0x01 前言

红蓝对抗的思想最早可追溯到我国现存最早的一部兵书《孙子兵法》，在孙子·谋攻篇有这么一句话：“知彼知己，百战不殆；”，意为如果对敌我双方的情况都能了解透彻，打多少次仗都不会失败。在信息安全领域目前大家都有一个共识：“未知攻，焉知防”，攻防对抗本身是一个持续的过程，在具体的对抗中，对对手了解越多就会占据主导地位。红蓝对抗的主要目的在于，提高公司安全成熟度及其检测和响应攻击的能力。Red Teams attack, and Blue Teams defend, but the primary goal is shared between them: improve the security posture of the organization.

0x02 准备工作

1）组织结构图

2）全网拓扑图

3）各系统逻辑结构图

4）各系统之间的调用关系

5）数据流关系

6）核心资产清单

7）应急响应计划

8）业务连续性计划

9）灾难恢复计划

0x03 简单安全评估

1.端口扫描和漏洞检测

1.1 主机发现（Ping 探测）

nmap -sn -PE IP 地址或地址段

1.2 端口扫描

nmap –open IP 地址或地址段

1.3 服务版本检测

nmap -sV IP 地址或地址段

1.4 扫描多个端口

nmap -p 80,443 IP 地址或地址段

1.5 UDP 扫描

nmap -sU -p 53 IP 地址或地址段

1.6 TCP/UDP 扫描（-Pn 跳过主机发现）

nmap -v -Pn -SU -ST -p U:53,111,137,T:21-25,80,139,8080 IP 地址或地址段

1.7 Nessus 扫描

nessus -q -x -T html 服务器 IP 服务器端口 管理员帐号 密码 目标.txt 输出报告.html

1.8 OPENVAS 扫描

apt -y install pcregrep

wget https://goo.gl/TYbLwE

chmod +x openvas-automate.sh && ./openvas-automate.sh 目标 IP

2. WINDOWS 系统篇

2.1 网络发现

基本网络发现：

C:> net view /all

C:> net view 主机名

Ping 探测：

C:> for /L %I in (1,1,254) do ping -w 30 -n 1 192.168.1.%I | find "回复" >> 输出.txt

2.2 DHCP

启用 DHCP 服务器日志功能：

C:> reg add HKLMSystemCurrentControlSetServicesDhcpServerParameters /v ActivityLogFlag /t REG_DWORD /d 1

默认日志文件目录：

C:> %windir%System32Dhcp

2.3 DNS

启用 DNS 服务器日志功能:

C:> DNSCmd DNS 服务器名 /config /logLevel 0x8100F331

配置日志文件目录:

C:> DNSCmd DNS 服务器名 /config /LogFilePath C:dns.log

配置日志文件大小:

C:> DNSCmd DNS 服务器名 /config /logfilemaxsize 0xffffffff

2.4 哈希值

文件校验和完整性验证（FCIV）:

Ref：http://support2.microsoft.com/kb/841290

单个文件:

C:> fciv.exe 文件名

计算 C 盘所有文件并把结果保存到文件中:

C:> fciv.exe c: -r -sha1 -xml 结果.xml

列出所有 hash 值:

C:> fciv.exe -list -sha1 -xml 结果.xml

certutil & PowerShell

certutil -hashfile 文件名 SHA1

PS C:> Get-FileHash 文件名 | Format-List

PS C:> Get-FileHash -algorithm md5 文件名

2.5 NETBIOS

nbtstat 扫描

C:> nbtstat -A 目标 IP 地址

NetBIOS 缓存

C:> nbtstat -c

批量扫描

C:> for /L %I in (1,1,254) do nbtstat -An 192.168.1.%I

2.6 微软基线安全分析器(MBSA)

扫描单个 IP

C:> mbsacli.exe /target IP 地址 /n os+iis+sql+password

扫描 IP 地址段

C:> mbsacli.exe /r IP 地址段 /n os+iis+sql+password

3. LINUX 系统篇

3.1 网络发现

查看开放的 SMB 共享

smbclient -L 目标主机名

Ping 探测

for ip in ip>/dev/null; [Misplaced &ip UP" || : ; done

3.2 DHCP

DHCP 日志

RHEL/CentOS

cat /var/lib/dhcpd/dhcpd. leases

Debian/Ubuntu

grep -Ei 'dhcp' /var/log/syslog.1

3.3 DNS

DNS 日志

rndc querylog && tail -f /var/log/messages | grep named

3.4 哈希值

计算某目录下所有可执行文件的 HASH 值

find /sbin -type f -exec md5sum {} >> md5sums.txt ;

md5deep -rs /sbin > md5sums.txt

3.5 NETBIOS

nbtstat 扫描

nbtscan 目标 IP 地址或 IP 地址段

举例：nbtscan 192.168.1.2-100

4. 安全加固

4.1 WINDOWS 系统篇

4.1.1 禁用/停止服务

C:> sc query

C:> sc config "服务名" start= disabled

C:> sc stop "服务名"

C:> wmic service where name="服务名" call ChangeStartmode Disabled

4.1.2 防火墙管理理

列出所有规则:

C:> netsh advfirewall firewall show rule name=all

启用或禁用防火墙:

C:> netsh advfirewall set currentprofile state on

C:> netsh advfirewall set currentprofile firewallpolicy blockinboundalways,allowoutbound

C:> netsh advfirewall set publicprofile state on

C:> netsh advfirewall set privateprofile state on

C:> netsh advfirewall set domainprofile state on

C:> netsh advfirewall set allprofile state on

C:> netsh advfirewall set allprof ile state off

配置举例:

netsh advfirewall firewall add rule name="开放 TCP:80 端口" dir=in action=allow protocol=TCP localport=80

netsh advfirewall firewall add rule name="开放 TCP:443 端口" dir=in action=allow protocol=TCP localport=443

netsh advfirewall firewall add rule name="屏蔽 TCP:445 端口" dir=in action=block protocol=TCP localport=445

netsh advfirewall firewall add rule name="允许 MyApp" dir=in action=allow program="C:MyAppMyApp.exe" enable=yes

4.1.3 清除 DNS 缓存和 Netios 缓存

C:> ipconfig /flushdns

C:> nbtstat -R

4.1.4 应用控制

AppLocker 配置

导入 Applocker 模块

PS C:> import-module Applocker

查看 system32 目录下所有 exe 文件的 Applocker 信息

PS C:> Get-ApplockerFileinformation -Directory C:WindowsSystem32 -Recurse -FileType Exe

增加一条针对 system32 目录下所有的 exe 文件的允许规则

PS C:> Get-Childitem C:WindowsSystem32*,exe | Get-ApplockerFileinformation | New-ApplockerPolicy -RuleType Publisher, Hash -User Everyone -RuleNamePrefix System32

4.1.5 IPSEC

#使用预共享密钥的方式新建一条 IPSEC 本地安全策略，应用到所有连接和协议

C:> netsh ipsec static add filter filterlist=MyIPsecFilter srcaddr=Any dstaddr=Any protocol=ANY

C:> netsh ipsec static add filteraction name=MyIPsecAction action=negotiate

C:> netsh ipsec static add policy name=MyIPsecPolicy assign=yes

C:> netsh ipsec static add rule name=MyIPsecRule policy=MyIPsecPolicy filterlist=MyIPsecFilter filteraction=MyIPsecAction conntype=all activate=yes psk=密码

#新建一条允许访问外网 TCP 80 和 443 端口的 IPSEC 策略

C:> netsh ipsec static add filteraction name=Allow action=permit

C:> netsh ipsec static add filter filterlist=WebFilter srcaddr=Any dstaddr=Any protocol=TCP dstport=80

C:> netsh ipsec static add filter filterlist=WebFilter srcaddr=Any dstaddr=Any protocol=TCP dstport=443

C:> netsh ipsec static add rule name=WebAllow policy=MyIPsecPolicy filterlist=WebFilter filteraction=Allow conntype=all activate=yes psk=密码

#查看和禁用某条 IPSEC 本地安全策略

C:> netsh ipsec static show policy name=MyIPsecPolicy

C:> netsh ipsec static set policy name=MyIPsecPolicy assign=no

新建一条 IPSEC 对应的防火墙规则，源地址和目的地址为 any

C:> netsh advfirewall consec add rule name="IPSEC" endpointl=any endpoint2=any action=requireinrequireout qmsecmethods=default

新建一条 IPSEC 对应的防火墙规则，所有出站请求必须提供预共享密钥

C:> netsh advfirewall firewall add rule name="IPSEC_Out" dir=out action=allow enable=yes profile=any localip=any remoteip=any protocol=any interfacetype=any security=authenticate

4.1.6 其他安全策略

禁用远程桌面连接

C:> reg add "HKLMSYSTEMCurrentControlSetControlTerminalServer" /f /v fDenyTSConnections /t REG_DWORD /d 1

只发送 NTLMv2 响应（防止“永恒之蓝”漏洞攻击）

C:> reg add HKLMSYSTEMCurrentControlSetControlLsa /v lmcompatibilitylevel /t REG_DWORD /d 5 /f

禁用 IPV6

C:> reg add HKLMSYSTEMCurrentControlSetservicesTCPIP6Parameters /v DisabledComponents /t REG_DWORD /d 255 /f

禁用 sticky 键

C:> reg add "HKCUControlPanelAccessibilityStickyKeys" /v Flags /t REG_SZ /d 506 /f

禁用管理共享（Servers/Workstations）

C:> reg add HKLMSYSTEMCurrentControlSetServicesLanmanServerParameters /f /v AutoShareServer /t REG_DWORD /d 0

C:> reg add HKLMSYSTEMCurrentControlSetServicesLanmanServerParameters /f /v AutoShareWks /t REG_DWORD /d 0

禁用注册表编辑器和 CMD 命令提示符

C:> reg add HKCUSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem /v DisableRegistryTools /t REG_DWORD /d 1 /f

C:> reg add HKCUSoftwarePoliciesMicrosoftWindowsSystem /v DisableCMD /t REG_DWORD /d 1 /f

启用 UAC

C:> reg add HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem /v EnableLUA /t REG_DWORD /d 1 /f

启用防火墙日志

C:> netsh firewall set logging droppedpackets = enable

C:> netsh firewall set logging connections = enable

4.2 LINUX 系统篇

4.2.1 服务管理

查看服务状态

service –status-all

ps -ef OR ps -aux

initctl list

systemctl list-unit-files

启动，停止和禁用服务

For Upstart services:

/etc/init.d/apache2 start | stop | status

service apache2 start | stop | status

update-rc.d apache2 disable

For Systemd services:

systemctl start | stop | status ntp.service

systemctl disable sshd.service

4.2.2 防火墙管理

iptables 常用操作:

iptables-save > filewall_rules.bak # 导出当前规则

iptables -vnL –line # 列出所有规则

iptables -S # 同上

iptables -P INPUT DROP # 默认策略，禁止所有连接

iptables -A INPUT -s 10.10.10.10 -j DROP # 禁止单个 IP

iptables -A INPUT -s 10,10.10.0/24 -j DROP # 禁止一个网段

iptables -A INPUT -p tcp –dport ssh -s 10.10.10.10 -j DROP # 禁止某 IP 访问本机 SSH 服务

iptables -A INPUT -p tcp –dport ssh -j DROP # 禁止访问本机 SSH 服务

iptables -I INPUT 5 -m limit –limit 5/min -j LOG –log-prefix "

iptables denied: " –log-level 7 # 启用日志

iptables -F # 清除所有已加载的工作

4.2.3 DNS 缓存

Unix/Linux 系统没有系统级别 DNS 缓存

4.2.4 配置 IPSEC

在两台服务器之间建立 IPSEC 通道

1.）添加防火墙规则允许 IPSEC 协议

iptables -A INPUT -p esp -j ACCEPT

iptables -A INPUT -p ah -j ACCEPT

iptables -A INPUT -p udp –dport 500 -j ACCEPT

iptables -A INPUT -p udp –dport 4500 -j ACCEPT

2.）安装 Racoon

apt -y install racoon

3.）编辑配置文件：/etc/ipsec-tools.conf

flush;

spdflush;

spdadd 主机 A 的 IP 地址 主机 B 的 IP 地址 any -P out ipsec

esp/transport//require;

spdadd 主机 B 的 IP 地址 主机 A 的 IP 地址 any -P in ipsec

esp/transport//require;

4.）编辑配置文件：/etc/racoon/racoon.conf

log notify;

path pre_shared_key "/etc/racoon/psk.txt";

path certificate "/etc/racoon/certs";

remote anonymous {

exchange_mode main,aggressive;proposal { encryption_algorithm aes_256;

hash_algorithm sha256; authentication_method

pre_shared_key;

dh_group modp1024;

}

generate_policy off;

}

sainfo anonymous{

pfs_group 2;encryption_algorithm aes_256;authentication_algorithm hmac_sha256;compression_algorithm deflate;

}

5.）添加预共享密钥

主机 A：echo 主机 B 123 >> /etc/racoon/psk.txt

主机 B：echo 主机 A 123 >> /etc/racoon/psk.txt

6.)重启服务，检查协商及配置策略

service setkey restart

setkey -D

setkey -DP

5. 检测（Visibility）

5.1 网络安全监控

5.1.1 数据包捕捉与分析

1.）TCPDUMP

tcpdump -tttt -n -vv # 打印时戳、不进行名称解析及 verbose 方式显示

tcpdump -nn -c 1000 | awk '{print $3}' | cut -d. -f1-4 | sort -n | uniq -c | sort -nr # 捕捉 1000 个数据包，找出 Top talkers

tcpdump -w target.pcap -i any dst targetIP and port 80 # 在所有接口上捕捉目标 IP 为：targetIP 且端口为 80 的数据包并写入 target.pcap 文件

tcpdump host 10.0.0.1 && host 10.0.0.2 # 捕捉两个主机之间的数据包

tcpdump not net 10.10 && not host 192.168.1.2 #检视非 10.10 网段及非 192.168.1.2 主机的数据包

tcpdump host 10.10.10.10 && (10.10.10.20 or 10.10.10.30) # 检视主机 A 和主机 B 或 C 的数据包

tcpdump -n -s0 -C 100 -w 001.pcap # 轮询，文件大小超过 100M 后自动创建新文件

tcpdump -w – | ssh ServerIP -p 50005 "cat – > /tmp/remotecapture.pcap" # 保存捕获的数据包到远程服务器上的/tmp/remotecapture.pcap 文件

tcpdump -n -A -s0 port http or port ftp or port smtp or port imap or port pop3 | egrep -i 'pass=|pwd=|log=|login=|user=|username=|pw=|passw=|Passwd=|password=|pass:|user:|username:|password:|login:|pass|user' –color=auto –line-buffered -B20 # 抓取明文密码

tcpdump -s 1500 -A '(tcp[((tcp[12:1] & 0xf0) >> 2)+5:1] = 0x01) and (tcp[((tcp[12:1] & 0xf0) >> 2):1] = 0x16)' #查找自签名证书

2.）TSHARK

tshark -nr 001.pcap -Y "ssl.handshake.ciphersuites" -Vx | grep "ServerName:" | sort | uniq -c | sort -r # 提取证书 Server Name 字段

tshark -D # 列出所有接口

tshark -i eth0 -i eth1 # 监听多个接口

tshark -nn -w 001.pcap # 禁用名称解析并保存到文件

tshark arp or icmp # 捕捉 arp 或者 icmp

tshark "host 主机 A && host 主机 B" # 捕捉两个主机之间的数据包

tshark -r 001.pcap # 对已保存的数据包进行分析

tshark -n -e ip.src -e ip.dst -T fields -E separator=, -2 -R ip -r 001.pcap # 提取源/目的 IP 地址

tshark -n -e ip.src -e dns,qry.name -E separator=';' -T fields port 53 # 提取 DNS 查询的源 IP 及 DNS 查询的域名

tshark -2 -R http.request -T fields -E separator=';' -e http.host -e http.request.uri -r 001.pcap # 提取 HTTP 请求中的 host 参数和请求 uri

tshark -n -c 150 I awk '{print $4}' I sort -n | uniq -c | sort -nr # 提取 top talkers

tshark -q -z io,phs -r 001.pcap # 协议统计 tshark -n -c 100 -e ip.src -Y "dns.flags.response eq 1" -T fields port 53 # 提取响应的 DNS 服务器地址

tshark -n -e http.request.uri -Y http.request -T fields | grep exe # 提取通过 http 下载 exe 可执行文件的数据包

3.）SNORT

snort -T -c /etc/snort/snort.conf # 测试配置文件配置

snort -dv -r 001.log # 分析数据包

snort -dvr 001.log icmp # 取 icmp 数据包

snort -K ascii -l 001 # 抓包，ASCII 格式显示

snort -q -A console -i eth0 -c /etc/snort/snort.conf # 在终端打印

snort eventsecho 'log tcp 192.168.1.0/24 any -> 192.168.1.95 22 (msg: "ssh access" ; sid:1618008;)' > 001.rule && snort -T -c 001.rule # 规则测试

mkdir logs && snort -vd -c 001.rule -r 001.pcap -A console -l logs # 执行规则

4.）Bro NSM

apt -y install bro bro-aux

pip install bro-pkg

bro-pkg install bro/hosom/file-extraction

wget https://www.malware-traffic-analysis.net/2018/01/12/2018-01-12-NanoCore-RAT-traffic.pcap.zip

wget https://www.bro.org/static/exchange-2013/faf-exercise.pcap

bro -r 2018-01-12-NanoCore-RAT-traffic.pcap # 从 pcap 文件中读取数据并创建相关日志文件

bro -r faf-exercise.pcap /root/.bro-pkg/scratch/file-extraction/scripts/plugins/extract-pe.bro && ls -lhct ./extract_files/ # 提取 exe 文件

bro -r faf-exercise.pcap /usr/share/bro/policy/frameworks/files/extract-all-files.bro # 提取多个类型的文件

bro -C -r faf-exercise.pcap && cat ssl.log | bro-cut server_name , subject , issuer # 提取证书中的 server_name,issuer 和 subjects 字段

cat conn.log | bro-cut id.orig_h , id.orig_p , id.resp_h , id.resp_p , proto , conn_state

提取源 IP，源端口，目的 IP，目的端口，协议类型，tcp 标记

cat dns.log | bro-cut query | sort -u # 提取 DNS 查询 namecat http.log | bro-cut id.orig_h , id.orig_p , id.resp_h , id.resp_p , host , uri , referrer # 提取源 IP，源端口，目的 IP，目的端口，host，uri，referrer 字段

cat http.log | bro-cut user_agent | sort -u # 提取 user_agent 字段

5.）EDITCAP

editcap -F pcap -c 1000 orignal.pcap out_split.pcap # 以 1000 为单位进行分割

editcap -F pcap -t+3600 orignal.pcap out_split.pcap # 以 1 小时为单位进行分割

6.）MERGECAP

mergecap -w merged_cap.pcap capl.pcap cap2.pcap cap3.pcap # 合并多个文件

7.）PacketTotal

https://www.packettotal.com/app/analysis?id=c8c11b792272ac19a49299a3687466be&name=files

8.）NetworkMiner

http://netres.ec/?b=173588E

5.2 蜜罐技术

5.2.1 WINDOWS 系统篇

1.）端口蜜罐

原理：监听一些端口，客户端成功建立 TCP 连接后，记录访问日志，然后添加防火墙规则封禁此 IP

PS C:> certutil.exe -urlcache -split -f https://raw.githubusercontent.com/Pwdrkeg/honeyport/master/honeyport.ps1

PS C:> .honeyport.ps1 -Ports 4444,22,21,23 -WhiteList 192.168.10.1,192.168.10.2 -Block $true -Verbose

PS C:> Get-EventLog HoneyPort # 查看日志信息

PS C:> stop-job -name HoneyPort # 停止任务

PS C:> remove-job -name HoneyPort # 移除任务

5.3.2 LINUX 系统篇

1.）端口蜜罐

原理同上

wget https://raw.githubusercontent.com/gchetrick/honeyports/master/honeyports-0.5.

pypython honeyports-0.5.py -p 1234 -h 192.168.1.100 -D

2.) (PASSIVE)监控 DNS 解析

apt -y install dnstop

dnstop -l 3 eth0

dnstop -l 3 001.pcap | out.txt

5.3 日志审计

5.3.1 WINDOWS

增加日志文件大小进行日志审计

C:> reg add HKLMSoftwarePoliciesMicrosoftWindowsEventlogApplication /v MaxSize /t REG_DWORD /d 0x19000

C:> reg add HKLMSoftwarePoliciesMicrosoftWindowsEventlogSecurity /v MaxSize /t REG_DWORD /d 0x64000

C:> reg add HKLMSoftwarePoliciesMicrosoftWindowsEventLogSystem /v MaxSize /t REG_DWORD /d 0x19000

查看 Windows 事件日志-安全日志的配置

C:> wevtutil gl Security

检查审核策略

auditpol /get /category:*

对所有项启用成功和失败的审核策略

C:> auditpol /set /category:* /success:enable /failure:enable

查看已配置的事件日志的概要信息

PS C:> Get-Eventlog -list

取最近 5 条应用程序日志

PS C:> Get-Eventlog -newest 5 -logname application | Format-List

取 Eent ID：4672 的所有日志

PS C:> Get-Eventlog Security | ? { $_.Eventid -eq 4672}

登录与注销事件

PS C:> Get-Eventlog Security

4625,4634,4647,4624,4625,4648,4675,6272,6273,6274,6275,6276,6277,6278,6279,6

280,4649,4778,4779,4800,4801,4802,4803,5378,5632,5633,4964 -after

((get-date).addDays(-1))

DPAPI 行为，进程终止，RPC 事件

PS C:> Get-EventLog Security 4692,4693,4694,4695,4689,5712 -after

((get-date).addDays(-1)

文件共享，文件系统，SAM，注册表，证书时间

PS C: Get-EventLog Security

4671,4691,4698,4699,4700,4701,4702,5148,5149,5888,5889,5890,4657,5039,4659,4

660,4661,4663,4656,4658,4690,4874,4875,4880,4881,4882,4884,4885,4888,4890,48

91,4892,4895,4896,4898,5145,5140,5142,5143,5144,5168,5140,5142,5143,5144,516

8,5140,5142,5143,5144,5168,4664,4985,5152,5153,5031,5140,5150,5151,5154,5155

,5156,5157,5158,5159 -after ((get-date).addDays(-1))

查看 Eent ID：4672 的详细信息

Get-Eventlog Security | ? { $_.Eventid -eq 4672} | Format-List

5.3.2 LINUX

认证日志

tail /var/log/auth. log

```
grep -i "fail" /var/log/auth. log

tail /var/log/secure

grep -i "fail" /var/log/secure

# samba，cron,sudo 相关日志

grep -i samba /var/log/syslog

grep -i samba /var/log/messages

grep -i cron /var/log/syslog

grep -i sudo /var/log/auth. log

grep -i sudo /var/log/secure

# Apache 404 错误日志

grep 404 apache.log | grep -v -E "favicon.ico|robots.txt"

# 监控新文件，5 分钟刷新一次

watch -n 300 -d ls -lR /web_root
```

5.4 响应（取证）

5.4.1 WINDOWS 系统篇

1.）系统信息

```
C:> echo %DATE% %TIME%

C:> hostname

C:> systeminfo

C:> systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

C:> wmic csproduct get name

C:> wmic bios get serialnumber

C:> wmic computersystem list brief

C:> psinfo -accepteula -s -h -d

2.）用户信息

C:> whoamiC:> net users

C:> net localgroup administrators

C:> net group administrators

C:> wmic rdtoggle list

C:> wmic useraccount list

C:> wmic group list

C:> wmic netlogin get name,lastlogon,badpasswordcount

C:> wmic netclient list brief

C:> doskey /history > history.txt

3.）网络信息

C:> netstat -e

C:> netstat -naob

C:> netstat -nr

C:> netstat -vb

C:> nbtstat -s

C:> route print

C:> arp -a

C:> ipconfig /displaydns

C:> netsh winhttp show proxy

C:> ipconfig /allcompartments /all

C:> netsh wlan show interfaces

C:> netsh wlan show all

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionInternet SettingsConnectionsWinHttpSettings"

C:> type %SYSTEMROOT%system32driversetchosts

C:> wmic nicconfig get descriptions,IPaddress,MACaddress

C:> wmic netuse get name,username,connectiontype, localname

4.）服务信息

C:> at

C:> tasklist

C:> tasklist /svc

C:> tasklist /SVC /fi "imagename eq svchost.exe"

C:> tasklist /SVC /fi "imagename eq svchost.exe"

C:> schtasks

C:> net start

C:> sc query

C:> wmic service list brief | findstr "Running"

C:> wmic service list conf ig

C:> wmic process list brief

C:> wmic process list status

C:> wmic process list memory

C:> wmic job list briefPS

C:> Get-Service | Where-Object { $_.Status -eq "running" }

5.）策略、补丁、环境变量信息

C:> set

C:> gpresult /r

C:> gpresult /z > output.txt

C:> gpresult /H report.html /F

C:> wmic qfe

6.）自启动信息

C:> wmic startup list full

C:> wmic ntdomain list brief

6.1）检查自启动文件目录

C:> dir "%SystemDrive%ProgramDataMicrosoftWindowsStart MenuProgramsStartup"

C:> dir "%SystemDrive%Documents and SettingsAll UsersStart MenuProgramsStartup"

C:> dir %userprofile%Start MenuProgramsStartup

C:> %ProgramFiles%Startup

C:> dir C:WindowsStart MenuProgramsstartup

C:> dir "C:Users%username%AppDataRoamingMicrosoftWindowsStart MenuProgramsStartup"

C:> dir "C:ProgramDataMicrosoftWindowsStart MenuProgramsStartup"

C:> dir "%APPDATA%MicrosoftWindowsStart MenuProgramsStartup"

C:> dir "%ALLUSERSPROFILE%MicrosoftWindowsStart MenuProgramsStartup"

C:> dir "%ALLUSERSPROFILE%Start MenuProgramsStartup"

C:> type C:Windowswinstart.bat

C:> type %windir%wininit.ini

C:> type %windir%win.ini

C:> type C:Autoexec.bat"

6.2）使用 autoruns

C:> autorunsc -accepteula -m

6.3）自启动注册表位置

HKEY_CLASSES_ROOT:

C:> reg query HKCRComfileShellOpenCommand

C:> reg query HKCRBatfileShellOpenCommand

C:> reg query HKCRhtafileShellOpenCommand

C:> reg query HKCRExefileShellOpenCommand

C:> reg query HKCRExefilesShellOpenCommand

C:> reg query HKCRpiffileshellopencommand

HKEY_CURRENT_USERS:

C:> reg query "HKCUControl PanelDesktop"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionPoliciesExplorerRun"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionRun"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionRunonce"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionRunOnceEx"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionRunServices"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionRunServicesOnce"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionWindowsRun"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionWindowsLoad"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionWindowsScripts"

C:> reg query "HKCUSoftwareMicrosoftWindowsNTCurrentVersionWindows" /f run

C:> reg query "HKCUSoftwareMicrosoftWindowsNTCurrentVersionWindows" /f load

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionPoliciesExplorerRun"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerRecentDocs"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerComDlg32LastVisitedMRU"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerComD1g32OpenSaveMR

U"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerComDlg32LastVisitedPidlMRU"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerComD1g32OpenSavePidlMRU" /s

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerRunMRU"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerShell Folders"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerUser Shell Folders"

C:> reg query "HKCUSoftwareMicrosoftWindowsCurrentVersionAppletsRegEdit" /v LastKey

C:> reg query "HKCUSoftwareMicrosoftInternetExplorer" TypedURLs

C:> reg query "HKCUSoftwarePoliciesMicrosoftWindowsControlPanelDesktop"HKEY_LOCAL_MACHINE:

C:> reg query "HKLMSOFTWAREMicrosoftActive SetupInstalled Components" /s

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionexplorerUser Shell Folders"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionexplorerShell

Folders"

C:> reg query "HKLMSoftwareMicrosoftWindowsCurrentVersionexplorerShellExecuteHooks"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionExplorerBrowser Helper Objects" /s

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerRun"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionRunonce"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionRunOnceEx"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionRunServices"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionRunServicesOnce"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionWinlogonUserinit"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsCurrentVersionshellServiceObjectDelayLoad"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsNTCurrentVersionScheduleTaskCacheTasks" /s

C:> reg query "HKLMSOFTWAREMicrosoftWindowsNTCurrentVersionWindows"

C:> reg query "HKLMSOFTWAREMicrosoftWindowsNTCurrentVersionWindows" /f Appinit_DLLs

C:> reg query "HKLMSOFTWAREMicrosoftWindowsNTCurrentVersionWinlogon" /f Shell

C:> reg query "HKLMSOFTWAREMic rosoftWindowsNTCurrentVersionWinlogon" /f Userinit

C:> reg query "HKLMSOFTWAREPoliciesMicrosoftWindowsSysternScripts"

C:> reg query "HKLMSOFTWAREClassesbatfileshellopencornrnand"

C:> reg query "HKLMSOFTWAREClassescornfileshellopencornrnand"

C:> reg query "HKLMSOFTWAREClassesexefileshellopencommand"

C:> reg query "HKLMSOFTWAREClasseshtafileShellOpenCommand"

C:> reg query "HKLMSOFTWAREClassespiffileshellopencommand"

C:> reg query "HKLMSOFTWAREWow6432NodeMicrosoftWindowsCurrentVersionExplorerBrowser Helper Objects" /s

C:> reg query "HKLMSYSTEMCurrentControlSetControlSessionManager"

C:> reg query "HKLMSYSTEMCurrentControlSetControlSessionManagerKnownDLLs"

C:> reg query "HKLMSYSTEMControlSet001ControlSessionManagerKnownDLLs"

7.）取日志文件

C:> wevtutil epl Security C:bakSecurity-logs.evtx

C:> wevtutil epl System C:bakSystem-logs.evtx

C:> wevtutil epl Application C:bakApplication-logs.evtx

8.）文件、目录、共享信息

C:> net use 目标 IP

C:> net share

C:> net session

C:> wmic volume list brief

C:> wmic logicaldisk get description,filesystem,name,size

C:> wmic share get name,path

查找多个类型的文件或某个文件

C:> dir /A /S /T:A *.exe *.dll *.bat *.PS1 *.zip

C:> dir /A /S /T:A evil.exe

查找 2017/1/1 之后创建的文件

C:> forfiles /p C: /M *.exe /S /D +2017/1/1 /C "cmd /c echo @fdate @ftime @path"

C:> for %G in (.exe, .dll, .bat, .ps) do forfiles -p "C:" -m *%G -s -d +2017/1/1 -c "cmd

/c echo @fdate @ftime @path"

查找文件大小>20MB 的文件

forfiles /S /M * /C "cmd /c if @fsize GEQ 2097152 echo @path @fsize"

在 Alternate Data Streams 中查找文件

C:> streams -s 文件或目录

检查数字签名，vt 扫描

C:> sigcheck -e -u -vr -s C:

C:> listdlls.exe -u# 扫描病毒

C:> "C:Program FilesWindows DefenderMpCmdRun.exe" -SignatureUpdate

C:> "C:Program FilesWindows DefenderMpCmdRun.exe" -Scan “

5.4.2 LINUX 篇

1.）系统信息

uname -a

uptime

timedatectl

mount

2.）用户信息

Wlastlog　last

faillog -a

cat /etc/passwd

cat /etc/shadow

cat /etc/group

cat /etc/sudoers

查找 UID 为 0 的用户

awk -F:　'($3 == "0") {print}' /etc/passwd

egrep ':0+' /etc/passwd

cat /root/.ssh/authorized_keys

lsof -u root

cat /root/.bash_history

3.）网络信息

查看网络接口

ifconfig OR ip a l

查看监听端口

netstat -tupnl

查看网络连接

netstat -tupnlanetstat -tupnlax

路由信息

route OR netstat -r OR ip r l

ARP 表

arp -ne

监听端口的进程

lsof -i

4.）服务信息

列出所有进程

ps aux OR ps -ef

已加载内核模块

lsmod

打开的文件

lsof

lsof -c sshd

lsof -p PID

lsof -nPi | cut -f1 -d" " | uniq | tail -n +2

监控日志

less +F /var/log/messages

tail -F /var/log/messages

journalctl -u ssh.service -f

列出所有服务

chkconfig –list

systemctl list-units

5.）策略、补丁、环境变量信息

检查 pam.d 目录相关文件

cat /etc/pam.d/common*

自启动信息 – 计划任务

crontab -l

crontab -u root -l

cat /etc/crontab

ls /etc/cron,*

6.）命令历史

cat /root/.*history

7.）文件、目录、共享信息

df -ah

ls -lhcta /etc/init.d/

stat -x filenamefile

filename

特殊属性文件

lsattr -R / | grep "-i-"

全局可写文件

find / -xdev -type d (-perm -0002 -a ! -perm -1000) -print

某时间点之后新建的文件

find / -newermt 2018-01-22q

打印文件的所有属性信息

find /labs -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%pn"

查看文件的元数据 stat 文件名

8.）简单基线检查

wget

https://raw.githubusercontent.com/pentestmonkey/unix-privesc-check/1_x/unix-p

rivesc-check && ./unix-privesc-check > output.txt

9.）检测 rootkit

chkrootkit

rkhunter –update && rkhunter -check

tiger && less /var/log/tiger/security.report.*

lynis && lynis audit system && more /var/logs/lynis. log

10.) Fastir Collector Linux，收集 artefacts，包括：内核版本、内核模块、网卡、系统版本、主机名、登录、网络连接、SSH know_host、日志文件、进程数据、自启动等信息

wget

https://raw.githubusercontent.com/SekoiaLab/Fastir_Collector_Linux/master/fastIR_collector_linux.py

python fastIR_collector_linux.py –debug –output_dir output

11.) Sysdig and Sysdig Falco 行为监控

观察 root 用户查看过的目录

sysdig -p"%evt.arg.path" "evt.type=chdir and user.name=root"

观察 SSHD 行为

sysdig -A -c echo_fds fd.name=/dev/ptmx and proc.name=sshd

id 为 5459 的登录 shell 执行过的所有命令

sysdig -r trace.scap.gz -c spy_users proc.loginshellid=5459

安装，启动 falco

curl -s https://s3.amazonaws.com/download.draios.com/DRAIOS-GPG-KEY.public | apt-key add -curl -s -o /etc/apt/sources.list.d/draios.list http://download.draios.com/stable/deb/draios.list

sudo apt update

apt -y install falco

modprobe sysdig-probe

service falco start

falco

5.4.2 病毒样本分析

```
# 静态分析
# 挂载 Sysinternals 工具集
live.sysinternals.comtools
# 检查数字签名
C:> sigcheck.exe -u -e C:malware
C:> sigcheck.exe -vt malware.exe
# 16 机制和 ASCII 方式查看 PE 文件
hexdump -C -n 500 malware.exe
od -x mailware.exe
xxd malware.exe
strings -a malware.exe | more
# 内存镜像分析
python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 malfind -D
/output
python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 malfind -p PID
-D /output
python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 pslist
python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 pstree
```

python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 dlllist

python vol.py -f malware_memory_dump.raw -profile=Win7SPFix64 dlldump -D /output

HASH 分析

curl -v －request POST －url https://www.virustotal.com/vtapi/v2/file/report' -d apikey=VT API KEY -d 'resource=样本文件 hash'

curl -v -F 'file=malware.exe' -F apikey=VT API KEY>https://www.virustotal.com/vtapi/v2/file/scanwhois -h hash,cymru.com 样本文件 hash

获取磁盘和内存镜像

WINDOWS

C:> psexec.exe IP -u <DOMAIN>administrator -p 123 -c mdd_l.3.exe –o C:memory.dmp

C:> dc3dd.exe if=.c: of=d:diskiamge.dd hash=md5 log=d:output.log

LINUX

dd if=/dev/fmem of=/tmp/mem_dump.dd

使用 LiME

get https://github.com/504ensicslabs/LiME/archive/master.zip

unzip master.zip

cd LiME-master/src

make

```
cp lime-*.ko /media/USB/

insmod lime-3.13.0-79-generic.ko "path=/media/USB/mem_dump.lime format=
raw"

# 从内存中拷贝 PE 文件

cp /proc/进程 ID/exe /output

# 创建进程 core dump

gcore 进程 ID

strings -a gcore.* | more

dd if=/dev/sda of=/root/sda.dd

dd if=/dev/sda | ssh root@RemoteIP "dd of=/root/sda.dd"

# 通过 netcat 传送接收镜像文件

bzip2 -c /dev/sda | nc 8.8.8.8 53

nc -p 53 -l | bzip2 -d | dd of=/root/sda.dd
```

6. 常用技巧和工具

6.1 技巧

6.1.1 WINDOWS 系统篇

```
# 将命令结果通过管道输出到粘帖板，然后将粘帖板的内容重定向到文件

C:> some_command.exe | clip

PS C:> Get-Clipboard > clip.txt
```

检查注册表某路径是否存在

PS C:> Test-Path "HKCU:SoftwareMicrosoft123"

可靠文件复制

robocopy c:src 目标计算机 dst /E

检查某目录是否存在 ps1,vbs 扩展的文件

PS C:> Test-Path C:ScriptsArchive* -include *.ps1, *.vbs

合并多个文件

C:> type 1.txt 2.txt > output.txt

多个桌面窗口（Desktops）

C:>"%ProgramFiles%Internet Exploreriexplore.exe"

https://live.sysinternals.com/desktops.exe

在远程计算机执行命令

C:> psexec.exe 远程计算机 -u admin -p 123 /c c:123.exe

PS C:> Invoke-Command -远程计算机 { ls }

比较两个文件的差异

PS C:> Compare-Object (-Content 1.log) -DifferenceObject (Get-Content 2.log)

进制转换与编码

C:> set /a 0xff

PS C:> 0xff

C:> certutil -decode BASE64 编码文件 output.file

解码 XOR，搜索关键字：http

C:> xorsearch.exe -i -s input.file http

6.1.2 LINUX 系统篇

1.)SNORT

通过 ssh 在远程服务器上抓包

ssh root@8.8.8.8 tcpdump -i any -U -s 0 -w – 'not port 22'

SNORT 规则检测 Meterpreter

Snort rules by Didier Stevens (http://DidierStevens.com)

alert tcp HOME_NET any -> EXTERNAL_NET HTTP_PORTS (msg:"Metasploit Meterpreter"; flow:to_server,established; content:"RECV"; http_client_body; depth:4; fast_pattern; isdataat:!0,relative; urilen:23<>24,norm; content:"POST"; pcre:"/^/[a-z0-9]{4,5}_[a-z0-9]{16}//Ui"; classtype:trojan-activity; reference:url,blog.didierstevens.com/2015/05/11/detecting-network-traffic-from-metasploits-meterpreter-reverse-http-module/; sid:1618008; rev:1;)

https://didierstevens.com/files/software/snort-rules-V0_0_1.zip

SNORT 规则检测 PSEXEC

alert tcp HOME_NET any -> HOME_NET [139,445] (msg:"POLICY-OTHER use of psexec remote administration tool"; flow:to_server,established; content:"|FF|SMB|A2|"; depth:5; offset:4; content:"|5C 00|p|00|s|00|e|00|x|00|e|00|c|00|s|00|v|00|c"; nocase; metadata:service netbios-ssn; reference:url,technet.microsoft.com/en-us/sysinternals/bb897553.aspx; classtype:policy-violation; sid:24008; rev:1;)

alert tcp HOME_NET any -> HOME_NET [139,445] (msg:"POLICY-OTHER use of psexec remote administration tool SMBv2"; flow:to_server,established; content:"|FE|SMB"; depth:8; nocase; content:"|05 00|"; within:2; distance:8; content:"P|00|S||E|00|X|00|E|00|S|00|V|00|C|00|"; fast_pattern:only; metadata:service netbios-ssn;

reference:url,technet.microsoft.com/en-us/sysinternals/bb897553.aspx;

classtype:policy-violation; sid:30281; rev:1;)

2.) Bro NSM

检测横向渗透

wget

https://raw.githubusercontent.com/richiercyrus/Bro-Scripts/master/detect-mal-smb-files.bro

bro -r faf-exercise.pcap detect-mal-smb-files.bro

less notice.log

检测勒索软件

wget

https://raw.githubusercontent.com/fox-it/bro-scripts/master/smb-ransomware/smb-ransomware.bro

bro -r faf-exercise.pcap smb-ransomware.bro

3.) 检测 DOS/DDOS

检测攻击类型 SYN Flood，ICMP Flood，UDP Flood

tshark -r 001.pcap -q -z io,phs

tshark -c 1000 – -z io,phs

tcpdump -tnr $ | awk -F '.' '{print $1"."$2"."$3"."$4}' | sort | uniq -c | sort -n | tail

tcpdump -qnn "tcp[tcpflags] & (tcp-syn) != 0"

netstat -s

tcpdump -nn not arp and not icmp and not udp

netstat -n | awk '{print $6}' | sort | uniq -c | sort -nr | head

应用层

tshark -c 10000 -T fields -e http.host | sort | uniq -c | sort -r | head -n 10

tshark -r capture6 -T fields -e http.request.full_uri | sort | uniq -c | sort -r | head -n 10c

tcpdump -n 'tcp[32:4] = 0x47455420' | cut -f 7- -d":"

查找 http 请求中包含：GIF,ZIP,JPEG,PDF,PNG 扩展的数据包

tshark -Y "http contains "ff:d8"" || "http contains "GIF89a"" || "http contains "x50x4Bx03x04"" || "http contains "xffxd8"" || "http contains "%PDF"" || "http contains "x89x50x4Ex47""

取'user-agent'和 refer 字段

tcpdump -c 1000 -Ann I grep -Ei 'user-agent' | sort | uniq -c | sort -nr | head -1

tcpdump -i en0 -A -s 500 | grep -i refer

第二层攻击

tcpdump 'arp or icmp'

tcpdump -tnr 001.pcap ARP | awk -F '.' '{print 1"."2"."3"."4}' | sort | uniq -c | sort -n |

tail

tshark -r 001.pcap -q -z io,phs | grep arp.duplicate-address-detected

6.2 兵器谱

1.）KALI 渗透测试发行版

https://www.kali.org

2.）SIFT SANS 取证工具箱

http://sift.readthedocs.org/

3.）REMNUX 软件逆向和病毒分析发行版

https://remnux.org

4.) OPENVAS

http://www.openvas.org

5.) Security Onion 入侵检测、网络安全监控、日志分析发行版

https://securityonion.net

6.）OSSEC 开源主机入侵检测系统

http://ossec.github.io

0x4　参考

https://www.4hou.com/technology/10173.html

https://github.com/fu4ck/btfm