Pillage the Village

Pilfering & Plundering for better Penetration Tests

Agenda

- Appetizer
  - Focus of the preso & State of the Onion
- Main Course
  - Network Plundering
  - File System & Memory Pilfering
  - Internet Pillaging
- Desert

Focus of the Presentation

- Lots of information out there on exploiting systems
  - Ready made exploits
  - Exploitation frameworks
    - Core Impact
    - Metasploit
  - Live CD's
    - Backtrack
    - Samurai
  - Great SANS courses: 504, 560, etc </shameless plug>
- Few focus on what to do during recon and exploitation, beyond recon and exploitation
  - Focus on tips and techniques to further the penetration of an organization

State of the Onion

- Current methodology
  - Recon
  - Scanning
  - Exploitation
  - Maintain Access
- Reality requires recursion
- Each new level of discovery adds potential new avenues of exploitation

Plunder ye Network

- Look for:
  - Recent communications
  - Common controller sites
  - VOIP traffic
  - Internet history
  - VLAN info
  - Routing info

Recent Communications

- Arp
  - *arp –a* or *arp –an*
  - Display known MAC addresses
- Netstat
  - *netstat –a* or *netstat –an*
  - Display current network connections

Recent Communications cont.

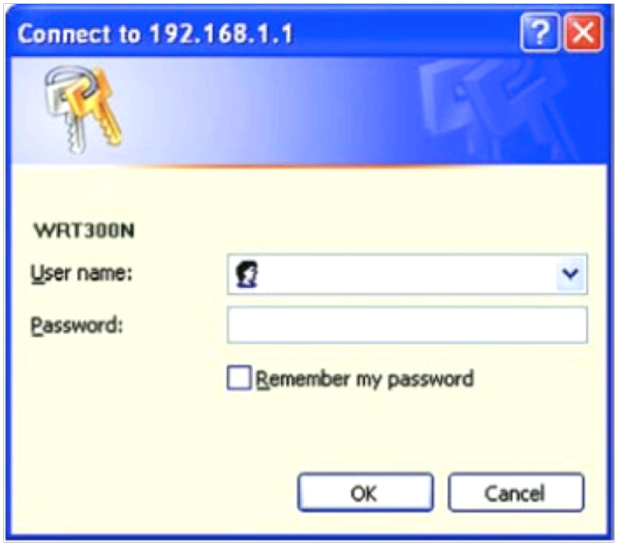
- ipconfig
  - *ipconfig /displaydns*
  - This will show all of the hosts cached dns records
  - Only work on Windows

Recent Communications

- Browser History
  - IE (Windows 2000 & XP)
    - C:\Documents and Settings\[username]\Local Settings\History
  - IE (Vista)
    - C:\Users\[username]\AppData\Local\Microsoft \Windows\Temporary Internet Files
  - Firefox
    - C:\Documents and Settings\[username]\Local Settings \Application Data\Mozilla\Firefox \Profiles[FF profile] \Cache

Common Controller Sites

- Login pages for Admin consoles
  - Default login to routers
  - Printers
  - Web consoles
- DNS entries that might lead
- to further penetration
  - Names like: test., vpn., *printer*, lab., beta.,etc



Run a Sniffer

- Run a sniffer!
  - Tcpdump is command line
    - Available for Linux and Windows
    - May already be installed
  - Ngrep is also command line
    - Very powerful regex engine
    - Search for usernames, passwords, etc
    - Available for Linux and Windows
- Once you have the packets, bring them back and go through them

Packets… what to look for

- Clear text protocols – look for logins
  - POP, IMAP, Telnet, HTTP, FTP, SMTP, IM and more
- VOIP traffic
  - H.323 uses ports 1719 & 1720 for signaling, dynamic for data
  - SIP uses port 5060 for signaling, dynamic for data
  - Bring packets back and run them through Wireshark or Cain & Abel

Packets … continued

- VLAN tags
  - Can tell you that you are vlan'ed
  - Gives you a starting point to try and hop
- Admin traffic
  - Traffic to/from admin consoles
  - SNMP, telnet, HTTP traffic
- Pull the routing table off the box
  - nestat –rn
  - Look closely for static routes to networks or boxes of interest

Pillage ye Filesystem

- Brower History
  - IE (Windows 2000 & XP)
    - C:\Documents and Settings\{USER}\Local Settings \History
  - IE (Vista)
    - C:\Users\[username]\AppData\Local\Microsoft \Windows\Temporary Internet Files
  - Firefox
    - C:\Documents and Settings\{username}\Local Settings \Application Data\Mozilla\Firefox\Profiles\ {FF profile} \Cache

Linux - /etc & friends

- System & configuration files
  - /etc is primary ; may have /usr/local/etc/ or /opt/local/etc
  - *# find / -name etc –print*
- */etc/passwd & /etc/shadow are gimies*
- *Web server configuration files*

Linux file plundering cont.

- Users home directory
  - .ssh directory
    - config file – configuration for ssh connections
    - keys (public and private)
  - .gnupg directory
    - conf file contains aliases and more
    - key rings
  - users PATH
    - Look for interesting tools (downloads, desktop)
  - Browser Autocomplete data

Windows file plundering

- SAM db
  - extract hashes and crack
  - Pull cached credentials with fgdump
- RSA SecureID Auth Manager server seed file (.asc)
  - import the file to Cain & Abel to generate tokens

Windows plundering cont.

- Browser Autocomplete data
- Downloads folder
  - possible tools that you can use
  - types of downloads can profile your targets
- Desktop & Documents folders
  - look for recent items

Mac OSX plundering sidenote

- Keychain is king
  - Get access to users keychain : game over time
  - Stores all login credentials and certs for that user
  - Files stored:
    - /Library/Keychains
    - ~/Library/Keychains
    - /Network/Library/Keychains

Memory Sniffing

- Remote
  - Windows
    - win32dd from Matthieu Suiche
      - http://win32dd.msuiche.net/
      - Dumps memory to a file
  - Linux
    - apptrace by Bill Stearns
      - http://www.stearns.org/apptrace/
      - Memory traces any application by name

Social Pillaging

- Social network sites
  - Facebook
  - Myspace
  - LinkedIn
- Tools / Projects
  - Maltego, Social Butterfly
- What to mine?
  - Answers to security questions, relationships for social engineering, etc

Wrap up

- Always use these techniques for good
- Always use these techniques with permission
- Share your kung fu
- Thanks to SANS & Core!