1$ZAwqf2dl$ZukbihyQtU
ghNDsLAQaP31:10933:0:99999:7:::
Bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
```



The screenshot shows a Telnet window titled "Telnet 192.168.0.190". The window displays a list of system services and their status, arranged in a staircase pattern from top-left to bottom-right. The services listed are: MEM\_READ, MEM\_WRITE, MTAPl, PITEMLIST, PRINT\_LEVEL, PROM\_READ, PROM\_WRITE, READ\_FI, REBOOT, RECONF, RG\_CONF\_GET, RG\_CONF\_SET, RG\_SHELL, SETMIB, SHELL, STR\_READ, STR\_WRITE, SYSTEM, TFTP\_GET, TFTP\_PUT, UVER, and ST32. The prompt "00>" is visible at the bottom left of the window.

## WYNIKI TESTÓW - MITM

- Udane zatrucie tablicy ARP
- Umożliwienie ataku MITM
- Podśluchanie 13 sesji HTTP
- Przechwycenie loginów i haseł do usług sieciowych



The screenshot shows the Cain & Abel interface with the 'Sniffer' tab active. The left pane shows a tree view of sniffed protocols, with 'APR-HTTPS (13)' selected. The main pane displays two tables of sniffed data.

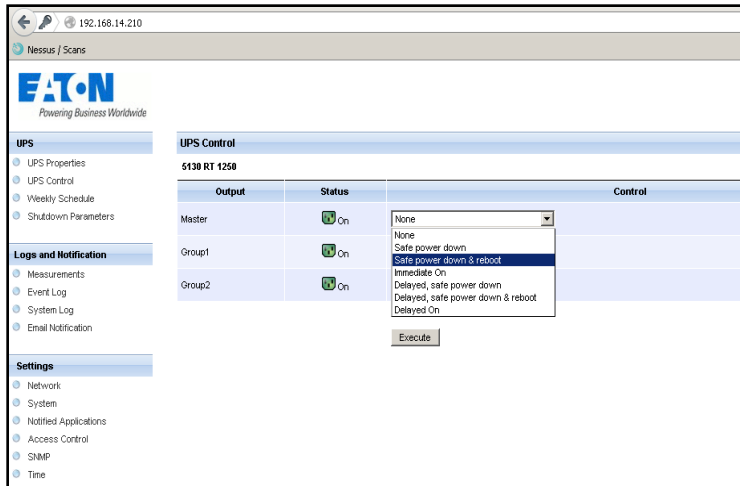
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.0.150	90B11C8D8C04	0	0	00090F090000	192.168.0.1
Poisoning	192.168.0.60	001074430FCB	0	0	00090F090000	192.168.0.1

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.0.150	90B11C8D8C04	34	0	00090F090000	
Full-routing	192.168.0.150	90B11C8D8C04	6	3	00090F090000	
Full-routing	192.168.0.150	90B11C8D8C04	5	5	00090F090000	
Half-routing	192.168.0.51	F04DA26FEE38	1	0	00090F090000	10.1.2.18
Half-routing	192.168.0.51	F04DA26FEE38	1	0	00090F090000	10.1.1.18



# WYNIKI TESTÓW – ADMIN: ADMIN

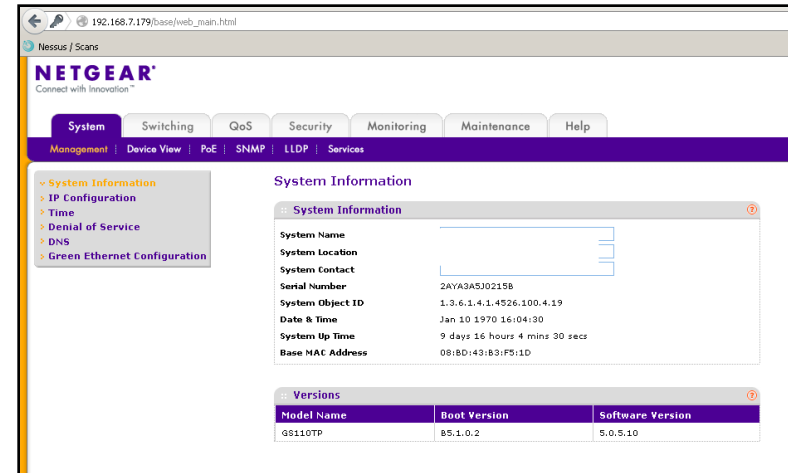


UPS Control

5130 RT 1250

Output	Status	Control
Master	On	None
Group1	On	Safe power down & reboot
Group2	On	Delayed, safe power down & reboot

Execute



System Information

System Name

System Location

System Contact

Serial Number: 2AY3A5J0215B

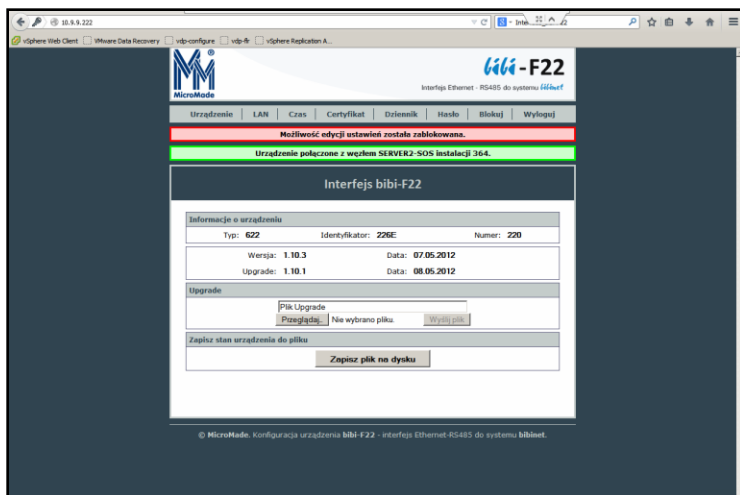
System Object ID: 1.3.6.1.4.1.4526.100.4.1.9

Date & Time: Jan 10 1970 16:04:30

System Up Time: 9 days 16 hours 4 mins 30 secs

Base MAC Address: 08:8D:43:83:F5:1D

Model Name	Boot Version	Software Version
GE110TP	B5.1.0.2	5.0.5.10



Interfejs bibi-F22

Informacje o urządzeniu

Typ: 622    Identyfikator: 226E    Numer: 220

Wersja: 1.10.3    Data: 07.05.2012

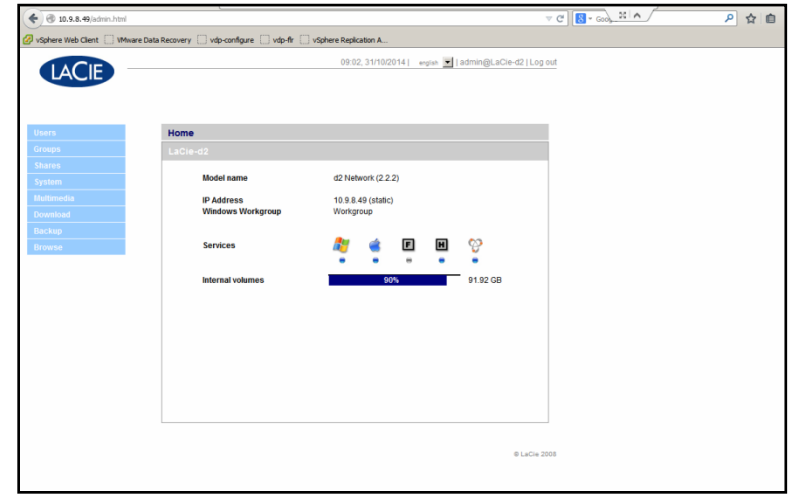
Upgrade: 1.10.1    Data: 08.05.2012

Plik Upgrade

Wybierz plik

Zapisz stan urządzenia do pliku

Zapisz plik na dysku



Home

Model name: d2 Network (2.2.2)

IP Address: 10.8.8.49 (static)

Windows Workgroup

Services

Internal volumes: 90% 91.92 GB

# WYNIKI TESTÓW – ADMIN: ADMIN

Generated with a demo version of Phoenix Contact® WebVisi 1

Sekcja	Licznik całkowity	Licznik zmiany	Material wsadowy
Sekcja A	6112339	613	OK
Sekcja B	6543700	620	OK
Sekcja C	7013774	676	OK

Generated with a demo version of Phoenix Contact® WebVisi 1

## Linia do produkcji palet LPP1

**Praca** (STOP)

**Wydajność maszyny** (0 to 4200)

**Podawanie** (OFF)

Licznik całkowity: 29966776  
Licznik zmiany: 576

A1: 0  
A2: 0

Komunikat

WEB SERVICE: Live, Odtwórz, Alarm, Ust., Wyłączone

KAM 1, KAM 2, KAM 3, KAM 12

2014-11-04 13:22:14, 2014-11-04 13:22:19, 2014-11-04 13:21:14, 2014-11-04 13:21:33

NOVUS MANAGEMENT SYSTEM

Podgląd na żywo | Statystyki

03-17-2015 Tue 21:19:00, 03-17-2015 Tue 21:17:30

Wybierz tryb obrazu: Obrazy

Wybierz podział obrazu: 1:1, 4:1

Wybierz źródło wideo: Strumień 1, Strumień 8, Strumień 10, Strumień 15

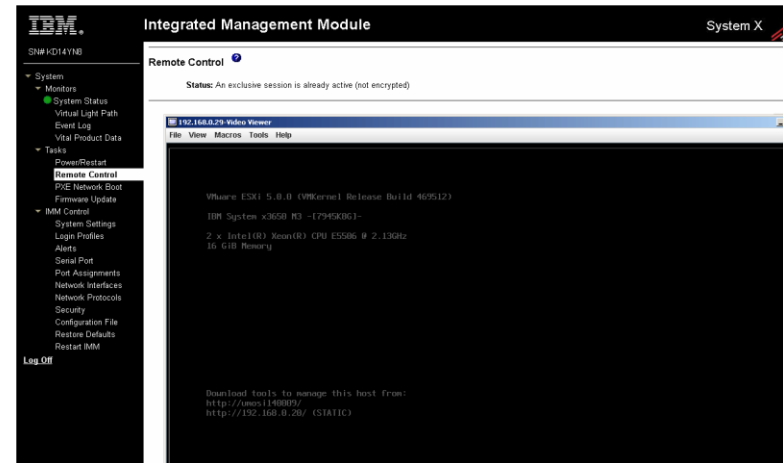
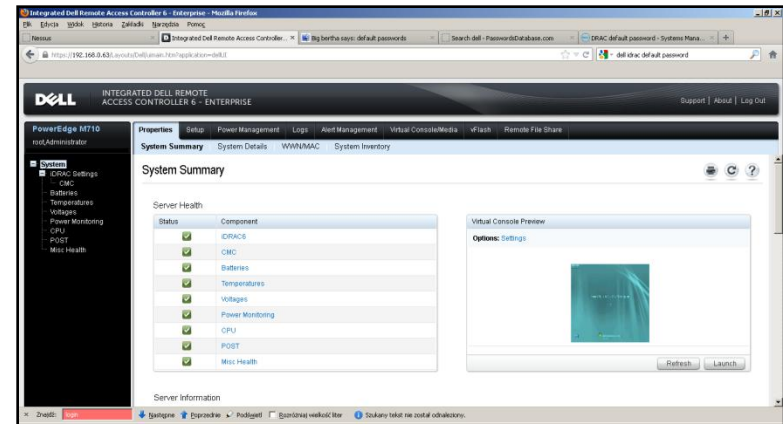
Jakość: VGA, QVGA

Odlizywanie: 1000 ms

Licznik klatek: 630

# WYNIKI TESTÓW – SERVER REMOT CONTROL

- DELL (DRAC) – root: calvin
- IBM, Lenovo – USERID: PASSWORD



## WYNIKI TESTÓW – CENTRALA TELEFONICZNA

- Centrala telefoniczna Alcatel Omni PCX
- Wyłączony interfejs WEB ale w źródle strony HTML:

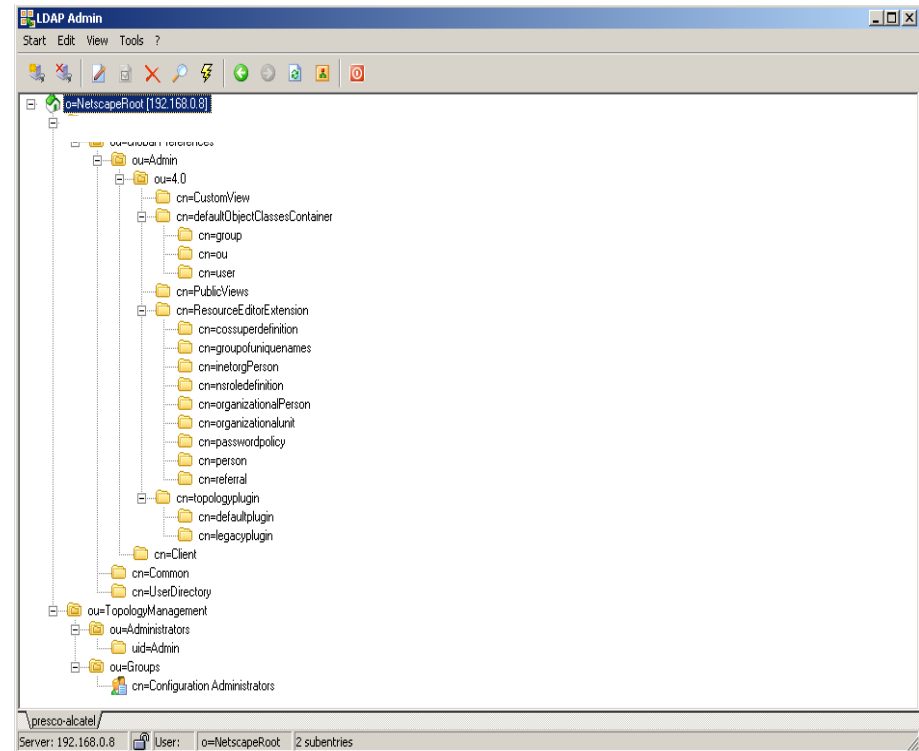
```
<PARAM NAME="LDAPServer" VALUE="ALCATEL">
<PARAM NAME="LDAPPort" VALUE="389">
<PARAM NAME="LDAPDn" VALUE="o=nmc">
<PARAM NAME="TraceFile" VALUE="Log.properties">
<PARAM NAME="TraceType" VALUE="NMCT_ALL">
```



## WYNIKI TESTÓW – CENTRALA TELEFONICZNA C.D.

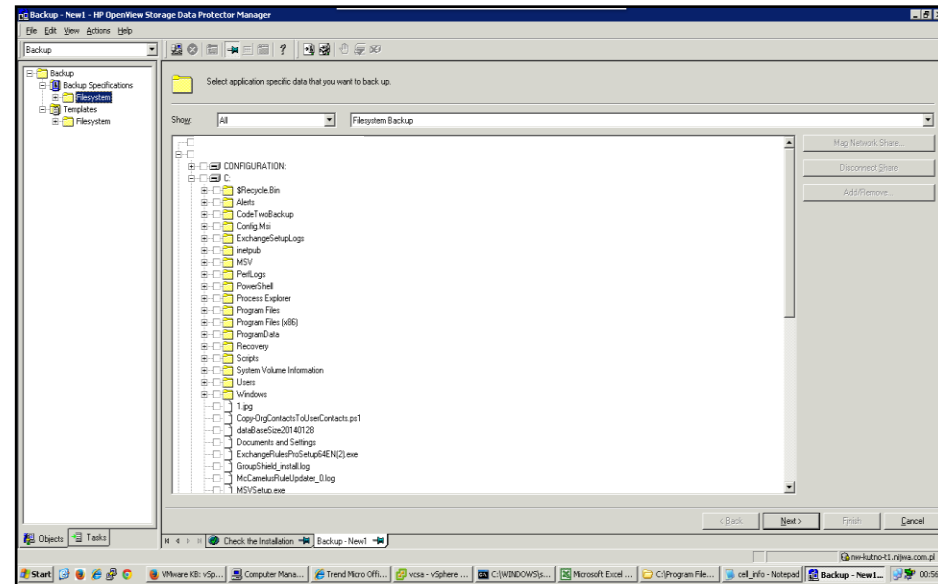
- Połączenie klientem LdapAdmin na dane ze źródła strony WWW
- Dostęp do zasobów usługi katalogowej, a w nich:

LDAP\_o-nmc.ldif:serverpassword: {NMC}cOskEilk  
LDAP\_o-nmc.ldif:swinstpassword: {NMC}OcsEskdi



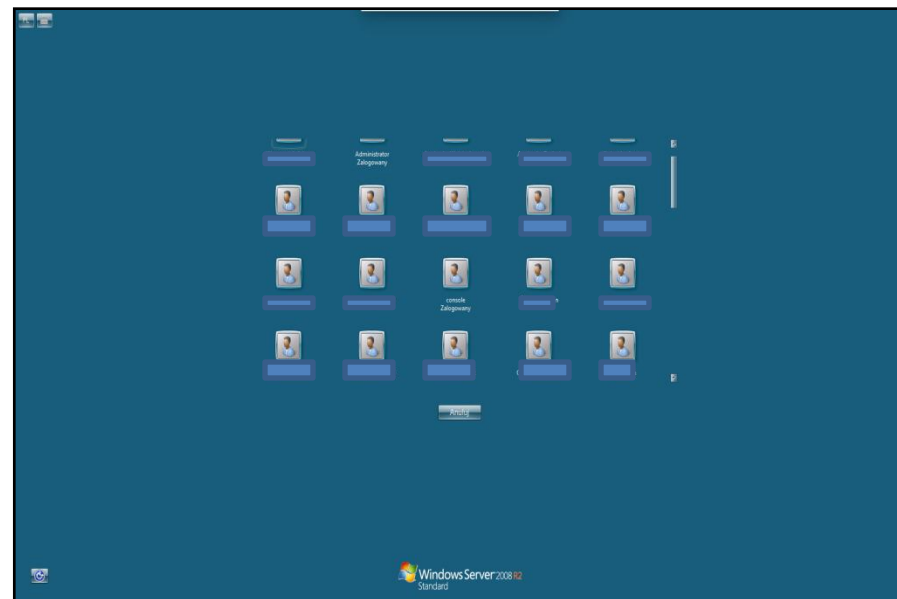
## WYNIKI TESTÓW – BACKUP DO CHMURY

- HP DataProtector Disk Agent na porcie 5555
- Brak ACL na firewallu
- Dostęp ograniczony na poziomie oprogramowania do backupu...
- ...Ale da się to ograniczenie obejść przez modyfikację tekstowego pliku z listą klientów



## WYNIKI TESTÓW – PO CO VPN?

- Brak profesjonalnych rozwiązań VPN dla pracowników zdalnych
- Protezy w postaci RDP, VNC
- Brak poprawnej polityki haseł
- Skutek? Wysokie prawdopodobieństwo, że użytkownik będzie się logował hasłem w stylu: Imie123, Imie2015.....
- Pełen dostęp do danych i infrastruktury firmy



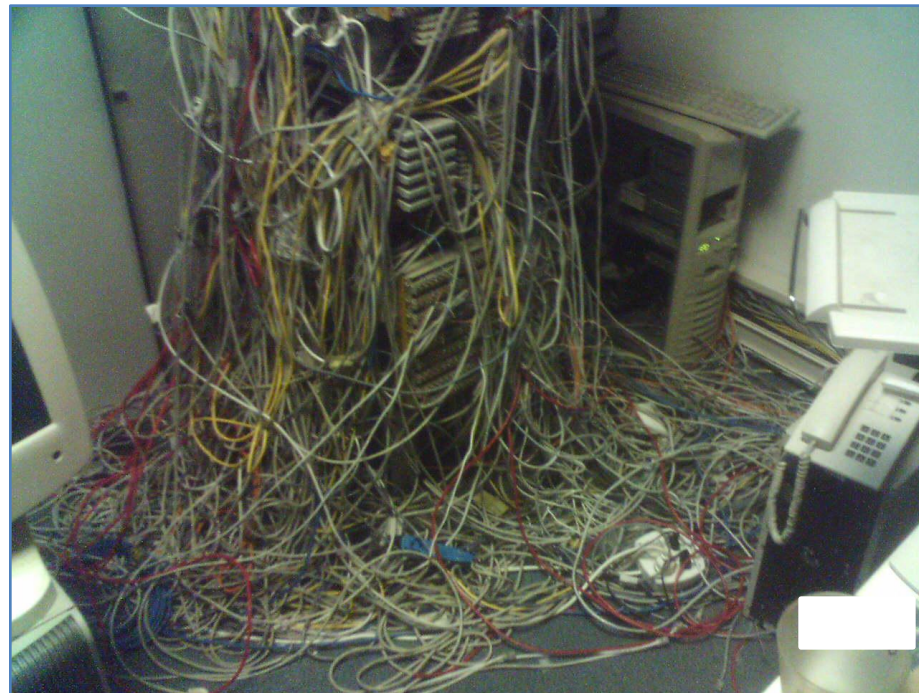
## WYNIKI TESTÓW – ZNALEZIONE „FANTY”

- Skany dowodów osobistych członków zarządu
- Dokumenty spółki (umowy, dokumenty księgowe, prawnicze)
- Dokumenty handlowe (cenniki, informacje o konkurencji, dane konkursowe)
- Katalogi: „faktury elektroniczne”, „księgowość”, „IT” (pliki z hasłami, certyfikaty NBP, klucze szyfrujące do dysków twardych)
- Bazy z danymi osobowymi



## NA CO JESZCZE ZWRACAMY UWAGĘ?

- Organizacja okablowania  
Uporządkowanie, oznaczenia, zabezpieczenia fizyczne.
- Swoboda dostępu do budynków i pomieszczeń  
Przepustki, osoba oprowadzająca
- Obecność ogólnodostępnych punktów sieciowych  
Np. możliwość podpięcia się pod drukarkę na korytarzu

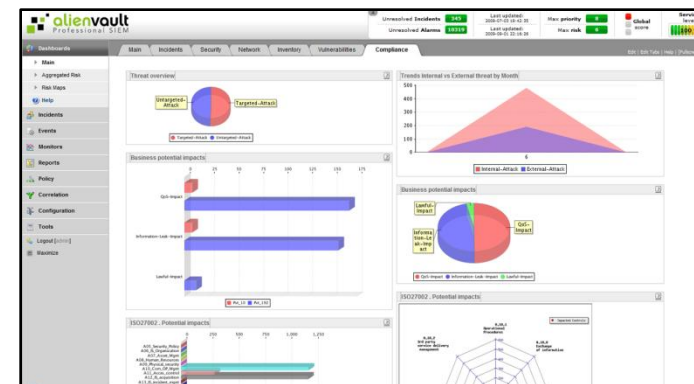


## JAK SIĘ ZABEZPIECZYĆ?

- **Okresowe audyty bezpieczeństwa i testy penetracyjne**  
Wymagane np. przez ISO27001 i rozporządzenie o KRI
- **Polityki bezpieczeństwa**  
Klasyfikacja aktywów, szacowanie ryzyka, zgodność z przepisami prawa, np. Ustawa O Ochronie Danych osobowych i KRI
- **Szkolenia pracowników**  
Kwestie ochrony danych, stosowania polityk, informacje o aktualnych zagrożeniach, konsekwencjach i metodach ochrony
- **SOC – Security Operations Center**  
Stała opieka, monitoring, dokumentacja, filtrowanie ruchu, IPS/IDS, SIEM, gromadzenie i archiwizacja logów, śledzenie zagrożeń, inwentaryzacja, zarządzanie podatnościami i aktualizacjami, reagowanie na incydenty bezpieczeństwa

## SOC – OUTSOURCING

- Problem z zatrudnieniem  
Brak specjalistów, wysokie koszty
- Problem z utrzymaniem  
Ryzyko znalezienia lepszej pracy. Tracimy eksperta z dużą wiedzą o naszej firmie.
- Problem z dostarczeniem narzędzi  
Drogie we wdrożeniu i utrzymaniu systemu wymagane do realizacji zadań SOC
- Zalety outsourcingu  
Większe zaplecze kadrowe z własnymi narzędziami. Doświadczenie, spojrzenie z szerszej perspektywy.





## Dziękuję za uwagę

- <http://www.upgreat.pl/blog>
- <http://www.facebook.com/upgreat.poznan>

Dziękuję za uwagę

**Jakub Staśkiewicz**

tel.: 667 768 452

mail: [jakub.staskiewicz@upgreat.pl](mailto:jakub.staskiewicz@upgreat.pl)

UpGreat Systemy Komputerowe Sp. z o.o.

60-122 Poznań, ul. Ostrobramska 22

<http://www.upgreat.com.pl>