Exploring Terminal Services

or, The Evil Admin and His Tools

Ian Vitek
Patrik Karlsson

FIRST WORDS

The new tools and this presentation will be available for download at:

http://www.cqure.net/itools02.html

Exploring Terminal Services

- Exploring
- Uploading Files
- Gain SYSTEM
- Controlling Users and Their Local Network

EXPLORING

Looking around:

- Netstat -na
- ARP
- Net
  - User
  - View
  - Session

EXPLORING

Authentication/Password guessing:

- Net Use
- Telnet
- Ftp
- VNC
- TS
- Citrix

EXPLORING

VBS:

- Excel Port Scanner (Hedgehog)
- User Switching (Wolfy,No release)
- Unlimited?

EXPLORING

Other:

- Progman.exe (explorer on w2k3)
- Compmgmt.msc
- Rundll32.exe
  - netplwiz.dll,AddNetPlaceRunDll
  - url.dll,TelnetProtocolHandler IP Port
  - More...

Uploading Files

Common ways:

- Normal TS or Citrix client map
- Normal HTTP or FTP transfer

UPLOADING FILES

Convert BIN to text file with NETSEND.EXE and upload the file with COPY and PASTE.

NETSEND.EXE transforms the file to 16-bit application (only readable characters) or uuencodes it.

MUUD.COM is a uudecoder (only readable characters)

UPLOADING FILES

If all fails; Upload files with keyboard.

Copywk.pl (Demo) copies files with keyboard to target window.

Can also transform files to DEBUG scripts (no size limit).

GAIN SYSTEM

Some examples:

- Replace SYSTEM binaries
  - File rights
  - No fully qualified path, .*.DLL
- Spawning processes from SYSTEM processes (Demo)
- Install a network printer with a trojan driver
  (No release)

CONTROLLING USERS

- Normal trickery. E.g. Login script
- Steal Citrix users disks (Demo)
- Steal credentials and spawn a reverse shell (Demo)
- Mount and access the users (local) network drives (Demo)

CONTROLLING USERS

Steal Citrix users disks:

- Winobj from Sysinternals
  - \Device\CmdRedirector\X:\1\C:
  - Administrators can access all DosDevices
  - Easy to enumerate drives and map
- Citrixmap.exe from Cqure
- Patch is available

CONTROLLING USERS

Steal credentials:

- Copy credentials as administrator
- Start new process with credentials; Reverse shell
- TSInject.exe from Cqure

Controlling Users

Mount and access client drives:

- Citrix
  - Net use * \\client\c$
- TS
  - Net use * \\tsclient\c
  - Can map clients mapped network drives

DEMO

- Breaking out from given environment
- Uploading files
- Gain SYSTEM
- Citrixmap.exe
- TSInject.exe
- Accessing client network drives on client LAN

PROTECTION?

Uploading files:

Normal TS/Citrix protection.

Disable 16-bit application support.

- Traffic filtering
- Restrict access to executables and script engines that can be used to upload binaries
- General RWX rights

PROTECTION?

Controlled execution:

- Active Directory
- Sanctuary www.securewave.com
- CIS www.se46.se (Not tested)

PROTECTION?

Gaining system:

- Fully qualified path problem
- Process isolation
- Validate access to critical API:s
  - Apiguard www.toolcrypt.org

PROTECTION?

Userland Apiguard:

- Calls to API:s must originate from the code segment of an already loaded module*
- Code injection most often use:
  - LoadLibraryA / LoadLibraryW
  - CreateProcessA / CreateProcessW
  - CreateThread, etc

  (Or native API representatives)

PROTECTION?

Kernel mode:

- Deny access to other process objects
- Deny access to thread objects outside of the current process

Exceptions? Antivirus?

Kernelguard will be released in autumn in Finland by yrg

THE END?

More?

- Alpha Wolfy.exe that switches sessions, like fast user switch
- Still no BO...

THANKS

Researcher:

Patrik Karlsson Cqure.net

Keeper:

Yrg Toolcrypt.org

Demo man:

Jonas Ländin Ixsecurity.com

Base defender:

Egil Mannerheim

EOF

The new tools and this presentation will be available for download at:

http://www.cqure.net/itools02.html

defcon-xii@sigtrap.org