taking one shell and turning it into ten thousand

POST EXPLOITATION

Outline – High Level

- Risk Management
  - Risk Assessment
- Operational Methodologies
  - OPSEC
  - Tactics / Techniques

Outline – Low Level

Windows

- Initial Cleanup
- Recon
- Privilege Escalation
- Persistence
- Pivoting
- Stealth
- Deception

*NIX (Linux)

- Initial Cleanup
- Recon
- Privilege Escalation
- Persistence
- Pivoting
- Stealth
- Deception

Risk Management

- Piece of Risk Management
  - identify, characterize, and assess threats
  - assess the vulnerability of critical assets to specific threats
- Risk Assessment
  - Pentest = Qualitative Assessment
  - Critical Assets

Assets (Goals)

- IP / Source Code
  - Developers
  - Access
    - svn, cvs, sourcesafe
  - Create
    - Visual studio
    - Eclipse
  - Test
    - Dev network – ssh
    - Virtual machines – vmware
  - Effects
- SCADA
  - Operators
  - Access
    - GUI
    - Segregated network
  - Control
    - GUI
  - Effects

Data VS Access

Operational Methodologies

- OPSEC (Operational Security)
- OPSEC is a systematic method used to identify, control, and protect critical information.

“If I am able to determine the enemy’s dispositions while at the same time I conceal my own, then I can concentrate and he must divide”

- Sun Tzu

Operational Methodologies

- OPSEC Countermeasures
  - are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system

"Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."

- George Washington

Operational Methodologies

- Tactics and Techniques
  - Recon
  - Persistence
  - Privilege Escalation
  - Pivoting
  - Stealth
  - Deception
  - Reporting / Logging
  - Automation

We’re In!!

Initial Cleanup

- Cleanup initial access
- Side effects
- Logs
- Report home

Recon

- User Related
- System Related
- Environment Related
- Target Related

Recon

Windows

- Meterpreter
- Boxcutter
- Tasklist.exe
- Netstat –an

Linux

- Xwd
- import (Imagemagik)
- ps aux / ps –elf
- Netstat –an

Recon

Windows

- Meterpreter
- Boxcutter

Linux

- Xwd
- import (Imagemagik)

Screen Shot

Recon

Windows	Linux
Connections, Processes	
Tasklist.exe	ps aux / ps –elf
Netstat -an	Netstat -an

Recon

Windows

- Arp –a
- Route print
- Ipconfig, netsh.exe
- Systeminfo.exe
- Applications
- Net Commands

Linux

- Arp –a
- Route (privledge)
- Ifconfig, iptables (privledge)
- Uname –a
- Applications
- Mounts
  - Nfs,cifs

Recon

Windows	Linux
Arp –a	Arp –a
Route print	Route (privledge)
Ipconfig, netsh.exe	Ifconfig, iptables

Network Configuration

Recon

Windows

Linux

System Configuration

- Systeminfo.exe
- Applications
- Net commands

- Uname –a
- Applications
- Mounts
  - Nfs, cifs

Recon

Windows

- Net commands
- reg.exe export
- HKCU - RunMRU

Linux

- .bashrc, .profile, bash_profile, bash_history
- Env
- Last, w
- Id, groups

User information / Other

Recon

Windows

Configuration Errors:

- Services
- Files
- Registry
- Processes
- Pipes

Linux

Configuration Errors:

- Suid, sgid binaries
- Open X11

Recon

Linux

Configuration Errors:

- Suid, sgid binaries
- Open X11

- find / \(-perm -004000 -o -perm -002000 \) -type f -print
- Xspy, xauth

Recon

Windows

Configuration Errors:

- Services
- Files
- Registry
- Processes
- Pipes

Securable Objects

DACL’s

SACL’s

ACE’s

- SDDL
  - Security Descriptor Definition Language

Recon

Windows Configuration Errors:

- Services

```
C:\WINDOWS\system32>sc sdshow alerter

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)
```

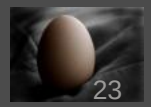
Recon

Windows Configuration Errors:

- Files

```
C:\WINDOWS\system32>cacls.exe svchost.exe

C:\WINDOWS\system32\svchost.exe BUILTIN\Users:R
                                BUILTIN\Power Users:R
                                BUILTIN\Administrators:F
                                NT AUTHORITY\SYSTEM:F
```



Recon

Windows

Configuration Errors:

- Services
- Files
- Registry
- Processes
- Pipes

Other Tools:

- Accesschk.exe
  - (sysinternals)
- Subinacl.exe
  - Microsoft resource kit

Recon

Windows

Network Info:

- Netbios NULL
  - Net, nbtstat
  - Enum
- Find_token
  - NetWksaUserEnum
- winpcap

Linux

Network Info:

- Netbios –U “” -N
  - Smbtree, rpcclient,
  - Smbclient, net, nmblookup
- Tcpdump / wireshark

Recon

Windows

Hashes:

- Network Sessions
- Local
- Wifi Secrets
- Tokens

Linux

Hashes:

- /etc/shadow
- Ssh keys
- Wifi secrets
  - Wpa_supplicant.conf

Gsecdump.exe, pass the hash toolkit

Privilege Escalation

- Configuration Errors
- Trojan
- Exploit

Privilege Escalation

Windows

Configuration Errors:

- HP Pml Driver
- Acrobat Getplus driver

Linux

Configuration Errors:

- Suid
  - Vim (!sh), nmap (!sh)
- Open X11
- NFS
  - nfsshell

Privilege Escalation

Windows

Trojan:

- Manifests.xml
- Registry settings
  - HKLM – AutoRun
  - HKCU – AutoRun
- Admin scripts
- keylogger

Linux

Trojan:

- LD_PRELOAD
- Alias
  - Sudo, su
- Add . To PATH
- Rc files
- Admin scripts
- keylogger

Privilege Escalation

Windows

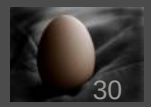
Exploit:

- Processes Running as SYSTEM
- Oracle

Linux

Exploit:

- Sock_sendpage
- udev
- Enlightenment



Persistence

- Legitimate Access (Username:Password)
- How do you keep persistence on your machine?

Persistence

Windows

- Session hashes
- Create Accounts
- RDP
- VNC
- At.exe
- Run keys
- Nc, cryptcat, socat

Linux

- SSH keys
- Kerberose Tickets
  - KRB5CC_NAME
- Create Accounts
- VNC
- Crontab
- Inittab, init.rd
- Nc,cryptcat, socat

Persistence

Windows

- Session hashes
- Create Accounts
- RDP
- VNC

Linux

- SSH keys
- Kerberose Tickets
  - KRB5CC_NAME
- Create Accounts
- VNC

Legitimate Access

Persistence

Windows

- RDP
- VNC
- At.exe
- Run keys
- Nc, cryptcat, socat

Linux

- VNC
- Crontab
- Inittab, init.rd
- Nc,cryptcat, socat

Listeners, alternate remote access

Persistence

Windows

- Install services
- Gina.dll
- Sethc.exe
- Re-enable accounts
- Introduce Vulns
  - VNC Auth bypass
  - Downgrade putty
- Rootkits

Linux

- /bin/login
- PAM
- X11
- Re-enable accounts
- Intruduce Vulns
  - VNC Auth bypass
- Rootkits

Persistence

Windows

- Install services
- Gina.dll

Linux

- /bin/login
- PAM

Standard Trojans

Persistence

Windows

- Sethc.exe
- Re-enable accounts
- Introduce Vulns
  - VNC Auth bypass
  - Downgrade putty

Linux

- X11
- Re-enable accounts
- Intruduce Vulns
  - VNC Auth bypass

Non-Standard

Pivoting

- Credential Exploitation
- Network Relay

Pivoting

Windows

- Pass the hash
- Downgrade putty
- Port Forwarding
  - Fpipe.exe
  - Nc.exe, socat.exe

Linux

- SSH master mode
  - (also for stealth)
- Port Forwarding
  - Nc , ssh –D , ssh –R -L

Stealth

- Ssh master mode

Deception

- Hping

Outline – High Level

- Risk Management
  - Risk Assessment
- Operational Methodologies
  - OPSEC
  - Tactics / Techniques

Outline – Low Level

Windows

- Initial Cleanup
- Recon
- Privilege Escalation
- Persistence
- Pivoting
- Stealth
- Deception

*NIX (Linux)

- Initial Cleanup
- Recon
- Privilege Escalation
- Persistence
- Pivoting
- Stealth
- Deception

Homework

Assignment 1:

Retrieve the username, password and hostname from putty_053b.exe memory space

Assignment 2:

Find 3 local privilege escalations by use of bad ACL's

- Service ACL
- Service through file ACL
- Service through registry ACL