Wykład 7

Temat: Hakerzy, wirusy i inne niebezpieczeństwa

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Kto to jest haker?

haker, hacker [wym. haker] «osoba włamująca się do sieci i systemów komputerowych»

Ale mamy także:
cracker [wym. kraker], kraker
1. «osoba włamująca się do systemów komputerowych w celu kradzieży lub niszczenia danych»
2. «osoba łamiąca zabezpieczenia programów komputerowych»

Oraz największą grupę:
script kiddie
Osoby posługujące się w atakach skryptami lub programami wytworzonymi przez innych. Zazwyczaj posiadają znikomą wiedzę z zakresu bezpieczeństwa oraz programowania. Jest to określenie pejoratywne.

Projekt „*Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe*”
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

Wirusy a systemy z rodziny Unix

Ze słownika języka polskiego: **wirus**

1. «organizm żywy znacznie mniejszy od bakterii, rozmnażający się tylko w żywych komórkach, wywołujący choroby»
2. «program komputerowy, który bez wiedzy i wbrew woli użytkownika przedostaje się do systemu komputerowego, zmieniając lub niszcząc informacje w nim przechowywane»

- definicja mało aktualna
- wirus ukrywa swoją obecność w systemie
- pozwala na zdalną kontrolę nad naszym komputerem/serwerem
- na systemy z rodziny Unix też są wirusy (rootkity)
- każdy wirus rozprzestrzenia się wykorzystując podatności (exploit)
- można je wykryć poprzez analizę zachowania procesów lub kodu programu

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Metody poszukiwania podatności w aplikacji

- sprawdzenie w Metasploit, czy ktoś już znalazł podatność za nas :)
- analiza kodu źródłowego aplikacji (jeśli jest dostępny)
- deasemblacja plików binarnych
- sprawdzenie popularnych podatności oraz fuzzing
- analiza ruchu sieciowego aplikacji

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Czego szukamy?

Naruszenia ochrony pamięci:

- Buffer overflows
- Dangling pointers

Brak walidacji danych wejściowych:

- Format string attacks
- SQL injection
- Code injection
- Directory traversal
- Cross-site scripting
- HTTP header injection

Wyścigi krytyczne:

- Time-of-check-to-time-of-use

Błędna kontrola uprawnień:

- Cross-site request forgery
- Clickjacking
- Privilege escalation

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przykład podstawowego skanowania systemu


```
# nmap -A -T4 scanme.nmap.org

Starting Nmap 6.46 ( http://nmap.org ) at 2015-02-22
14:07 CET
Nmap scan report for scanme.nmap.org
(74.207.244.221)
Host is up (0.20s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 5.3p1 Debian
3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd
(DSA)
|_  2048
79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
43/tcp   filtered whois
53/tcp   filtered domain
80/tcp   open     http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
9929/tcp open     nping-echo   Nping echo
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X (96%), Fortinet
Linux 2.6.X (86%), IPFire Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
cpe:/o:linux:linux_kernel:3 cpe:/o:fortinet:linux_kernel:2.6
cpe:/o:ipfire:linux:2.6.32
Aggressive OS guesses: Linux 2.6.32 - 2.6.39 (96%), Linux
2.6.32 - 2.6.35 (92%), Linux 2.6.38 (92%), Linux 2.6.30 (91%),
Linux 2.6.39 (91%), Linux 2.6.32 - 3.0 (91%), Linux 3.2 - 3.6
(90%), Linux 3.4 (89%), Linux 2.6.32 (89%), Linux 2.6.32 -
2.6.33 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt „*Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe*”
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY