Zagrożenia

Marcin Szeliga
marcin@wss.pl

Agenda

- Techniki wyszukiwania i rozpoznawania celów
- Podsłuchiwanie i modyfikowanie przesyłanych danych
- Włamanie i przejęcie kontroli
- Ukrycie ataku
- Podsumowanie

Atak

- **Wymierzony**
  - Atak wycelowany w konkretną organizację
- **Automatyczny**
  - Atak rozproszony, przypadkowe ofiary
  - Wirusy, robaki, spyware, pasożyty (Storm Worm)
- **Wewnętrzny**
  - Przypadkowe lub świadome naruszenie zasad bezpieczeństwa przez administratorów, pracowników, partnerów lub klientów
- **Zewnętrzny**

Zagrożenia

- Footprinting
- Scanning
- Enumeration
- Intelligence Gathering
- Sniffing
- Gaining Access
- Privilege Escalation
- Buffer Overflows
- Shovel a Shell
- Interactive Control
- Camouflaging
- Island Hopping
- Denial of Service
- Social Engineering

Zbieranie informacji: Footprinting

- **Definicja:**
  - **Atakujący używa narzędzi umożliwiających stworzenie profilu informacyjnego ofiary (organizacji lub osoby)**
  - Narzędzia:

http://www.google.com	Netcraft – http://www.netcraft.com
USENET http://groups.google.com	EDGAR - http://www.sec.gov
DNS Servers	TRACERT
WHOIS – http://www.arin.net & http://www.samspade.org	

Techniki przeciwdziałania

- **Ochrona informacji**
- **Maskowanie**
  - administrator@firma.foo, helpdesk@firmo.foo
  - Prywatne konto na publicznych grupach dyskusyjnych

Zbieranie informacji: Scanning

- **Definicja:**
  - Atakujący używa zestawu narzędzi umożliwiających uzyskanie listy otwartych portów, protokołów itp.
  - Narzędzia:

fping (ICMP-based)	**nmap (TCP-port-based)**
netcat	**SuperScan / Scanline**
Typhon II	**LANGuard**
Fluxay	**…**

Zbieranie informacji: Enumeration

- Definicja:
  - Atakujący używa narzędzi umożliwiających uzyskanie dokładnych informacji na temat systemów ofiary takich jak uruchomione serwisy, współdzielone zasoby, konta użytkowników ,grup, informacje o domenie, polisie itp.
- Narzędzia:
  - LANGuard
  - N-Stealth
  - Fluxay
  - Nessus

Techniki przeciwdziałania

- **Kontrolowanie dostępu do sieci**
  - Zapora, strefa zdemilitaryzowana
  - Zabezpieczenie punktów dostępowych (RADIUS)
- **Aktualizacja oprogramowania (Hotfixy)**
- **Bezpieczna konfiguracja (RestrictAnonymous=2)**
- **Blokada wszystkich nieużywanych portów (TCP 139 , UDP 137)**
- **Wyłączenie NetBIOS**
- **IPSec**
- **Zmiana etykiet**

Zbieranie informacji: Intelligence Gathering

- Przykłady:
  - Sniffing , Keystroke Logging, Ataki typu „Man In The Middle”
- Narzędzia:

Network Monitors	Distribution List ‘taps’
DSniff	FakeGINA
ScoopLM	LC3 SMB Capture
BeatLM	SMBProxy, SMBRelay2

Zbieranie informacji: Sniffing

- Definicja:
  - Przechwytywanie, ewentualne analizowanie i modyfikowanie przesyłanych w sieciach danych
- Narzędzia:

WireShark	EtterCap
TCPDump	Snort, AirSnort
SniffIt	Dsniff
Aircrack	AirMagnet Laptop Analyzer

Techniki przeciwdziałania

- **Kontrolowanie dostępu do sieci**
- **IPSec, SSL/TLS**
- **Sieciowe systemy wykrywania włamań**
- **Zabezpieczenie sieci Wi-Fl**
  - Rozgłaszanie SSID
  - Filtrowanie MAC
  - WPA(2) vs WEP
- **PKI (Infrastruktura klucza publicznego)**

Atak: Port Redirection

- Definicja:
  - Zestaw narzędzi umożliwiających stworzenie przekierowania pakietów danych z portu przeznaczenia do innego portu oraz hosta
- Tools:
  - FPipe.exe
  - RINETD(8)

Demonstracja, przekierowanie portów

Local Machine <----------> FPipe server <---------> Remote machine

Inbound connection

Outbound connection

fpipe -l 53 -s 53 -r 80 192.168.1.101

Techniki przeciwdziałania

- Aktualizacja oprogramowania (Hotfixy)
- Zabezpieczenie usług sieciowych (IIS)
- Kształtowanie ruchu w sieci lokalnej
- IPSec

Atak: Gaining Access

- Definicja:
  - Atakujący używa narzędzi umożliwiających bezpośredni dostęp do systemu często poprzez złamanie hasła
- Narzędzia:

Keystroke Loggers	L0phtcrack
Password Grinders	Remote Shells
John the Ripper	Getadmin
GetAdmin2	Brutus
Samdump	Pwdump

Techniki przeciwdziałania

- **Zapewnienie fizycznego bezpieczeństwa**
- **Bezpieczne przechowywanie danych uwierzytelniających**
  - Sygnatury vs kryptogramy
  - Syskey w trybie 2 i 3
- **Bezpieczne hasła (najlepiej 15 znaków, ze znakami nie alfanumerycznymi, np.ALT+)**
- **Zasada minimalnych uprawnień**
- **Szyfrowanie danych**

Atak: Privilege Escalation

- **Definicja:**
  - Atakujący zwiększa zwoje uprawnienia np.z roli ‘user’ do ‘administrator’
  - Tools:

GetAdmin, GetAdmin2	**PipeUpAdmin**
DebPloit	**L0phtcrack (LC3/LC4)**
John the Ripper	**Brutus**
Samdump	**Pwdump1,2,3,3e**
LSADump, LSADump2	

Techniki przeciwdziałania

- Aktualizacja oprogramowania (Hotfixy)
- Skaner antywirusowy
- Zasady ograniczeń oprogramowania
- Uruchamianie programów z ograniczonymi uprawnieniami
- Odebranie przywileju Debug Processes grupie Administrators
- Monitorowanie wszystkich operacji przeprowadzanych przez uprzywilejowanych użytkowników

Atak: Buffer Overflows

- Definicja:
  - Przepełnienie bufora polega nad nadpisaniu segmentu pamięci ponad oczekiwaną wartość dzięki czemu możliwe jest skok do dowolnego miejsca pamięci oraz wykonanie dowolnego kodu napastnika na uprzywilejowanych prawach
- Narzędzia:

JILL-WIN32.EXE	ISPC.EXE
IIS5hack.exe	HTTPODBC.DLL
Unicodeloader.pl	SQL buffer overflows

Techniki przeciwdziałania

- **Aktualizacja oprogramowania (Hotfixy)**
- **Uruchamianie tylko zaufanego oprogramowania**
  - Uwaga na działające w trybie jądra sterowniki
- **Zapobieganie wykonywaniu danych (DEP)**
- **Wyłączenie nieużywanych usług**
- **Zablokowanie nieużywanych protokołów oraz portów**
- **Systemy IDS**

Atak: Shovel a Shell

- Definicja:
  - Atakujący używa narzędzi umożliwiających uzyskanie zdalnej konsoli na maszynie ofiary
- Tools:
  - Netcat – „Hacker's swiss army knife"
  - PSExec.exe

Techniki przeciwdziałania

- Aktualizacja oprogramowania (Hotfixy)
- IPSec (blokowanie komunikacji)
- Zapora sieciowa
- Zasady ograniczeń oprogramowania

Atak: Interactive Control

- Definicja:
  - Atakujący używa narzędzi do zdalnej administracji maszyną ofiary
- Narzędzia:

Remote.exe	rclient
netcat	Virtual Network Computing (VNC)
Dameware Mini Remote Control	Terminal Services
Sub7	Back Orifice 2000
NT Rootkit	MMC

Techniki przeciwdziałania

- Programy antywirusowe
- IPSec (blokowanie komunikacji)
- Zapora sieciowa
- Zasady ograniczeń oprogramowania
- Monitorowanie nietypowej aktywności użytkowników

Ukrycie: Camouflaging

- Definicja:
  - Atakujący używa narzędzi ukrywających jego działalność
- Narzędzia:

WinZapper	Elsave
Event Log GUI	NT Rootkit
Loki/ Mimic	Rwwwshell
CryptCat	AckCMD

Techniki przeciwdziałania

- Sprawdzenie systemu off-line
- Sprawdzenie autentyczności plików
- Restrykcyjne listy ACL
- IDS (zmiana plików systemowych, otwarte nietypowe porty)
- Zabezpieczenie dzienników zdarzeń
- Monitorowanie nietypowego ruchu w sieci

Atak: Island Hopping

- Definicja:
  - Wykorzystanie przejętych systemów do zaatakowania kolejnych celów
  - W jednorodnym środowisku BARDZO proste i szybkie
- Tools:

netcat	Tftp
Fpipe	SMB Relay
Hash ‘cramming’	

Atak: Denial of Service

- Definicja:
  - Celem atakującego jest uniemożliwienie poprawnej pracy systemu
- Tools:
  - TFN2k
  - Stacheldraht
  - mIRC

Z innej beczki: Social Engineering

- Definicja:
  - Techniki zdobycia od uprawnionych osób niejawnych informacji
- Narzędzia:
  - Telephone
  - Voice Mail
  - Email
  - USENET
  - Temporary Employment
  - Enticing downloads

Podsumowanie

- **Wybór celu**
  Sam Spade / WHOIS / ARIN / USENET postings
- **Rozpoznanie**
  Languard / Dumpsec / Typhon / enum / Nesus / Fluxay / Nmap / Fport / Superscan / NAT / Whisker / Stealth
- **Zdobycie zdalnego dostępu**
  Netcat / cryptcat / JILL-WIN32 / psexec / IIS5Hack / UnicodeLoader.pl / SQLDict
- **Wgranie narzędzi**
  Misc. hacking tools used to escalate privileges, scan, cover tracks, pillage & plunder
- **Poszerzenie uprawnień**
  Pipeupadmin / Debploit
- **Zdobycie haseł**
  Pwdump3,3e / ScoopLM / SMBProxy / DSniff / LC3 / John the Ripper / CHNTPW
- **Zestawienie zdalnego połączenia**
  Loki / Mimic
- **Otwarcie „tylnej furtki”**
  Sub7, BO2k, Netbus
- **Ukrycie śladów**
  ELsave / WinZapper
- **Zniszczenie**
  Steal sensitive data
- **Albo zablokowanie systemu**
  Stacheldrat, Trinoo, TFN2k

Podsumowanie

- Mamy mnóstwo (technologicznych) zabezpieczeń:
  - Zapory
  - Programy antywirusowe
  - Systemy wykrywania włamań …
- Ale nie jesteśmy bezpieczni