
UpGreat
we know-how to do IT
Wsparcie dla biznesu

UpGreat
we know-how to do IT

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

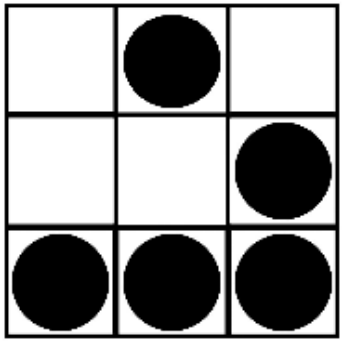
Jakub Staśkiewicz
UpGreat Systemy Komputerowe Sp. z o.o.

TESTY PENETRACYJNE - TERMINOLOGIA

- Ethical hacker / pentester
  Osoba wykorzystująca techniki, wiedzę i narzędzia hackerów do przeprowadzania kontrolowanych testów / ataków

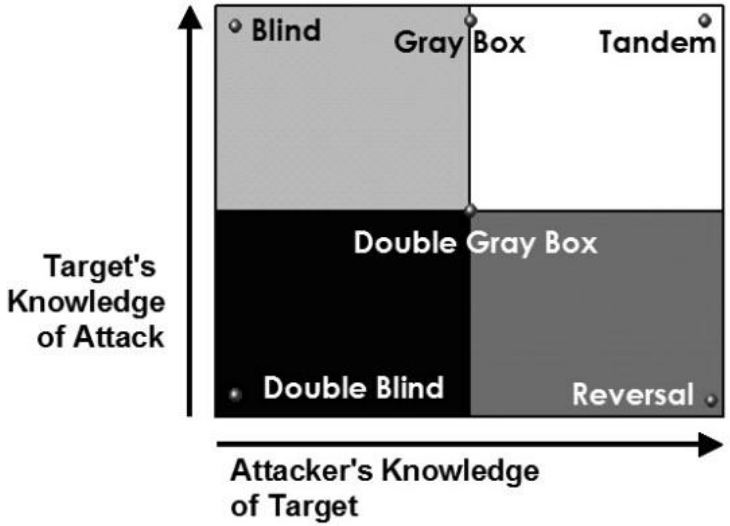
- Czy hacker jest zły?
  Nie, ale pojęcie to zostało nacechowane pejoratywnie przez media. W języku potocznym przyjęło się, iż hacker ma zawsze złe intencje.

- 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

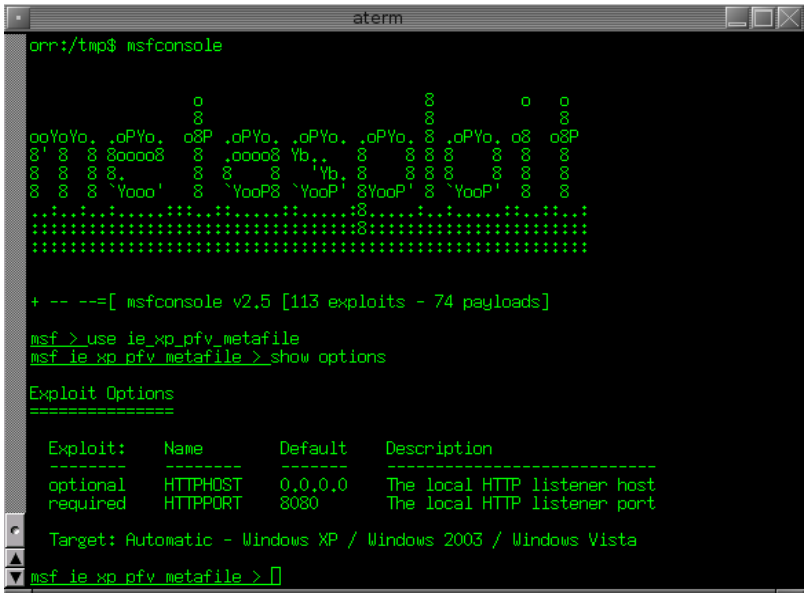


UpGreat
we know-how to do IT

FAZY TESTÓW PENETRACYJNYCH

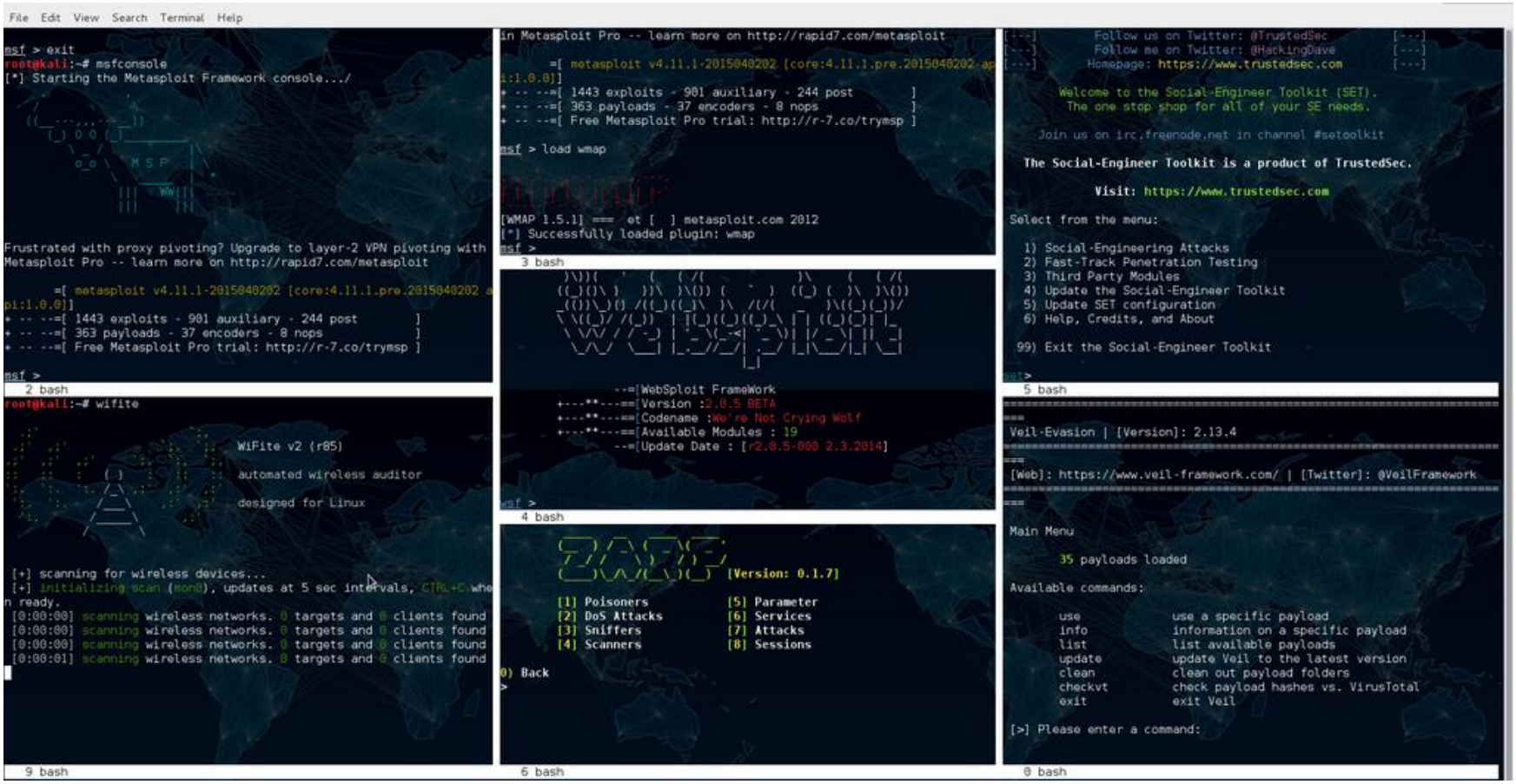
NARZĘDZIA (ETHICAL) HACKERA

- 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



UpGreat
we know-how to do IT

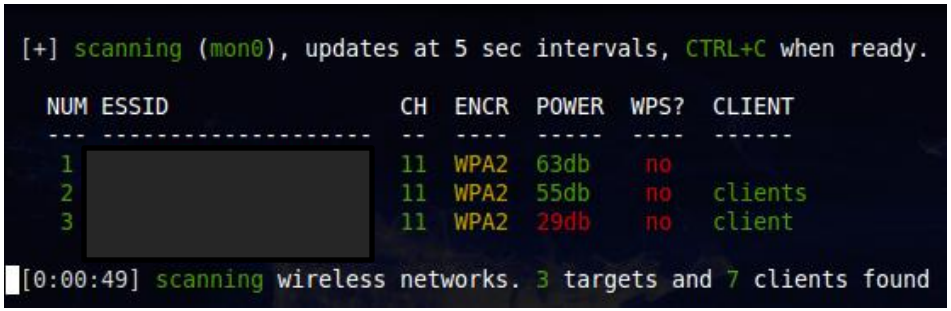
NARZĘDZIA (ETHICAL) HACKERA



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



LABORATORIUM

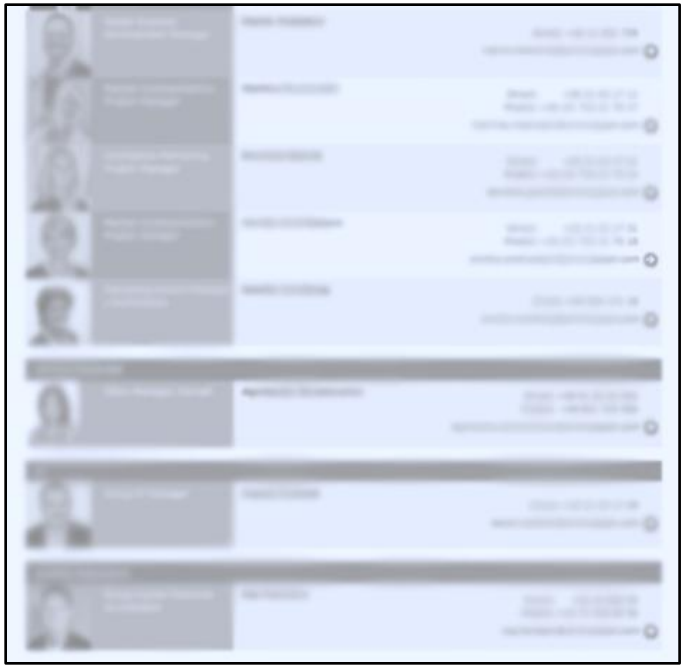
- Atak MITM przez zatruwanie ARP
  Cain&Abel oraz APR – arp poison routing
- Atak na WLAN WEP x 2
  Aircrack-ng, wifite
- Atak na WLAN WPA2
  Aircrack-ng, metody słownikowe
- Wektor ataku socjotechnicznego
  Metasploit Framework, file wrapping

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.

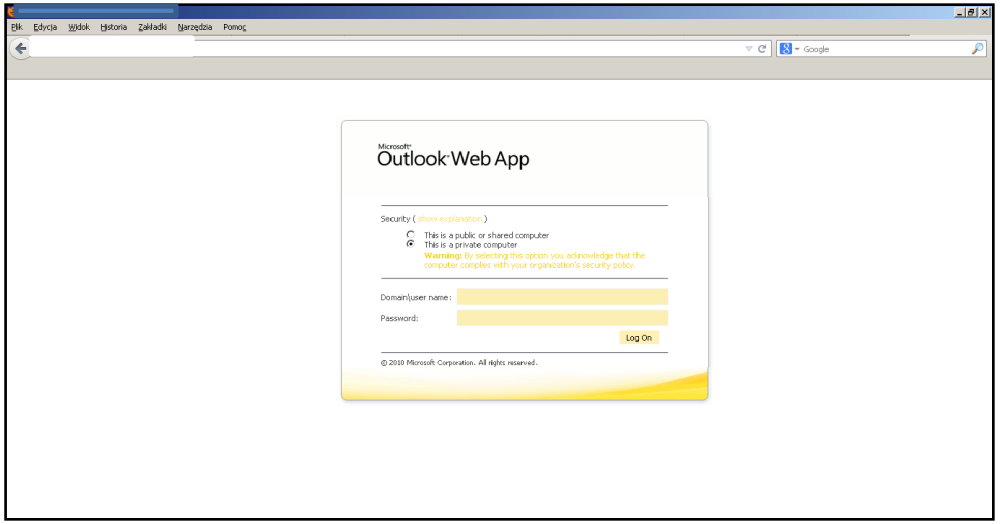
WYNIKI TESTÓW – REKONESANS INFORMACYJNY

- 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



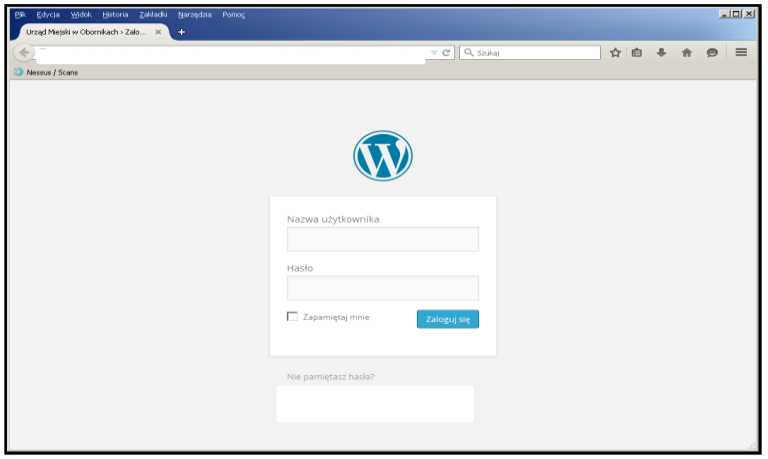
WYNIKI TESTÓW - PHISING

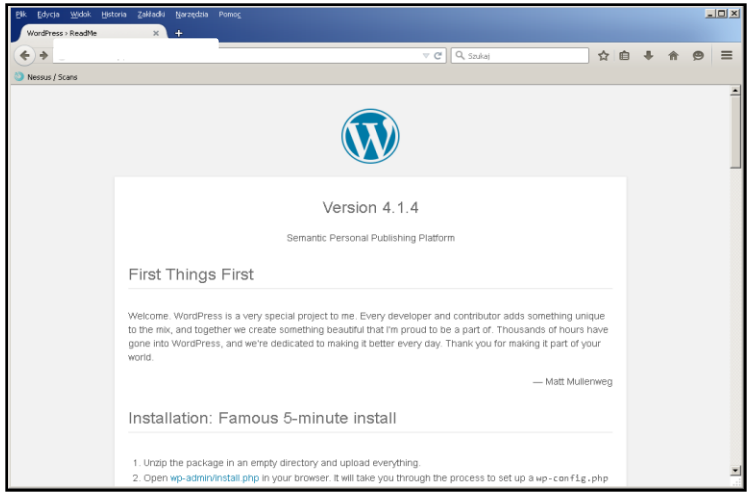
- Fałszywy serwis OWA pod nietypowym adresem URL z obcej domeny
- Wysłana prośba do użytkowników o weryfikację działania umotywowana wymianą serwera
- Skuteczność 50%

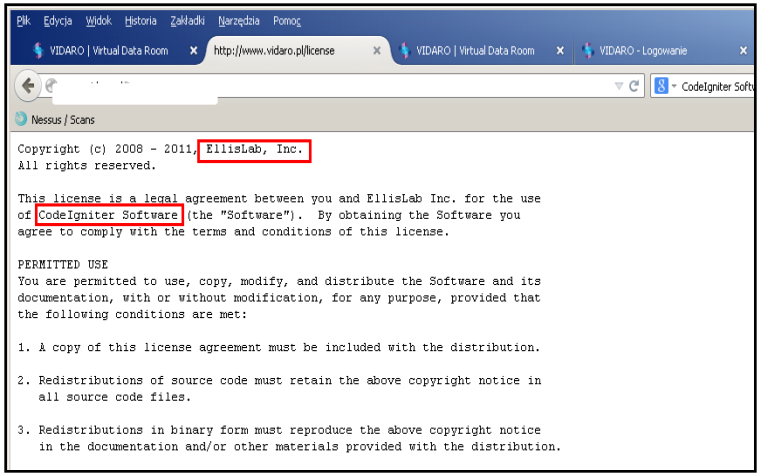


2013-05-28 13:14:02 10.20.30.40 **username=XXXXXXXX&password=XXXXXXXX&**SubmitCreds=Log+On
2013-05-28 13:46:29 10.20.30.40 **username=XXXXXXXX&password=XXXXXXXX&**SubmitCreds=Log+On

WYNIKI TESTÓW – OWASP TOP 10







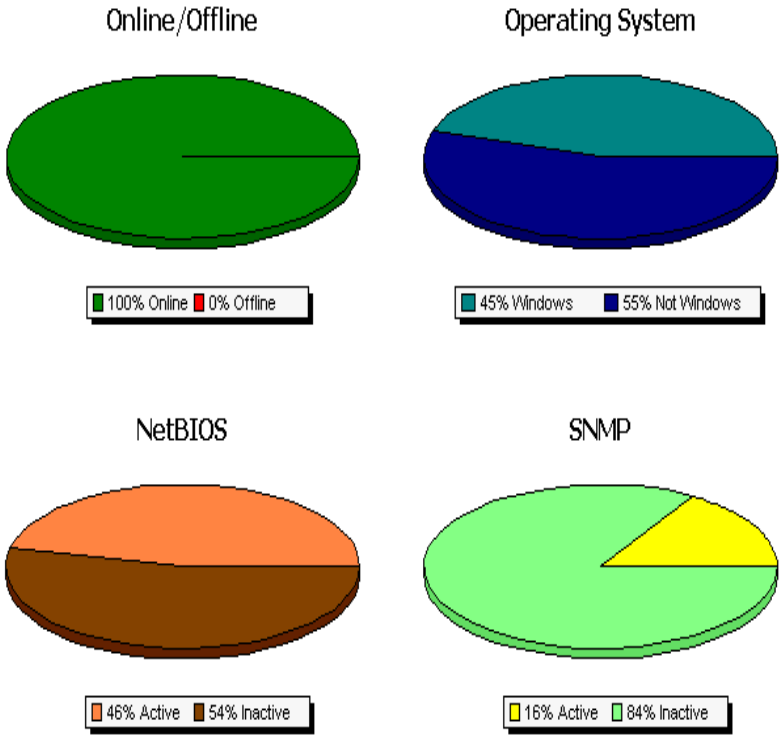
WYNIKI TESTÓW - SKANOWANIE

- Skanowanie nmap
- Ponad 20 otwartych portów TCP/UDP

Scanning xxxxxxxxx.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

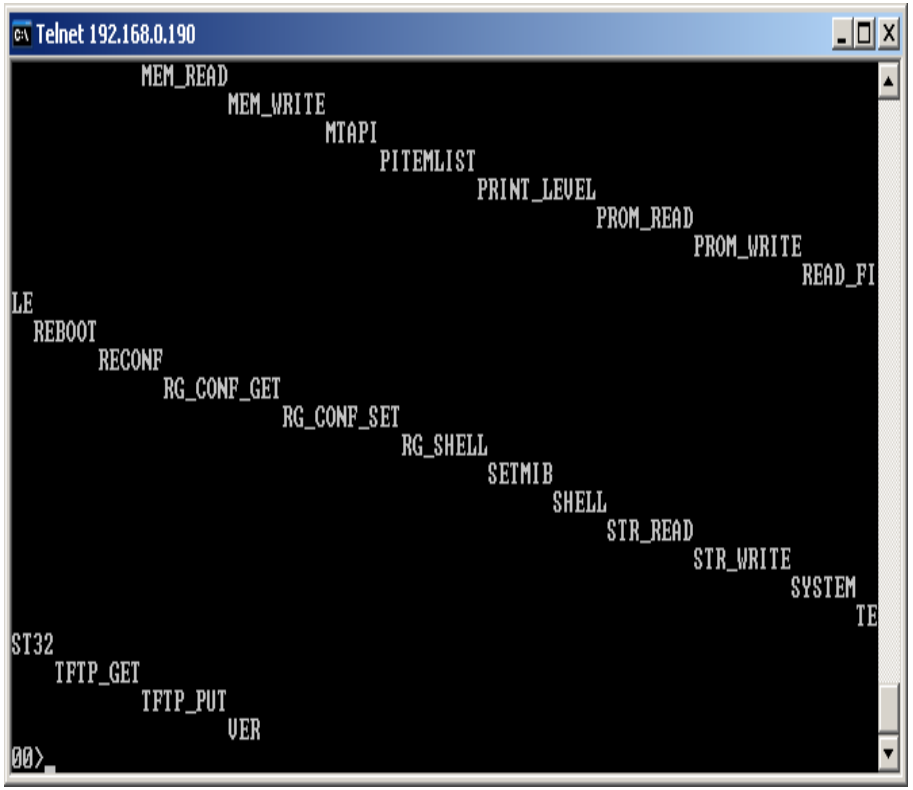
Scan Ranges	
FROM IP	TO IP
192.168.0.1	192.168.255.254



WYNIKI TESTÓW – OTWARTE PORTY

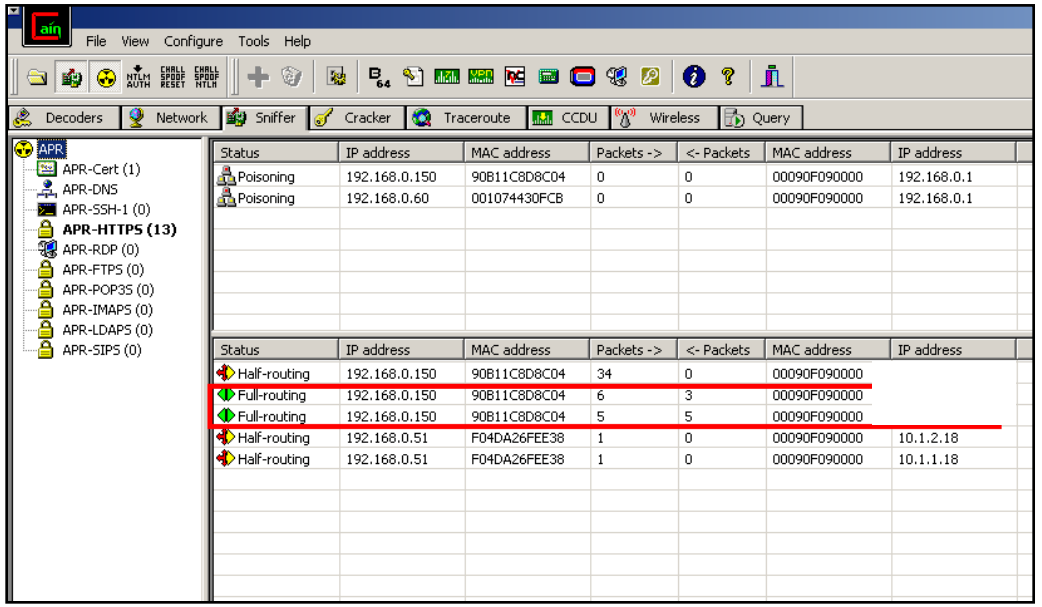
- AP WAP610N
- Otwarty port 1111
- telnet xx.xx.xx.xx 1111

> system cat /etc/shadow
root:1ZAwqf2dI$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:::*

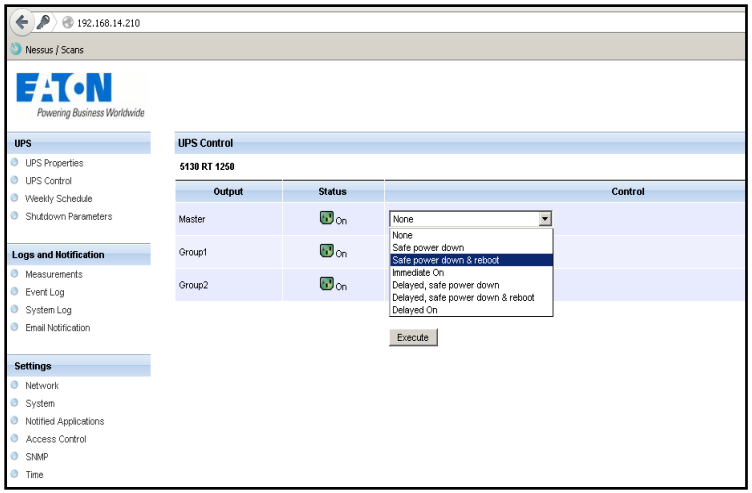


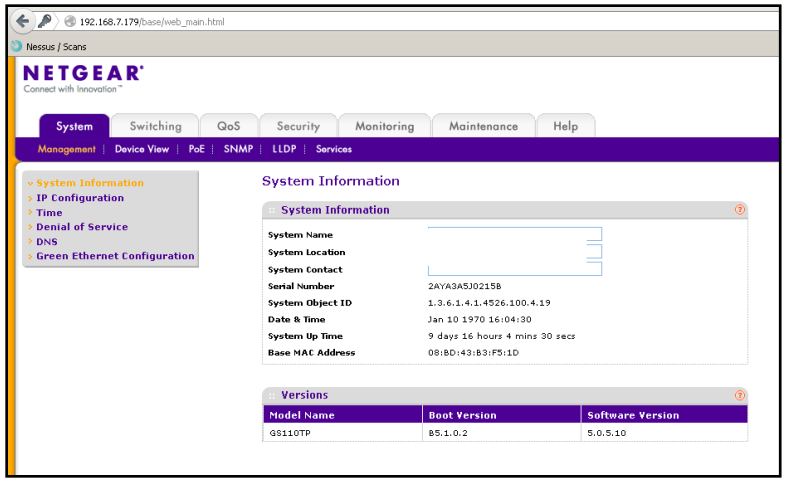
WYNIKI TESTÓW - MITM

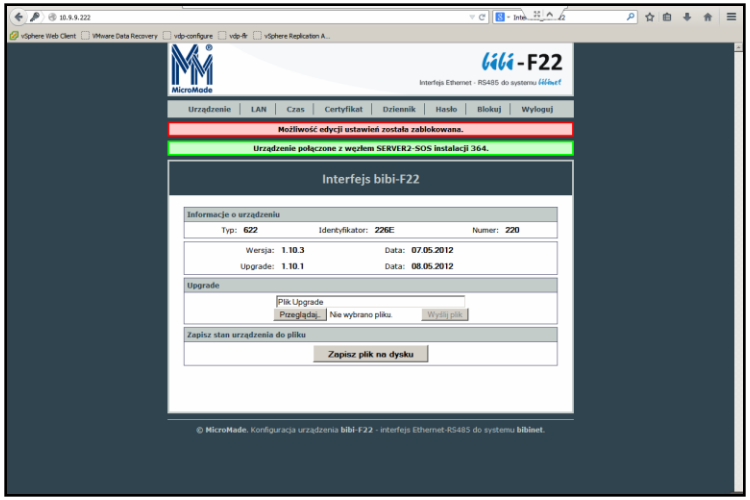
- Udane zatrucie tablicy ARP
- Umożliwienie ataku MITM
- Podsłuchanie 13 sesji HTTP
- Przechwycenie loginów i haseł do usług sieciowych

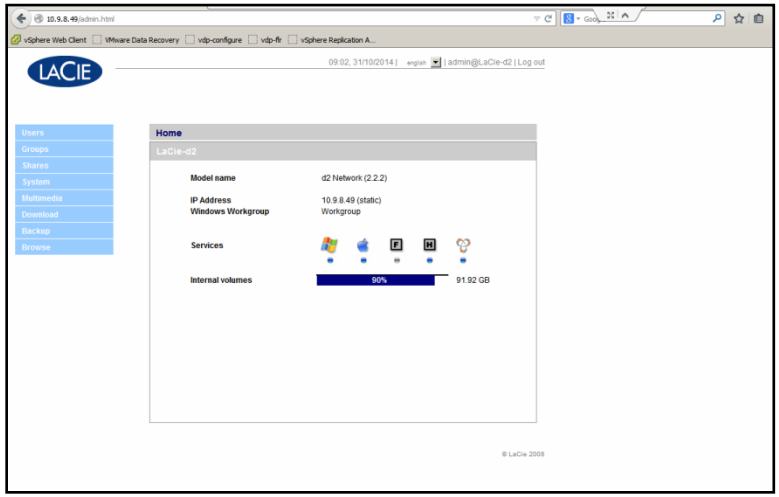


WYNIKI TESTÓW – ADMIN: ADMIN

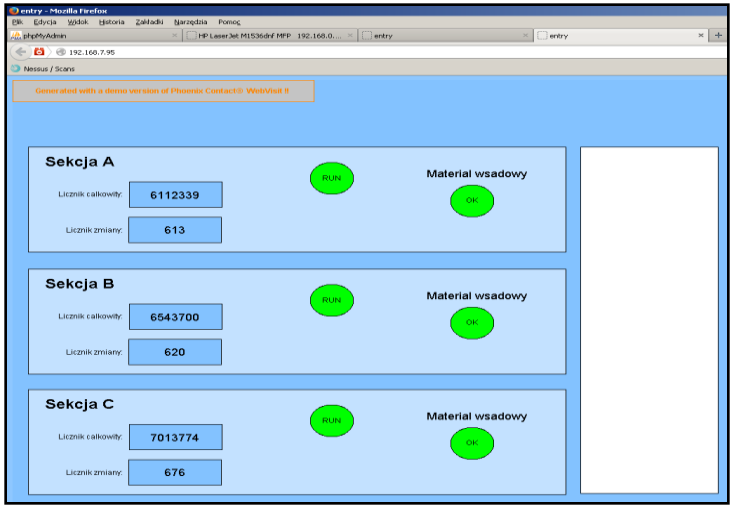


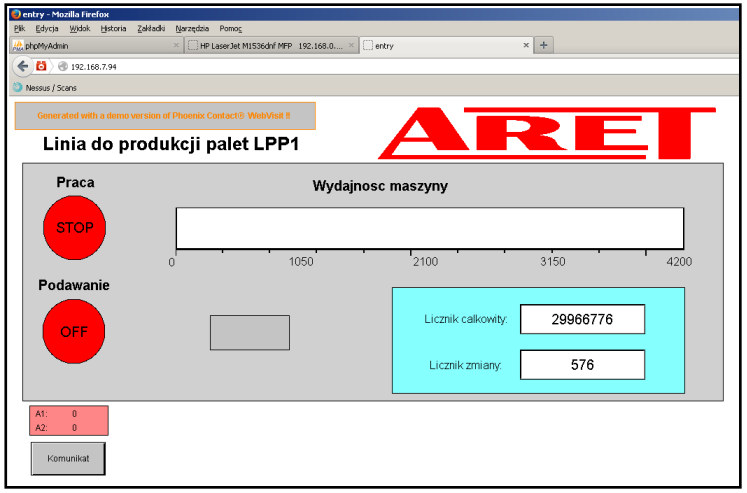


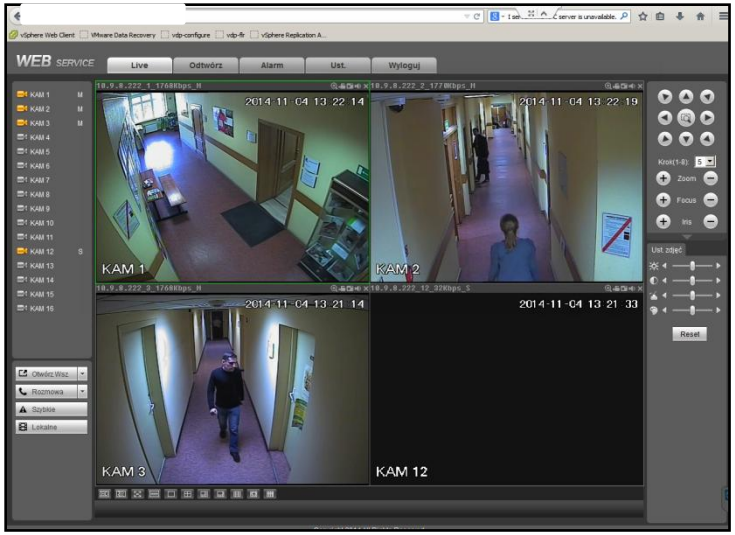


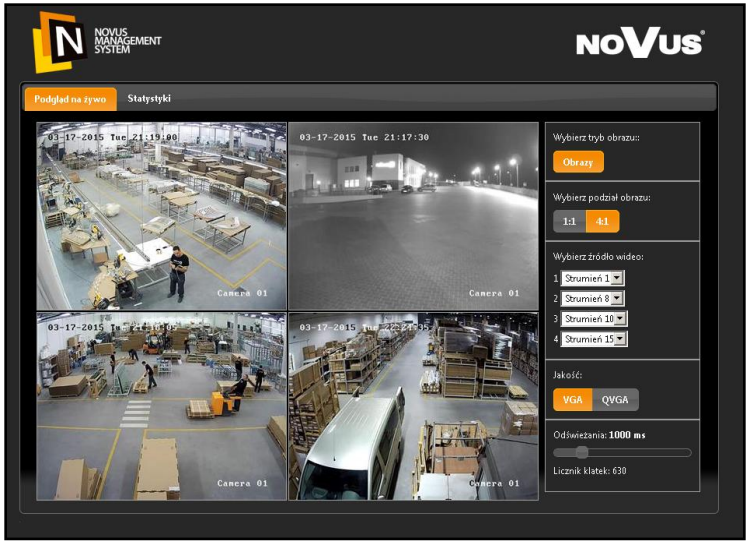


WYNIKI TESTÓW – ADMIN: ADMIN



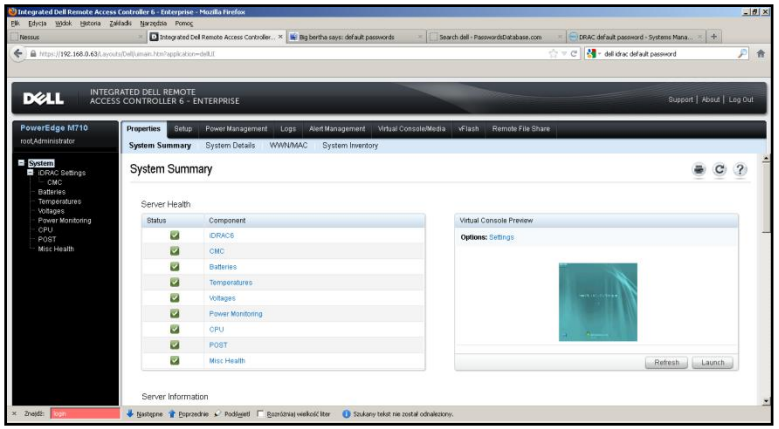


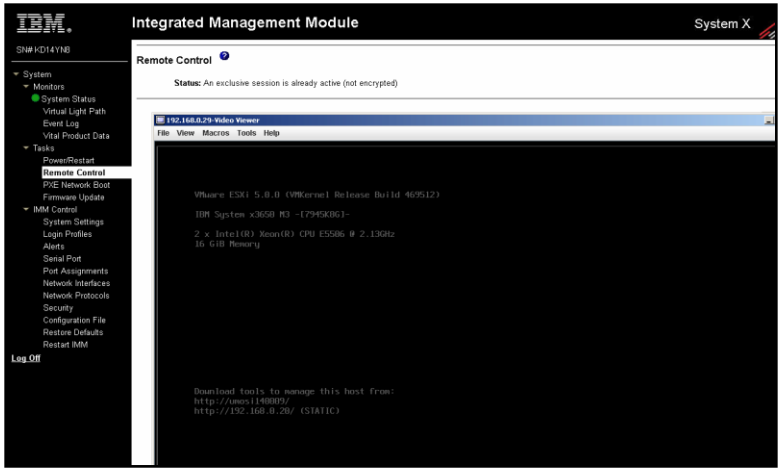




WYNIKI TESTÓW – SERVER REMOT CONTROL

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





WYNIKI TESTÓW – CENTRALA TELEFONICZNA

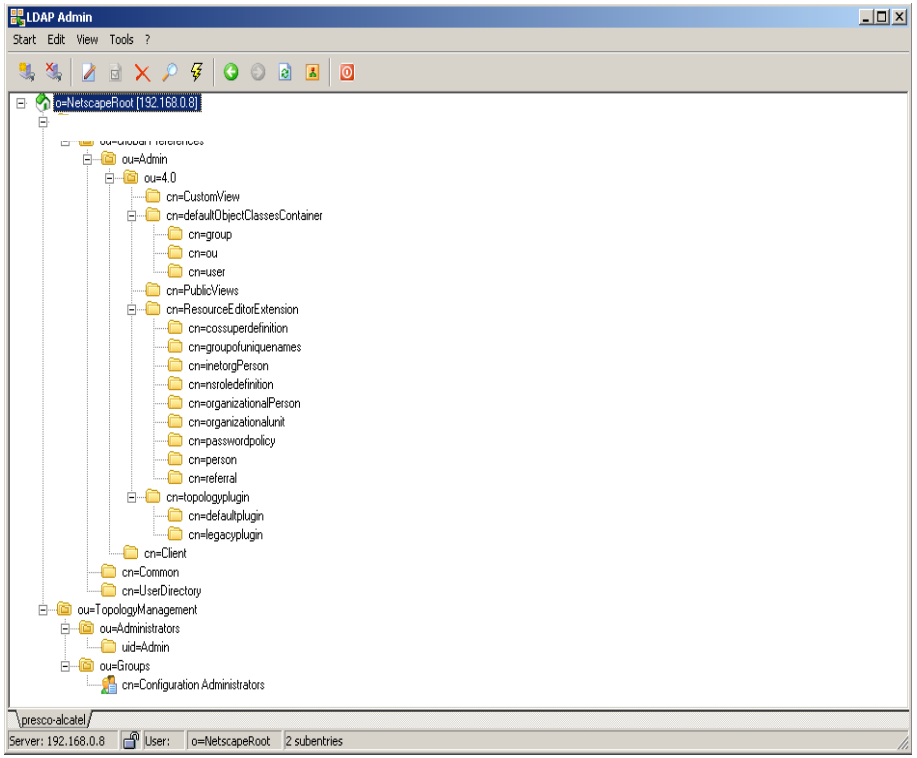
- Centrala telefoniczna Alcatel Omni PCX
- Wyłączony interfejs WEB ale w źródle strony HTML:

*<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.

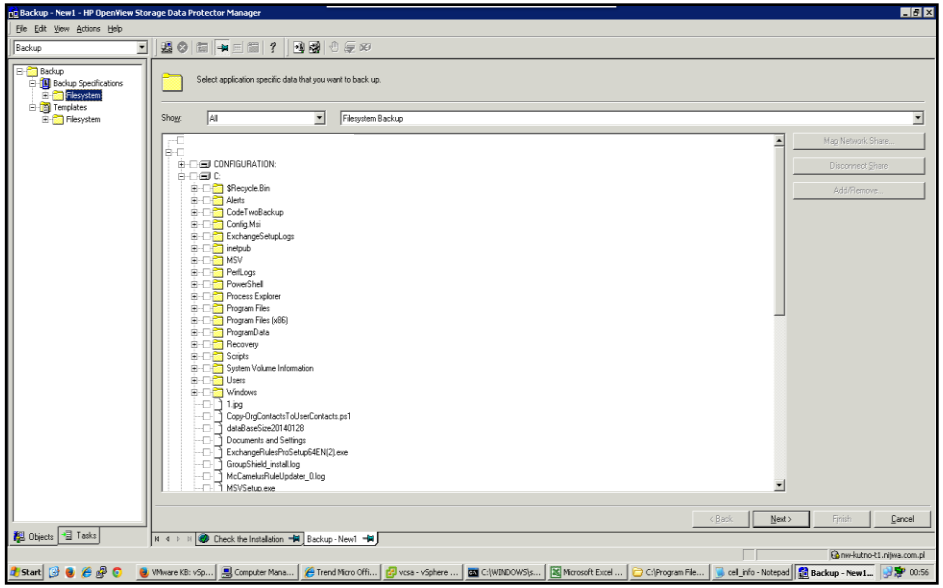
- Połączenie klientem LdapAdmin na dane ze źródła strony WWW
- Dostęp do zasobów usługi katalogowej, a w nich:

LDAP_o-nmc.ldif:**serverpassword: {NMC}cOskEilk**
LDAP_o-nmc.ldif:**swinstpassword: {NMC}OcsEskdi**



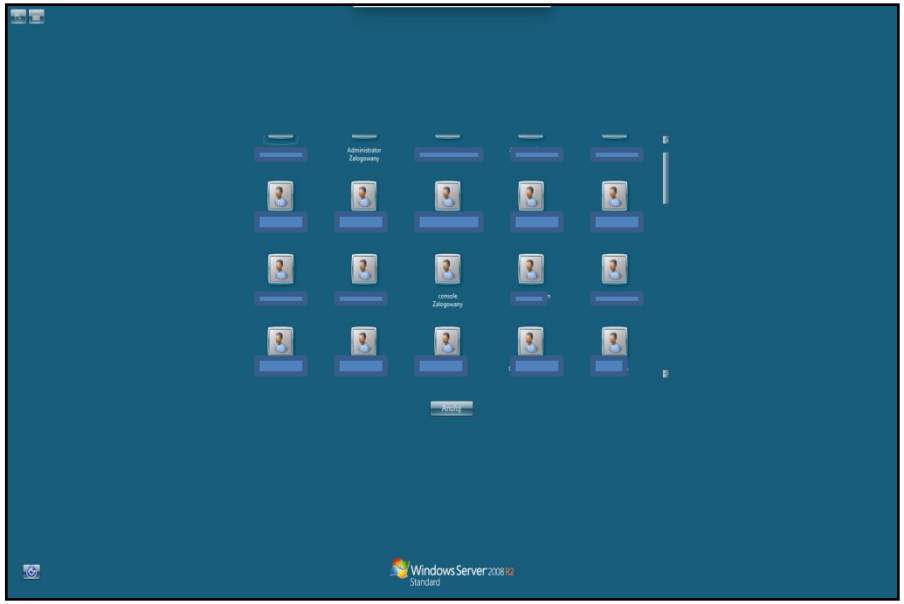
WYNIKI TESTÓW – BACKUP DO CHMURY

- 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

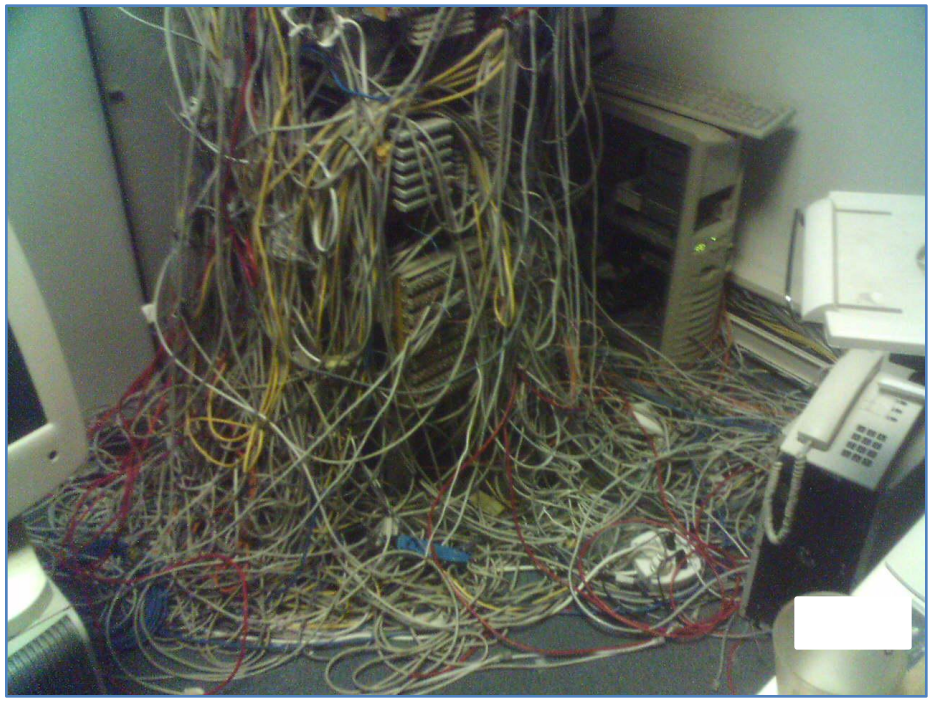


WYNIKI TESTÓW – ZNALEZIONE „FANTY”

- 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

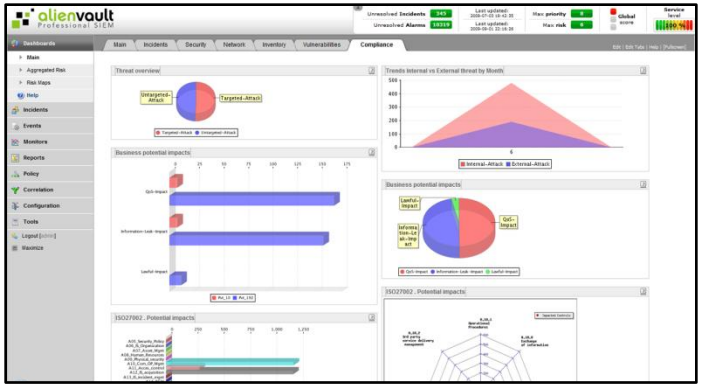
SOC – OUTSOURCING

- 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 systemy wymagane do realizacji zadań SOC

- Zalety outsourcingu
  Większe zaplecze kadrowe z własnymi narzędziami. Doświadczenie, spojrzenie z szerszej perspektywy.



UpGreat
we know-how to do IT

Dziękuję za uwagę

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

Jakub Staśkiewicz
UpGreat Systemy Komputerowe Sp. z o.o.

Dziękuję za uwagę

Jakub Staśkiewicz
tel.: 667 768 452
mail: jakub.staskiewicz@upgreat.pl

UpGreat Systemy Komputerowe Sp. z o.o.
60-122 Poznań, ul. Ostrobramska 22
http://www.upgreat.com.pl