Post Exploitation

Taking one shell and turning it into ten thousand

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." [1.]

- "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." [1.]

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

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.” [2.]

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)"[3.]

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” [4.]

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." [5.]

- "an activity midway between diplomacy and war." [6.]

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.”[7.]

Counterintelligence

- “In the first place, counterintelligence involves denying certain information to adversaries. This protection is accomplished by programs of security”[8.]
- “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”[9.]

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

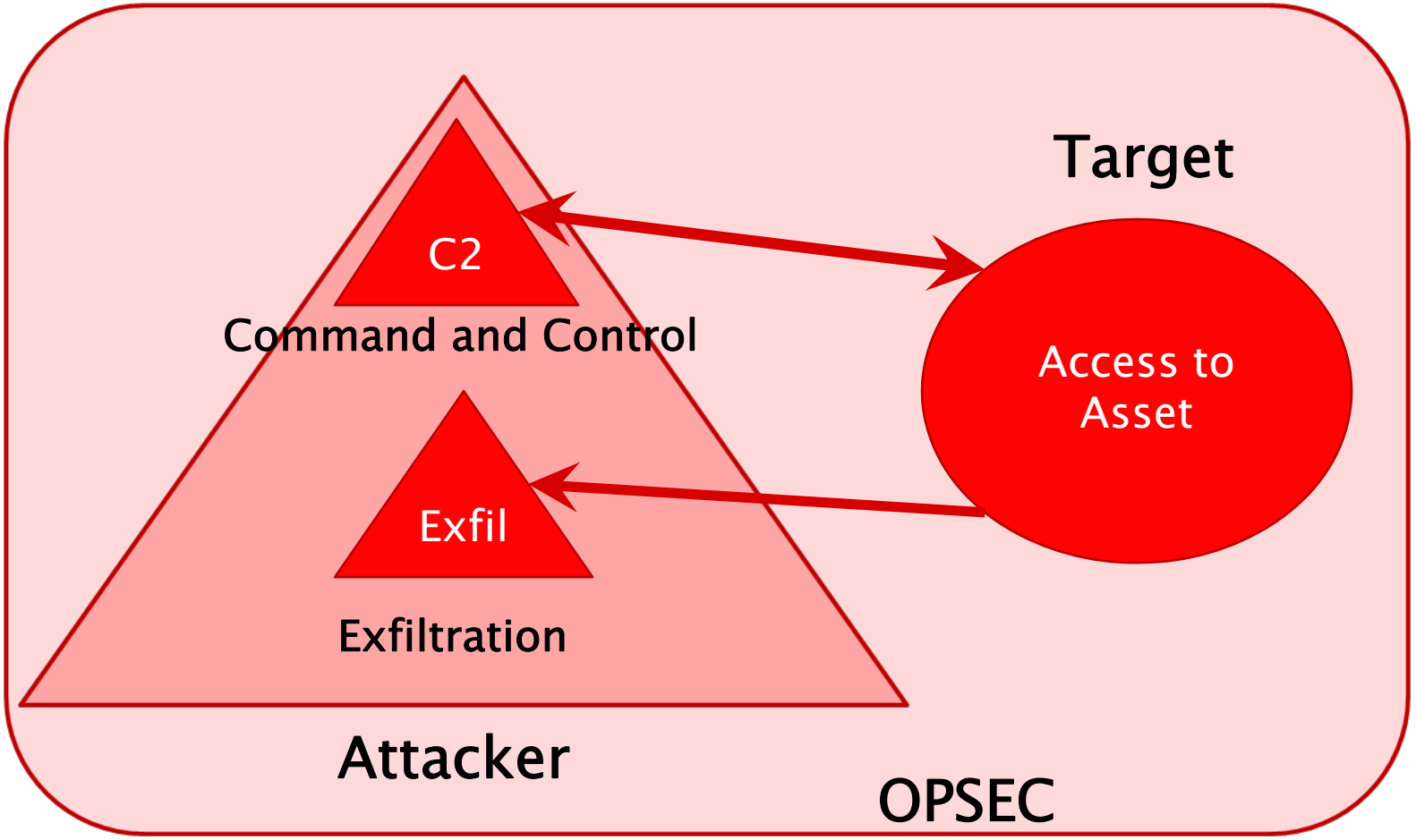
Elements

- Collection
- Analysis
- Counterintelligence

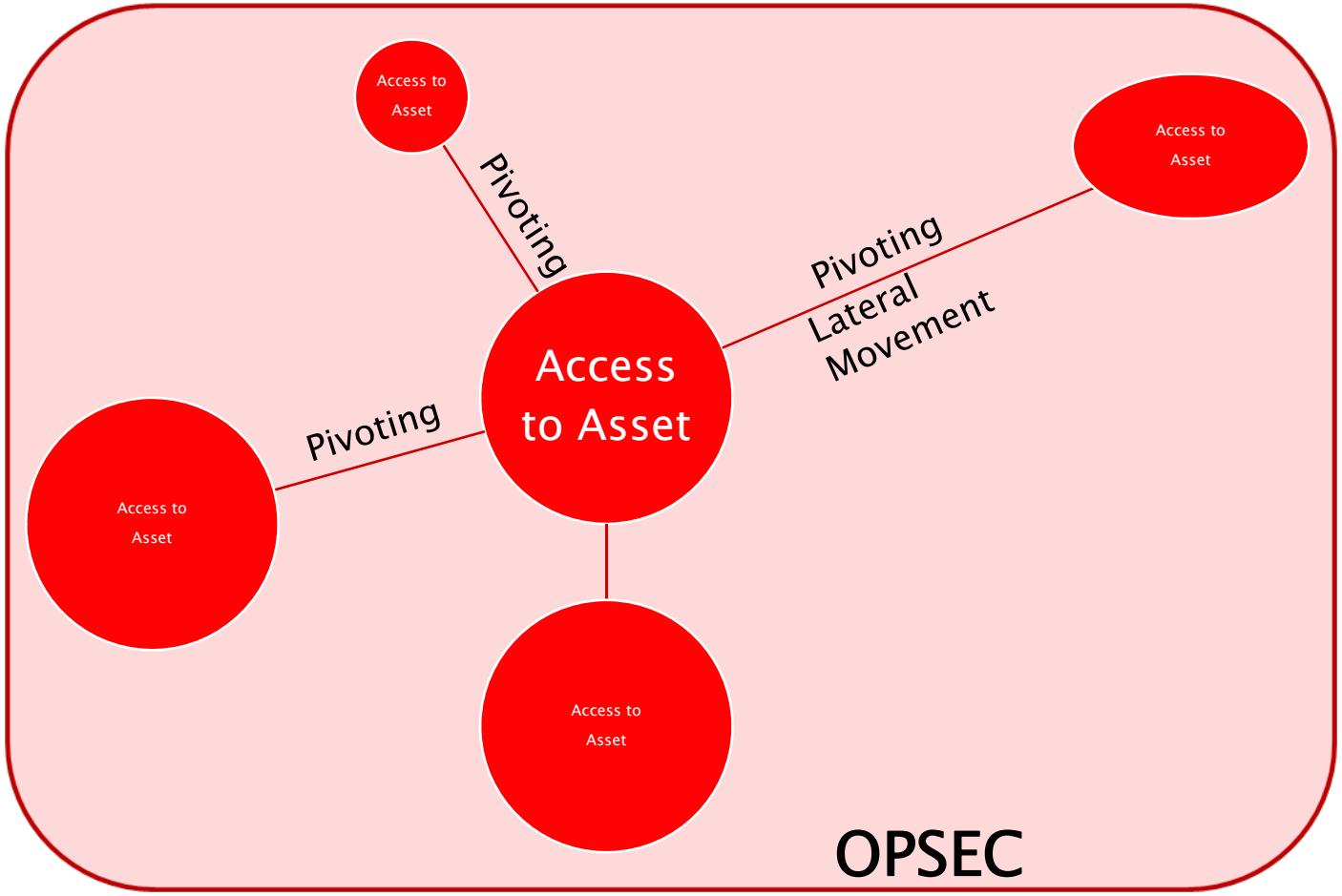
OPSEC

- Deny
- Deceive

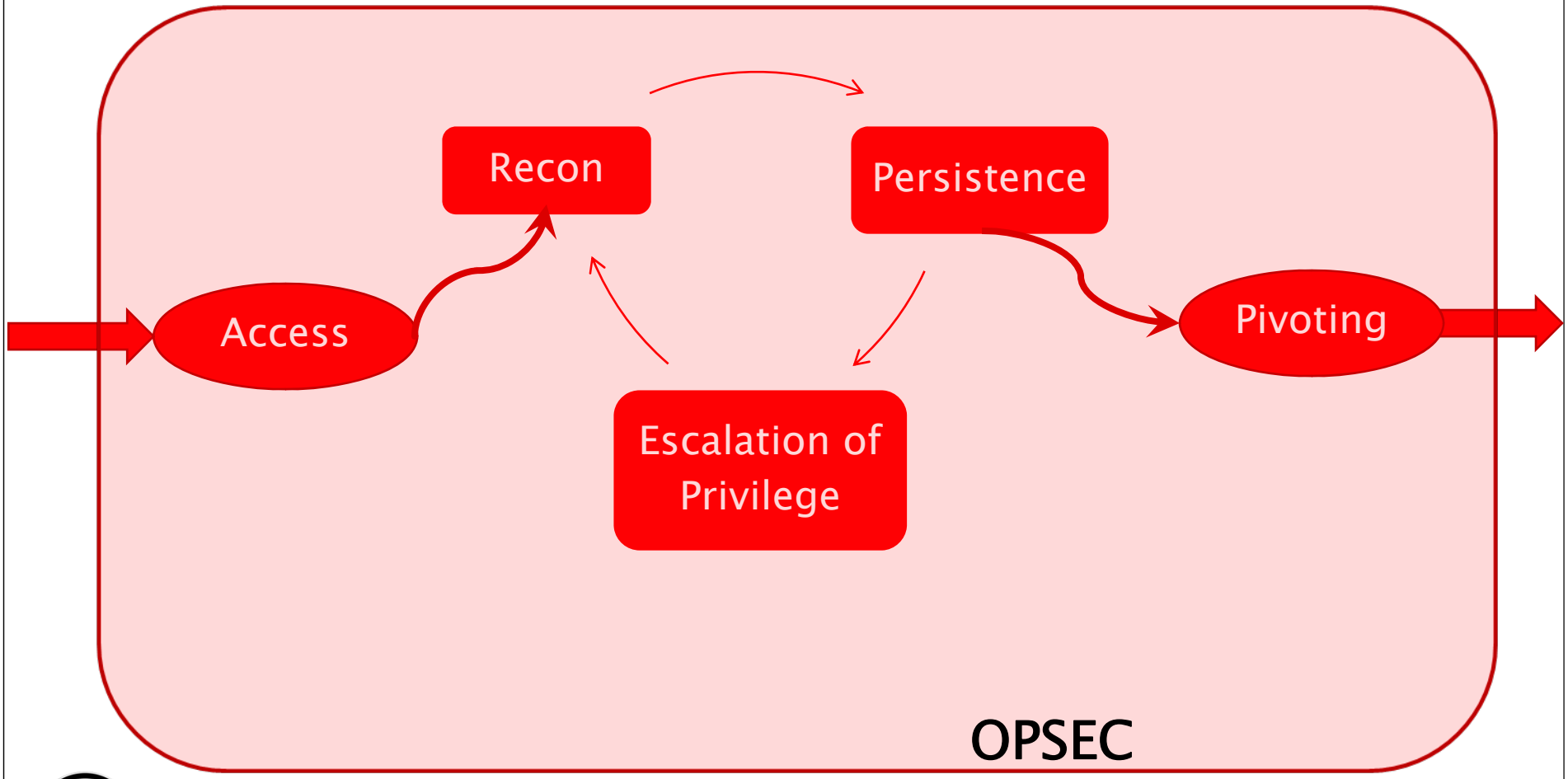
Post Exploitation



Post Exploitation



Post Exploitation



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
  - Part of Recon
- Deploy methods for
  - C2
  - Exfil
  - Part of Persistence

OPSEC

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
- Kerberose 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
- Intruduce 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

OPSEC

Linux configuration errors

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

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

OPSEC

Linux Trojans

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

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
- Network Relay

OPSEC

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. Denning D. (1999). Information Warfare and Security. Pg: 385
2. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 105
3. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 200
4. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 204
5. Shulsky A., Schmitt G. (2002). Silent Warfare: Understanding the World of Intelligence, 3d Edition [Kindle]. Loc: 206
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: 212
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: 216