

Attack



Research

# Post Exploitation

A practical introduction to offensive  
Information Warfare



# Information Warfare

- "Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary." [1.]



# Risk Management and Asset Valuation

- “Risk assessment is the process of determining whether existing or proposed safeguards are adequate to protect information resources from likely threats.” [2.]
- “It involves identifying assets to be protected, threats to those assets and the likelihood of their occurrence, vulnerabilities that could be exploited, losses that could result from an attack, and safeguards that are or could be installed.” [2.]



# Risk Management

## Application Assessment

- Clearly defined assets
- Clearly defined threats
- Narrow scope

## Network Assessment

- Unknown or poorly defined assets
- Unknown or poorly defined threats
- Hopefully Wide scope



# Briefing

- Intelligence**
- What is Intelligence
  - Elements of Intelligence
    - Collection, Analysis, Counter Intelligence, Cover Action
  - Operational Methodologies
    - Operational Security (OPSEC)



# Briefing

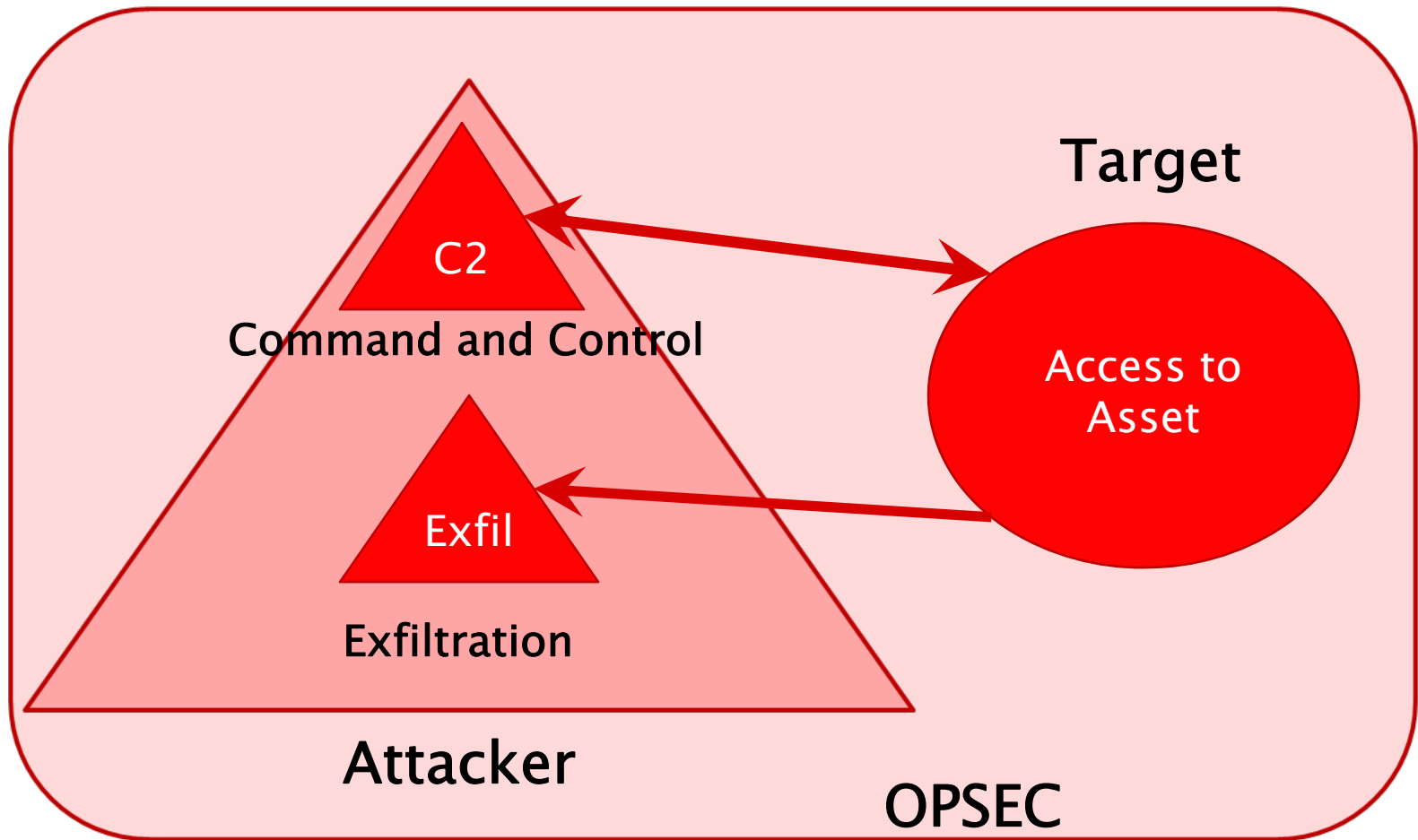
## Process of Post Exploitation

- Access to Asset
  - C2, Exfil
- Recon
- Persistence
- Escalation of Privilege
- Pivoting / Lateral Movement



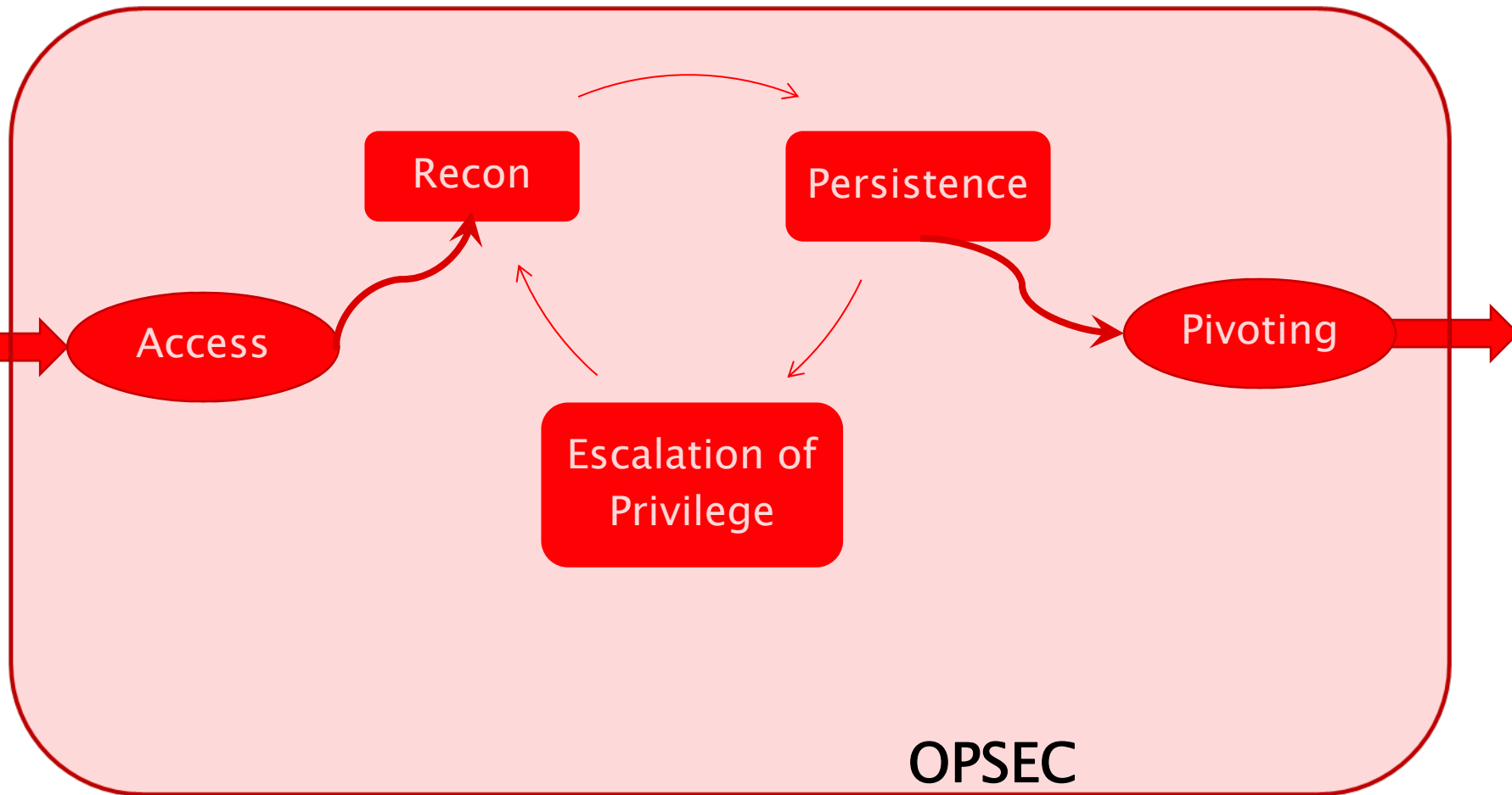
# Briefing

## Process of Post Exploitation



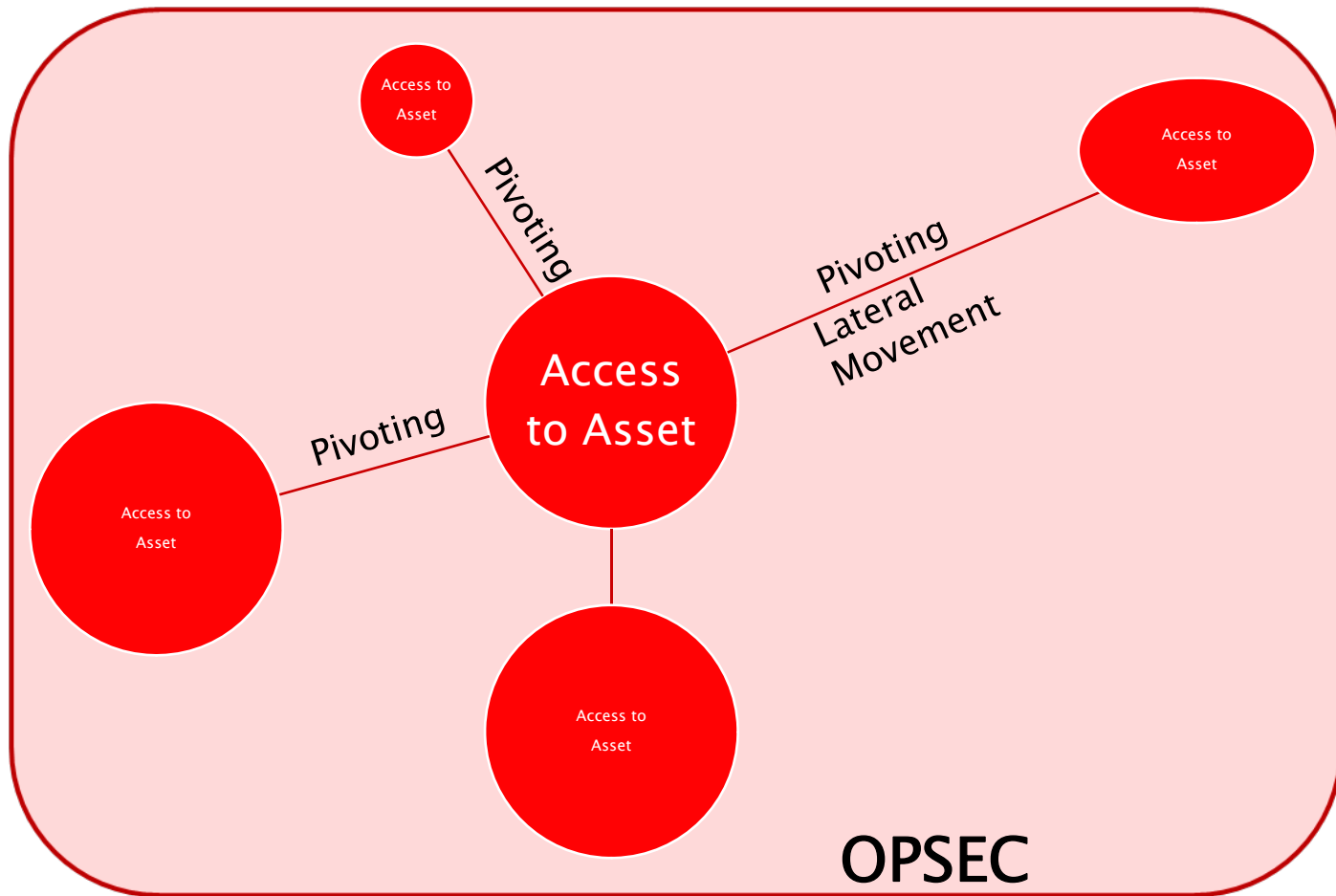
# Briefing

## Process of Post Exploitation



# Briefing

## Process of Post Exploitation



# Briefing

## Case Study Stuxnet



# Intelligence

SPY vs. SPY



# Intelligence

- “As an activity, intelligence involves the collection and analysis of intelligence information. It also includes activities undertaken to counter the intelligence activities of adversaries, either by denying them access to information or by deceiving them about the facts or their significance.”  
[3.]



# Elements of Intelligence

- **Collection**
- **Covert Action**
- **Analysis**
- **Counter-intelligence**



# Collection

- “Collection refers to the gathering of raw data, through **espionage**; technical means (photography, interception of electronic communications, and other methods involving technology)”[4.]



# Analysis

- “Thus, the process of analyzing the available information to make judgments about the capabilities, intentions, and actions of another party is a vital part of the intelligence process. Even more difficult is the process of forecasting the future capabilities, intentions, and actions of an adversary” [5.]



# Covert Action

- “Conceptually, covert action differs from the other elements of intelligence in that while the others are concerned with **seeking and safeguarding information**, covert action seeks to influence political events directly.” [6.]
- “an activity midway between diplomacy and war.” [7.]



# Counterintelligence

- “In its most general sense, counterintelligence seeks to protect a society (and especially its intelligence capabilities) against any harm that might be inflicted by hostile intelligence services.”[8.]



# Counterintelligence

- “In the first place, counterintelligence involves denying certain information to adversaries. This protection is accomplished by programs of security”[9.]
- “In addition, counterintelligence can seek to protect against an adversary’s intelligence analysis as well as his collection capability; this is done through deception operations”[10.]



# 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



# Intelligence and Operational Methodologies

## Elements

- Collection
- Analysis
- Counterintelligence

## OPSEC

- Deny
- Deceive



# Through the eyes of Stuxnet



## W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Stuxnet

## Access to Asset

- Command and Control (C2) / Exfil
  - Port 80 several servers
    - mypremierfutbol.com
    - todaysfutbol.com
  - [http://]www.mypremierfutbol.com/index.php?data=1234
  - HTTP Content Section
  - The decrypted server response has the following format:
    - 0x00 dword payload module size (n)
    - 0x04 byte command byte, can be 0 or 1
    - 0x05 byte[n] payload module (Windows executable)



# Stuxnet

## Access to Asset OPSEC

- First payload data XOR-ed data with 0xff
- Inject into legitimate Browser process
  - HKEY\_CLASSES\_ROOT\HTTP\SHELL\OPEN\COMMAND
- Server Response Encrypted HTTP content
- The payload is then XOR-ed with a static 31-byte long byte string



# Stuxnet

## Access to Asset Dossier Reference

- C2
  - Page 21
  - Page 22
  - Page 18
- Exfil
  - Page 21
  - Page 22

### W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Stuxnet Recon Dossier Reference

- Page 16
- Page 19
- Page 21
- Page 28
- Page 33
- Page 34

## W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Stuxnet

## Persistence Dossier Reference

- Page 13
- Page 14
- Page 17
- Page 18
- Page 20
- Page 25
- Page 27
- Page 33
- Page 34

### W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Stuxnet

Escalation of Privilege  
Dossier Reference

- Page 19

## W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Stuxnet

Pivoting / Lateral Movement  
Dossier Reference

- Page 18
- Page 25
- Page 26
- Page 27
- Page 29
- Page 31

## W32.Stuxnet Dossier

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)



# Initial Cleanup

- Cleanup initial access
- Side effects
- Logs
- Report home
  - Command and Control
  - Exfiltration



# Command and Control (C2) and Exfiltration (Exfil)

- Initial Vector
  - Leverage for C2 and Exfil
  - Call home
- Identify local methods for
  - C2
  - Exfil
  - Part of Recon
- Deploy methods for
  - C2
  - Exfil
  - Part of Persistence



# Command and Control (C2) and Exfiltration (Exfil)

- Initial Vector
  - Leverage for C2 and Exfil
  - Call home
- Identify local methods for
  - C2
  - Exfil **OPSEC**
  - Part of Recon
- Deploy methods for
  - C2
  - Exfil
  - Part of Persistence



# C2 and Exfil OPSEC

- Deny
  - Use Encryption
    - SSH, SSL, Public Key
    - Both in transit and storage
- Deceive
  - Use what they Use
    - Hide in noise
  - Use Obfuscation
    - XOR, Modified Base64
    - Java Script, Java
- Anti Virus
- HIDS
- NIDS
- Host Logs
- Network Logs
- Host Firewall
- Network Firewall
- Full Packet Capture
- Human (Adversary)



# C2 and Exfil

## Local methods

### Windows

- RDP
- VNC, SSH
- Meterpreter
- Netcat, Cryptcat, Socat
- (HTTP) wget, curl, VB, .NET
- ftp, tftp
- Netbios
- At
- DNS, ICMP

### Linux

- SSH
  - SCP, SFTP
- VNC, RDP
- Meterpreter
- Netcat, Cryptcat, Socat
- (HTTP) wget, curl, .NET (mono)
- ftp, tftp
- Netbios (Samba)
- DNS, ICMP



# C2 and Exfil

- Initial Cleanup
- Initial Vector
- Identified some local methods
- OPSEC
- Deny
- Deceive



# Recon & Persistence

---



# Recon

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



# Recon

## Screen Shots, Connections, and Processes

### Window

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

### Linux

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



# Recon

## System and Network information

### Window

- VB
- Arp -a
- Route print
- Ipconfig, netsh.exe
- Systeminfo.exe
- Applications
- Net Commands
- VB with Windows Indexing service

### Linux

- Arp -a
- Route (privledge)
- Ifconfig, iptables (privledge)
- Uname -a
- Applications
- Mounts
  - Nfs,cifs
- updatedb -l 0 -o db\_file -U source\_directory



# Recon

User information and Other

## Window

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

## Linux

- .bashrc, .profile, bash\_profile, bash\_history
- Env
- Last, w
- Id, groups



# Recon

## Configuration Errors

### Window

- Services
- Files
- Registry
- Processes
- Pipes

### Linux

- 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

## Network Info

### Window

- Netbios NULL
  - Net, nbtstat
  - Enum
- Find\_token
  - NetWksaUserEnum
- winpcap

### Linux

- Netbios -U "" -N
  - Smbtree, rpcclient,
  - Smbclient, net, nmblookup
- Tcpdump / wireshark



# Recon

## Hashes

### Window

- Network Sessions
- Local
- Wifi Secrets
- Tokens

### Linux

- /etc/shadow
- Ssh keys
- Wifi secrets
  - Wpa\_supplicant.conf



# Persistence

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



# Persistence

## Legitimate Access

### Window

- Session hashes
- Create Accounts
- RDP
- VNC

### Linux

- SSH keys
- Kerberos Tickets
  - KRB5CC\_NAME
- Create Accounts
- VNC



# Persistence

Listeners, alternate remote access

## Window

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

## Linux

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



# Persistence

## Standard Trojans

### Window

- Install services
- Gina.dll
- Rootkits

### Linux

- /bin/login
- PAM
- Rootkits



# Persistence

## Non-Standard Trojans

### Window

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

### Linux

- X11
- Re-enable accounts
- Introduce Vulns
  - VNC Auth bypass
- Rootkits



# Recon & Persistence

## Recon

- OPSEC
- Defines
  - C2
  - Exfil
  - Persistence
- Locates Assets
- Discovers Threats
  - To us
- Discovers Vulns
- Discovers Targets

## Persistence

- Legitimate Access
- User
- System
- Multiple
  - Leverage EoP
- OPSEC



# Escalation of Privilege (EoP)

- Configuration Errors
- Vulnerabilities
- Trojans



# Escalation of Privilege

## Windows configuration errors

- Bad ACL's
  - HP Pml Driver
  - Acrobat Getplus driver

## Linux configuration errors

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



# Escalation of Privilege

## Windows configuration errors

- Bad ACL's
  - HP Pml Driver
  - Acrobat Getplus driver

## Linux configuration errors

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

OPSEC



# EoP OPSEC Configuration errors

- Deny
  - Disable AV, Firewall
- Deceive
  - Use what they Use
    - Hide in noise
- Anti Virus
- HIDS
- NIDS
- Host Logs
- Network Logs
- Host Firewall
- Network Firewall
- Full Packet Capture
- Human (Adversary)



# Escalation of Privilege

## Windows Vulnerabilities

- Microsoft Windows NT #GP Trap Handler
  - CVE-2010-0232
  - metasploit
  - 17 years
- Task Scheduler
  - CVE-2010-3888

## Linux Vulnerabilities

- sock\_splice
  - CVE-2009-2692
  - Enlightenment
  - 8 years
- Pam MOTD
  - CVE-2010-0832
- Glib C \$ORIGIN
  - CVE-2010-3847



# Escalation of Privilege

## Windows Trojans

- Manifests.xml
- DLL load via Netbios
- Registry settings
  - HKLM – AutoRun
  - HKCU – AutoRun
- Admin scripts
- keylogger

## Linux Trojans

- LD\_PRELOAD
- Alias
  - Sudo, su
- Add . To PATH
- Rc files
- Admin scripts
- keylogger



# Escalation of Privilege



## Windows Trojans

- Manifests.xml
- DLL load via Netbios
- Registry settings
  - HKLM – AutoRun
  - HKCU – AutoRun
- Admin scripts
- keylogger

## Linux Trojans

- LD\_PRELOAD
- Alias
  - Sudo, su
- Add . To PATH
- Rc files
- Admin scripts
- keylogger

OPSEC



# EoP OPSEC

## Trojans

- Deny
  - Use Encryption
    - SSL, Public Key
    - Both in runtime and on disk
- Deceive
  - Hide in noise
  - Use Obfuscation
    - XOR, Modified Base64
- Anti Virus
- HIDS
- NIDS
- Host Logs
- Network Logs
- Host Firewall
- Network Firewall
- Full Packet Capture
- Human (Adversary)



# Escalation of Privilege

- Configuration Errors
  - Create our own for Persistence
- Vulnerabilities
  - Create our own for Persistence
- Trojans
- OPSEC



# Pivoting // Lateral Movement

- Credential Exploitation
- Network Vulnerabilities
  - Introduced
- System Vulnerabilities
  - Introduced
- Network Relay



# Pivoting // Lateral Movement

- Credential Exploitation
- Network Vulnerabilities
  - Introduced
- System Vulnerabilities
  - Introduced **OPSEC**
- Network Relay



# Pivoting OPSEC

- Deceive
  - Use what they Use
    - Hide in noise
  - Use Obfuscation
    - XOR, Modified Base64
    - Java Script, Java
  - Misdirection
- Deny
  - Use Encryption
    - SSH, SSL, Public Key
- Anti Virus
- HIDS
- NIDS
- Host Logs
- Network Logs
- Host Firewall
- Network Firewall
- Full Packet Capture
- Human (Adversary)



# Pivoting // Lateral Movement

## Windows

- RDP
- Netbios
  - Pass the hash
  - Find\_token
  - At
- Downgrade putty
- Port Forwarding
  - Fpipe.exe
  - Nc.exe, socat.exe

## Linux

- SSH
  - master mode
  - Host keys
- Port Forwarding
  - tcpxd
  - Nc
  - ssh -D , ssh -R -L



# Pivoting // Lateral Movement

## Pass the Hash

### Windows

- Gsecdump
- Pass the hash toolkit
- Wce (Windows credential editor)
- Incognito
  - Find\_token
- Net use
- Metasploit

### Linux

- Metasploit
- Patched version of Samba tools
- Patched version of winexec

<http://www.foofus.net/~jmk/passhash.html>



# Pivoting // Lateral Movement

- Credential Exploitation
- Network Vulnerabilities
  - Introduced
- System Vulnerabilities
  - Introduced
- Network Relay
- OPSEC
  - Deceive
  - Deny



# Notes

1. Winn Schwartau, Information Warfare, 2nd ed., 1996, Pg: 12
2. Denning D. (1999). Information Warfare and Security. Pg: 385
3. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 105
4. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 200
5. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 204
6. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 206
7. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 206
8. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 212
9. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 212
10. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 216

