



Privilegijų pasikėlimas sistemoje

By Gintar Sakas



Privilege escalation

Windows:

- ❑ Guest->administrator
- ❑ Guest->user
- ❑ User->administrator
- ❑ Administrator->LocalSystem
- ❑ LocalSystem->Kernel mode

Unix:

- ❑ Nobody->User
- ❑ Nobody->root
- ❑ nobody privilegijų išnaudojimas



Langai ir pingvinai

Privilegijų kėlimasis Windows ir Unix sistemose panašus:

❑ Exploit'ai

- 1) <http://www.milw0rm.com/>
- 2) <http://www.exploit-db.com/>
- 3) <http://www.metasploit.com/>

❑ Rootkit'ai

- 1) <http://packetstormsecurity.org/UNIX/penetration/rootkits/> (Unix)

❑ Buffer overflow



Hack'as langinėse (Guest/user->administrator)

- ❑ **SAM ir SYSTEM registro laužimas (Proactive Password Auditor)**

SAM šifruojamas NTLM, silpnoji grandis LM hash'as:

- 1) ACSII simboliai pakeičiami didžiaisiais
- 2) Reikšmė skaldoma po 7 ACSII simbolius

- ❑ **DreamPackPL:**

- 1) Įrankis apeinantis Win 2000/XP admin slaptažodį
- 2) <http://depositfiles.com/ru/files/395974>



Attack type: Brute-force Mask Dictionary Rainbow

Hashes Bruteforce attack

Bruteforce attack options

All Latin (A-Z) All Printable Password length: min max
 All Digits (0-9) Custom charset Passwords ranges:
 Special (!@...)

User name	User ID	Computer	Hash type	Password	Audit time	Status	Description
<input type="checkbox"/> ASPNET	1005		LM+NTLM	???????????????			Account
<input type="checkbox"/> Administrator	500		LM+NTLM	SHEFAS	7 min 40 sec		Built-in ac
<input type="checkbox"/> Guest	501			<empty>		Account is disabled	Built-in ac
<input type="checkbox"/> HelpAssistant	1000		LM+NTLM	???????????????		Account is disabled	Account
<input type="checkbox"/> SUPPORT_3...	1002		NTLM	???????		Account is disabled	This is a
<input type="checkbox"/> egzaminas	1007		LM+NTLM	egzaminas	0 sec	Account is disabled	egzaminu
<input type="checkbox"/> svecias	1006		LM+NTLM	svecias	0 sec	Account is disabled	

Timestamp	Message
12.03.2009 13:36:03	Current user has administrator rights
12.03.2009 13:36:03	Current user has privilege to debug programs
12.03.2009 13:39:27	Loading project from file [Redacted]...
12.03.2009 13:39:27	Project file successfully loaded.



Hack'as langinėse (Administrator->LocalSystem)

- ❑ **Logon screensaver teisių išnaudojimas:**

LocalSystem, jei Win<NT 5.0

LocalService, jei Win>=NT 5.0

- ❑ **Shedule tasks:**

At TIME /option (Interactive) "cmd.exe"

Išbandyta ant Win Server 2003 SP2



Kernel mode??

- ❑ 32bit'ų Intel procesorius turi keturis saugumo lygmenis
- ❑ Windows naudoja tik du (ring0 ir ring3)
- ❑ VISOS programos, dauguma virusų ir pan. – ring3
- ❑ Windows kernel'is – ring0

Kernel mode (ring0) – Dievo režimas



Hack'as langinėse (LocalSystem->kernel mode)

- ❑ Oficialus būdas: Tvarkyklės

Blogai, nes yra sunkios

- ❑ Hack būdas: CPU lentelių perrašymas

Gerai, nes užima nedaug kodo

Naudoja virusai/trojanai

Veikimas – specialaus “šliužo” įrašymas į vieną iš CPU sisteminių lentelių

Reikalingas priėjimas prie \Device\PhysicalMemory

- 1) Pvz.: phide (<http://vx.netlux.org/vx.php?id=ep12>)



Žaidimas Unix sistemose

- ❑ WEB hacking – Apache teisės sistemoje
 - ❑ Populiariausi metodai: Buffer overflow, exploits
 - ❑ Dažnai pasitaiko neteisingas privilegijų paskirstymas sistemoje
 - ❑ Nobody – tai jau šis tas! (Pvz. Proxy serveris)
- 1) <http://www.3proxy.ru/download/>



Ačiū už dēmesī

Klausimai?