DCIT

Hackerem snadno a rychle aneb nebezpeční script-kiddies

Autor: Martin Mačok

DCIT, s.r.o. - Praha, http://www.dcit.cz/

Obsah

DCIT

Úvod, terminologie
Scénář útoku
Metasploit Framework
Ukázka použití exploitu

Motto:

- Zneužít technologicky komplikovanou slabinu k získání kontroly nad serverem nemusí být vůbec složité

Slabina

DCIT

Slabinou rozumíme chybu v programu, kterou lze zneužít k nežádoucí činnosti, jako například

- získání kontroly nad programem
- získání kontroly nad operačním systémem
- získání přístupu k citlivým informacím
- vyřazení programu či celého systému z provozu

Pozorování: každý program obsahuje chyby, z velké části zneužitelné

- buffer overflow, integer overflow, format string, …

3

Exploit

DCIT

Exploit je program, který automatizuje zneužití slabiny v jiném programu.

Obvykle dostupný ve formě

- zdrojového kódu (C/C++, Perl, Shell) nebo
- binárního kódu (EXE, COM)
- privátní nebo veřejně dostupný
- testovací verze (Proof of Concept) nebo
- ostrá verze (Full), příp. s defektem

Exploity mají i legitimní použití

4

Script-kiddie

DCIT

Uživatel disponující funkčními exploity, které umí použít, aniž rozumí jejich činnosti.

Exploity lze získat

- google (exploit filetype:c)
- archív konference Bugtraq a Full-Disclosure
- volně dostupné: ExploitTree, Metasploit Framework
- komerční: Core Impact, Canvas, Retina, (Nessus)

Pozor na trojské koně!

Scénář útoku

DCIT

Zaměstnanec firmy

- zjistí verzi OS a provozovaného software
- (zjistí potenciální slabinu)
- najde odpovídající exploit a zkusí jej použít
- opakuje předchozí kroky, dokud neuspěje

V případě úspěchu může získat plnou kontrolu nad serverem a uloženými daty

Typický exploit

DCIT

- zpracuje uživatelský vstup (parametry)
- vyrobí zlomyslný kód (payload, shellcode)
- sestaví vhodně *poškozený* vstup (žádost)
- naváže síťové spojení
- zašle poškozený vstup (na serveru je spuštěn payload)
- (obslouží následnou interakci útočníka s obětí)

Pozorování: různé exploity mají mnoho společného

7

Metasploit Framework

DCIT

Prostředí pro komfortní tvorbu a použití exploitů

- http://metasploit.com/
- obsahuje všechny potřebné komponenty
- množství payloadů pro různé platformy
- aktualizovaná databáze funkčních exploitů
- jednoduché textové příp. webové rozhraní
- interaktivní nápověda

- multiplatformní (Perl, příp. Python)
- volně dostupný (GPL, Artistic License)

8

Metasploit - schéma použití

DCIT

1. Spuštění konzole Metasploitu
2. Volba exploitu
3. Volba payloadu
4. Volba cíle
5. (Volba parametrů exploitu a payloadu)
6. Spuštění exploitu

...

Metasploit - návod k použití

DCIT

```
$ msfconsole
> use <exploit>
> set PAYLOAD <payload>
> set RHOST <pocitac>
> show options
> set ...
> exploit
```


Demonstrace

DCIT

Praktická ukázka zneužití dvou slabin

Cíl: Microsoft Windows 2000 SP4 Advanced Server - v našem příkladě ve funkci doménového kontroleru

Slabiny

- LSASS (MS04-011)
- WINS (MS04-046)