



2022

可视化网络领导者

**网络安全攻防演习，准备好了吗？**

北京派网软件有限公司



# 目录

01

网络安全攻防演习简介

02

梳理资产，减少暴露面

03

如何溯源给防守方加分

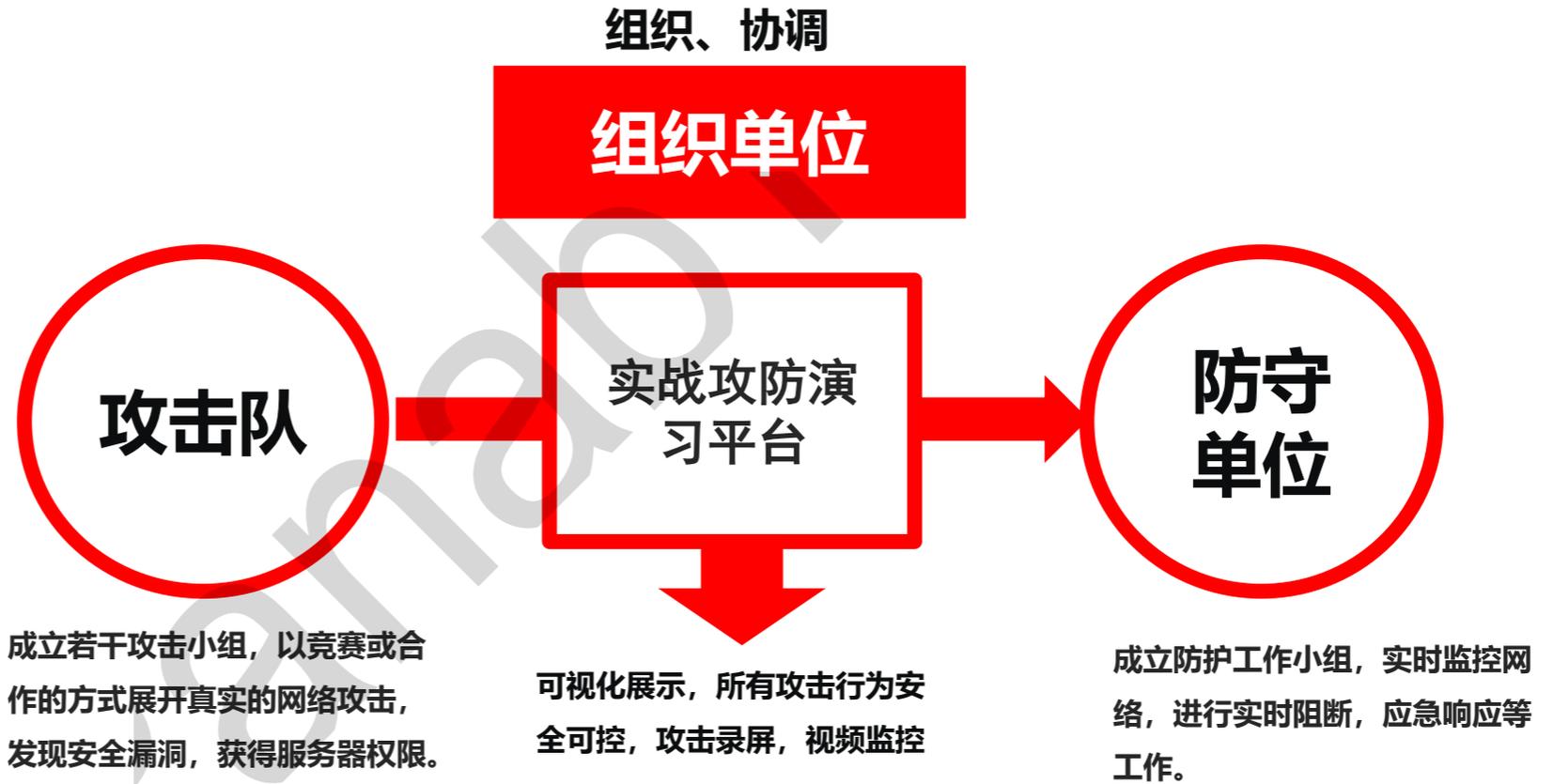


01

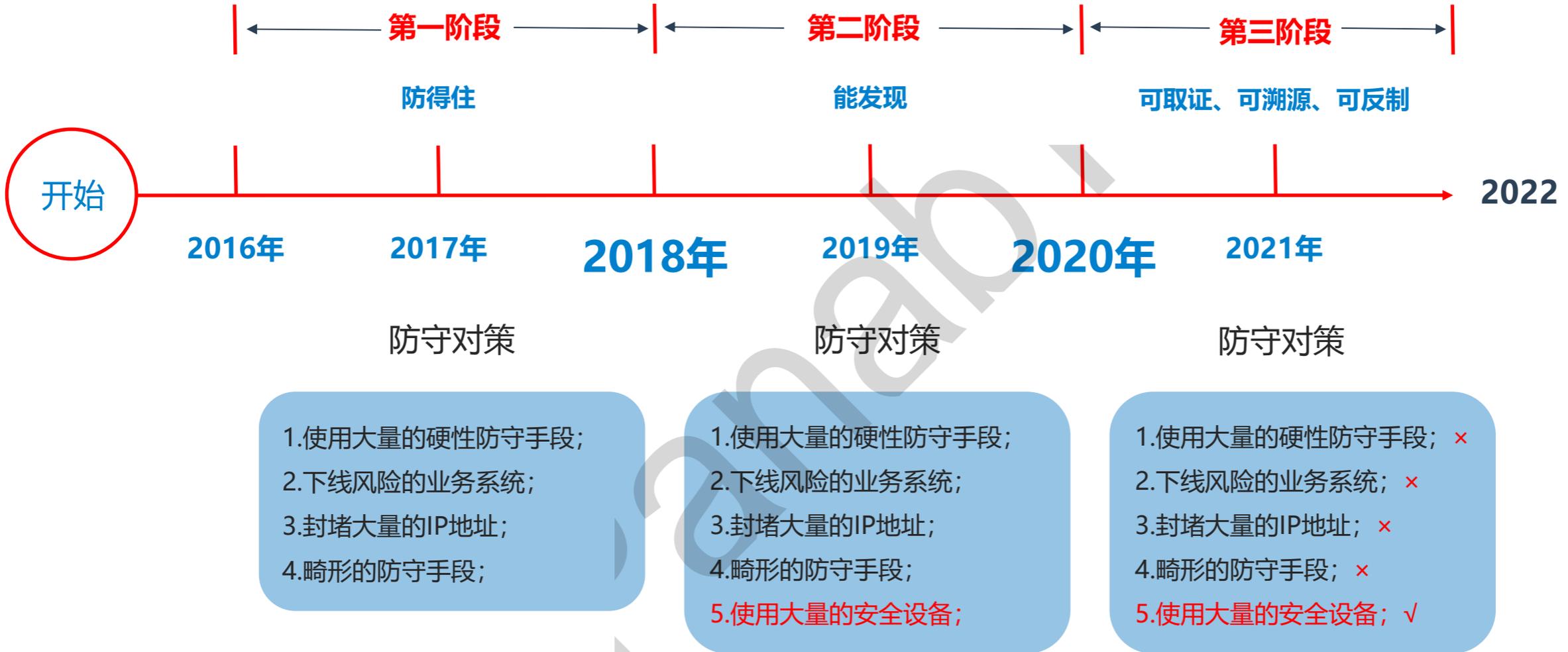
## 网络安全攻防演习简介

## 攻防演习

攻防演习通常是真实网络环境下对参演单位目标系统进行**全程可控、可审计的实战攻击**，拟通过演练检验参演单位的安全防护和应急处置能力，提高网络安全的综合防控能力。



# 攻防演习的三个阶段



## 教育部司局函件

教科信司〔2022〕54号

### 教育部科学技术与信息化司关于开展2022年教育系统网络安全攻防演习的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，有关高校，基础教育司、职业教育与成人教育司、教育部教育技术与资源发展中心、教育部教育管理信息中心、全国学生资助管理中心、教育部学生服务与素质发展中心、高等教育出版社：

根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》和《教育系统网络安全事件应急预案》，现定于4月至6月开展2022年教育系统网络安全攻防演习。现将有关事项通知如下。



**演习时间：5月9日-5月22日**

## 攻击方 常用手段

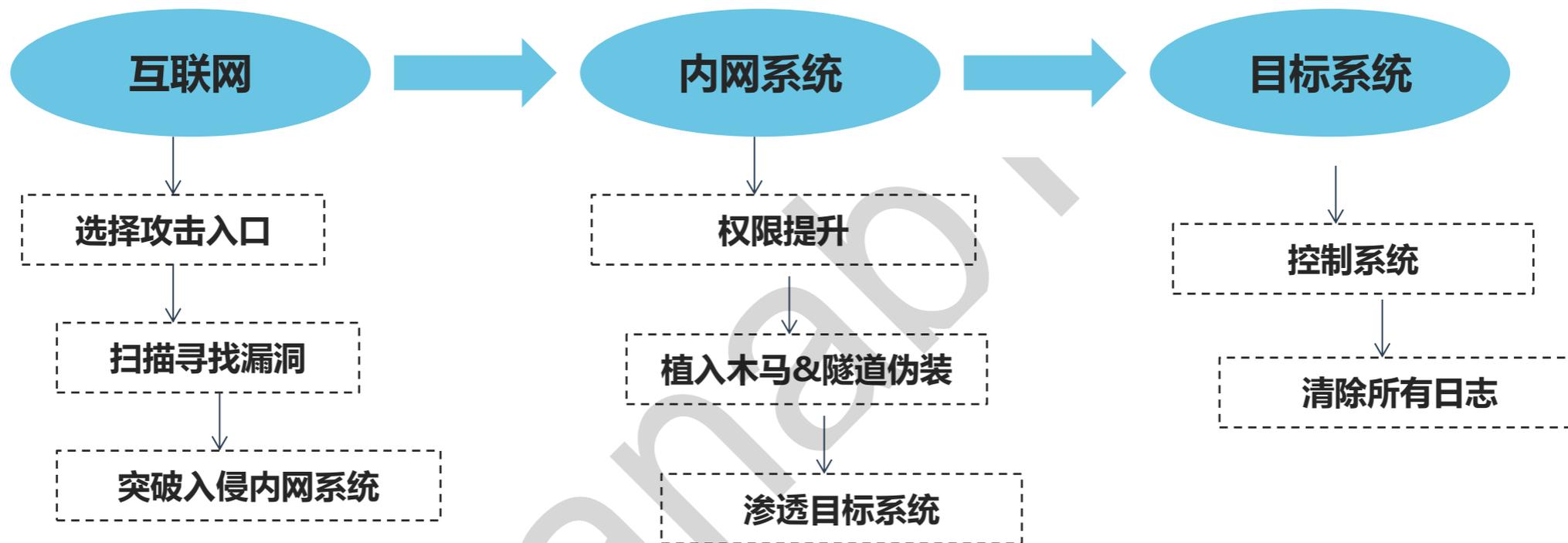
**探测**：通过扫描，暴力破解，钓鱼，嗅探等方式发现防守方的漏洞和弱点。

**攻击**：利用掌握的漏洞进行渗透攻击，同时，为了避免被IPS、WAF等安全设备拦截，会进行**伪装**，**加壳**等操作。

**渗透**：通过受控主机进行权限提升，**后门软件**等方式获得完全控制权，然后以这台主机为跳板，渗透内网。

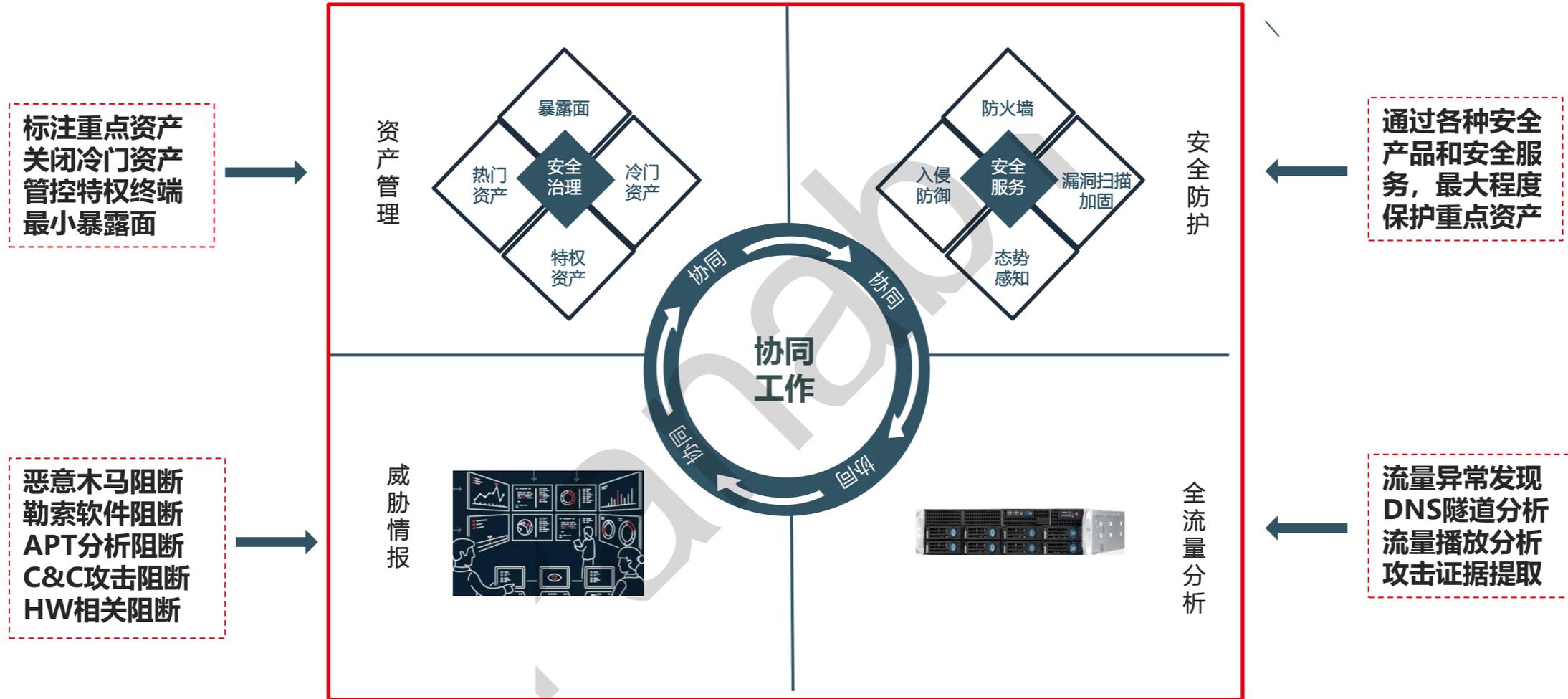
**伪装**：通过**DNS隧道等手段**欺骗安全设备进行伪装，达到持续渗透目的，同时删除操作日志。





**互联网突破口选择原则：选择防护意识薄弱系统，存在高危漏洞系统，第三方供应商，运维服务供应商，新型应用架构业务系统等。**

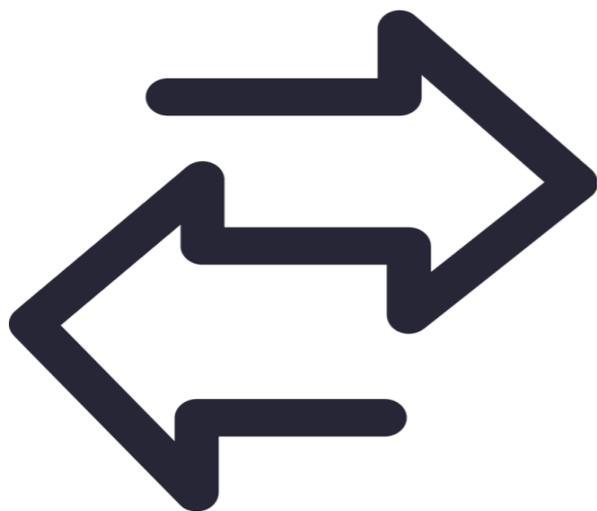
# 网络安全攻防演习— 防守方思路





02

梳理资产，减少暴露面



**方向1：互联网访问校内资产**

**方向2：校内资产访问互联网**

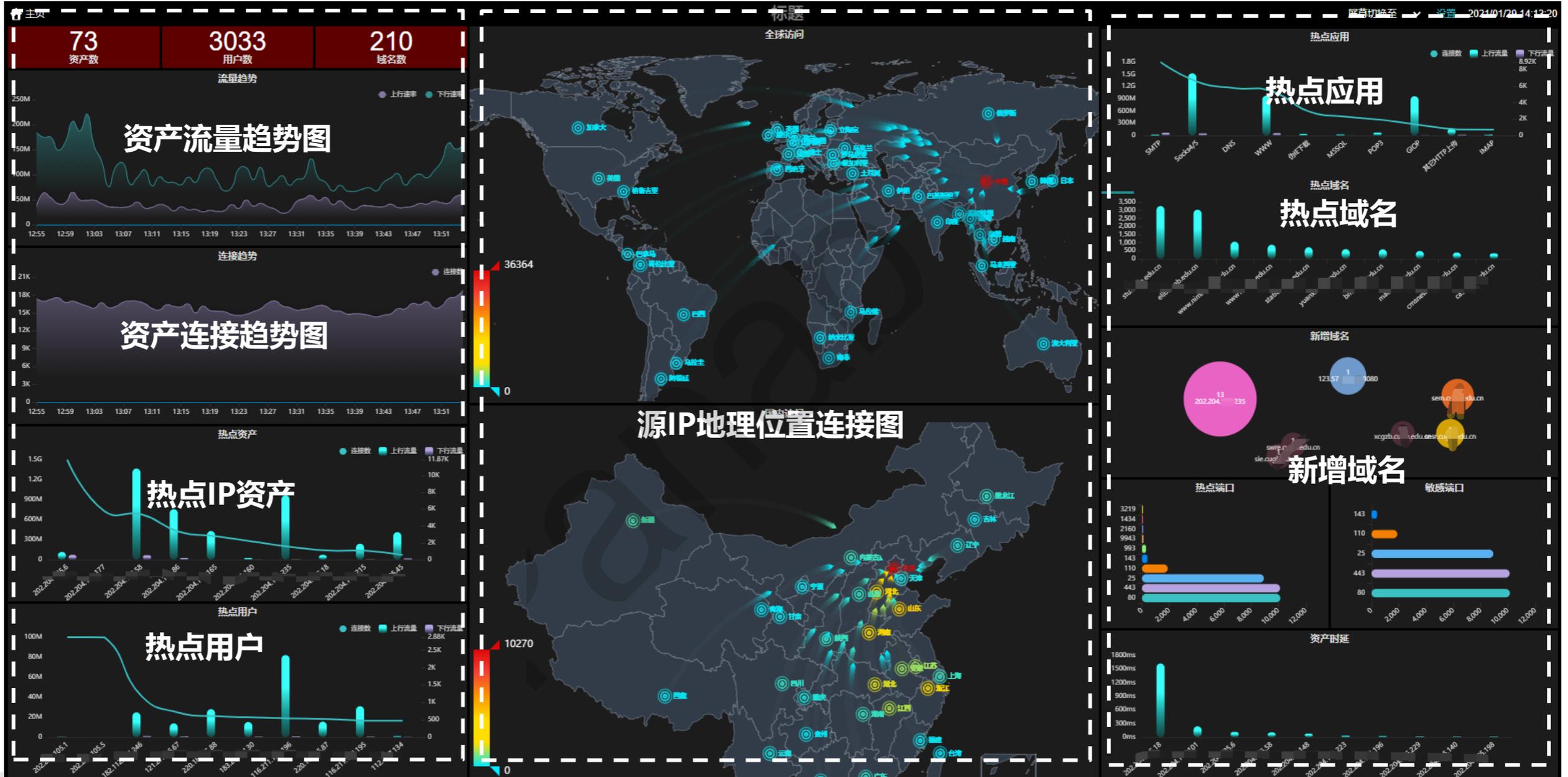
## 意义

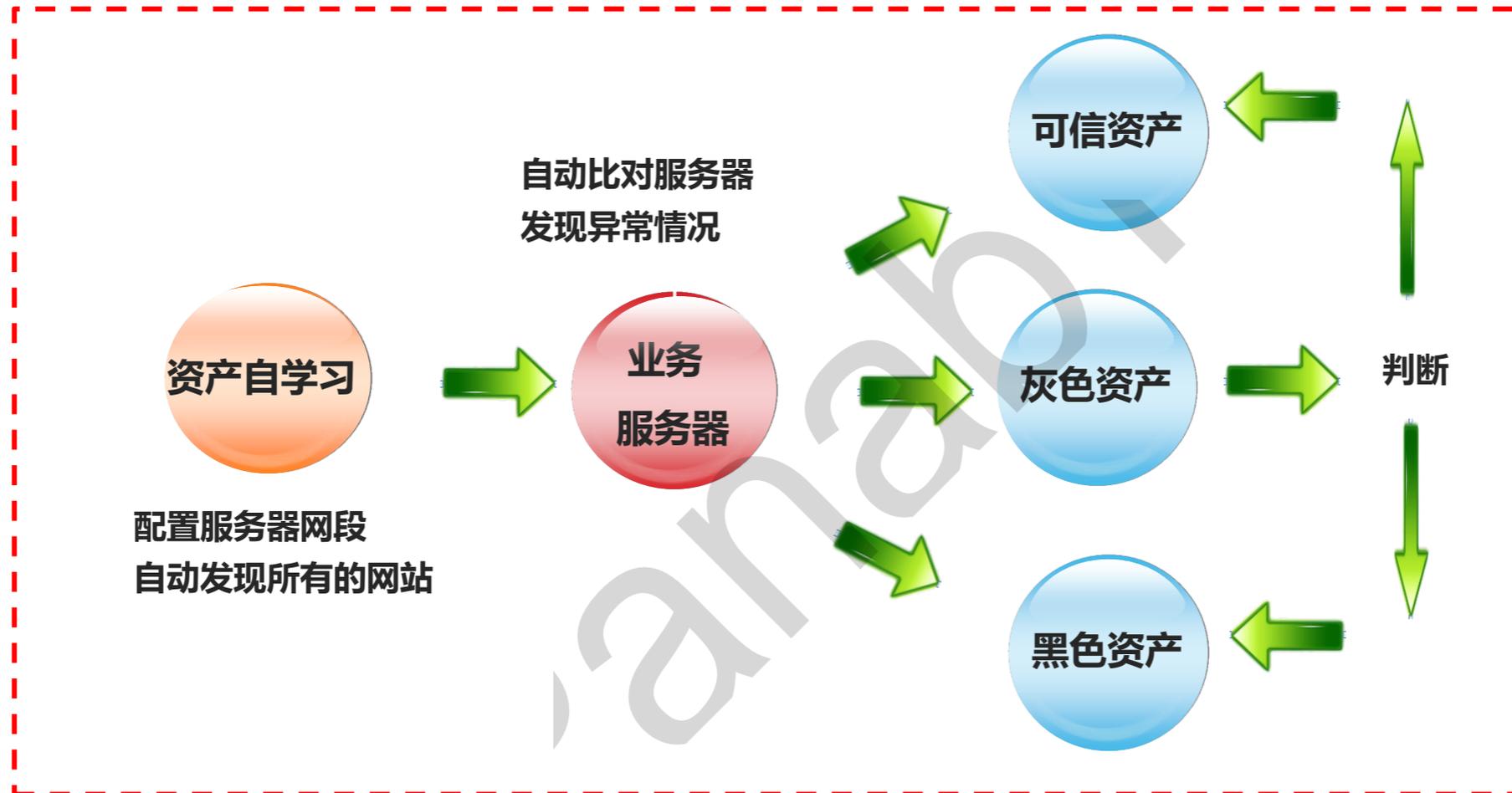
检测资产暴露面，及时发现暴露资产，确保资产暴露最小化。

## 作用：

网络攻防演习是针对于**全程可控、可审计**的实战攻击。因此，做好资产梳理，达到资产暴露最小化目的，便于我们下一步的监控和审计。

通过主动或者被动方式，**发现**目前对外暴露的所有资产，然后进行最小化暴露**管控**。





**作用：**检测资产暴露面，及时发现暴露资产，确保资产暴露最小化。

# 资产管理—资产分析



序号	域名	总请求次数	DNS请求次数	HTTP请求次数	HTTPS请求次数	HTTP20x	HTTP30x	HTTP40x	HTTP50x
1	www.t.edu.cn	172352	63338	108926	88	105583	514	2722	0
2	service.t.edu.cn	161110	1130	159833	147	158293	959	549	0
3	auth.t.edu.cn	141369	1057	140224	88	17768	122315	103	0
4	jwgl.t.edu.cn	36334	512	5201	30621	0	5199	1	0
5	apiucloud.t.edu.cn	35796	406	34932	458	32923	0	1956	3
6	ucloud.t.edu.cn	24028	904	22235	889	18476	3360	384	0
7	huorong.t.edu.cn	13593	4044	119	9430	119	0	0	0
8	yjxt.t.edu.cn	12960	7258	5702	0	4704	495	43	150
9	360.t.edu.cn	12117	1228	10889	0	270	10554	51	0
10	oa.t.edu.cn	9293	138	9022	133	6321	10	2690	0
11	teac.t.edu.cn	8514	242	3	3	4914	325	214	2383
12	news.t.edu.cn	8216	3212	5002	2	3729	261	1011	0
13	imgservice.t.edu.cn	7433	434	6990	9	6924	36	27	0
14	reservation.t.edu.cn	6369	559	5790	20	3986	1796	0	0
15	zsb.t.edu.cn	6072	86	5984	2	5402	25	556	0
16	scs.t.edu.cn	5877	114	5762	1	4392	575	795	0
17	my.t.edu.cn	5510	951	4559	0	2825	1377	352	2
18	jwglweixin.t.edu.cn	5387	1030	4357	0	3806	446	104	0

资产热度排名

资产访问排名

资产状态码排名



**资产管理**

全局访问

用户非法访问

序号	用户名	协议	连接数	上行流量	下行流量
1	73.150.2.211	WWW	1	3	2
2	73.150.2.211	WWW	1	3	2
3	73.150.2.211	WWW	1	3	2
4	73.150.2.211	WWW	1	3	2
5	73.150.2.211	WWW	1	3	2
6	73.150.2.211	WWW	1	3	2
7	73.150.2.211	WWW	1	3	2
8	73.150.2.211	WWW	1	3	2
9	73.150.2.211	WWW	1	3	2
10	73.150.2.211	WWW	1	3	2
11	73.150.2.211	WWW	1	3	2
12	73.150.2.211	WWW	1	3	2
13	73.150.2.211	WWW	1	3	2
14	73.150.2.211	WWW	1	3	2
15	73.150.2.211	WWW	1	3	2
16	73.150.2.211	WWW	1	3	2
17	73.150.2.211	WWW	1	3	2
18	73.150.2.211	WWW	1	3	2
19	73.150.2.211	WWW	1	3	2
20	73.150.2.211	WWW	1	3	2
21	73.150.2.211	WWW	1	3	2
22	73.150.2.211	WWW	1	3	2
23	73.150.2.211	WWW	1	3	2
24	73.150.2.211	WWW	1	3	2
25	73.150.2.211	WWW	1	3	2
26	73.150.2.211	WWW	1	3	2
27	73.150.2.211	WWW	1	3	2
28	73.150.2.211	WWW	1	3	2
29	73.150.2.211	WWW	1	3	2
30	73.150.2.211	WWW	1	3	2
31	73.150.2.211	WWW	1	3	2
32	73.150.2.211	WWW	1	3	2
33	73.150.2.211	WWW	1	3	2
34	73.150.2.211	WWW	1	3	2
35	73.150.2.211	WWW	1	3	2
36	73.150.2.211	WWW	1	3	2
37	73.150.2.211	WWW	1	3	2
38	73.150.2.211	WWW	1	3	2

关闭

热点应用

00

00

00

00

## 资产非授权访问告警

1. 定义资产访问白名单。  
例如：某台服务器只允许HTTPS访问
2. 如果有白名单外的访问，在资产大屏上就可以自动告警。

## 作用

通过该功能可以第一时间发现攻击方的扫描和探测，然后锁定攻击方的IP地址。便于我们下一步作出防御和事后取证。

中国电信 4G 中国移动 59% 下午3:28

## 一键断网

+ 添加 - 删除 ↻ 刷新 ⏻ 退出

对象	操作
<b>资源对象: oa.abc.wdu.cn</b> 简要说明: OA服务器 系统编码: wp2018072510 系统名称: <input type="checkbox"/>	联网
<b>资源对象: www.abc.edu.cn</b> 简要说明: 主页服务器 系统编码: wp2018072510 系统名称: <input type="checkbox"/>	断网

对象列表 登录日志 操作日志

中国电信 4G 中国移动 51% 晚上8:45

## Panabit

操作已执行通知  
4月22日

您好, 执行后的结果如下:

设备名称: 一键断网  
操作名称: allow=host host=oa.abc.wdu.cn device=wp2018072510  
操作结果: 发送设备=0,成功设备=0,失败设备=0  
操作时间: 2019-04-22 15:53:46

提示: 此命令只更新“云平台禁止上网IP”群组和“云平台禁止上网域名”群组。并生成策略ID号为1的阻断策略

序号	用户	操作时间	内容
1		2019/04/25 09:25:20	联网 设备/TEST11111111 对象/www.abc.cn 用户/c
2		2019/04/24 16:09:44	断网 设备/TEST11111111 对象/www.abc.cn 用户/c
3		2019/04/22 15:54:24	断网 设备/wp2018072510 对象/www.abc.edu.cn 用
4		2019/04/22 15:53:36	联网 设备/wp2018072510 对象/oa.abc.wdu.cn 用
5		2019/04/22 15:51:55	联网 设备/wp2018072510 对象/www.abc.edu.cn 用
6		2019/04/22 15:50:52	断网 设备/wp2018072510 对象/www.abc.edu.cn 用

## 资产管控

在出口网关出, 对互联网访问内网资产进行管控, 关闭不必要的IP地址和端口, 确保最小化暴露。

对于临时发现的暴露资产, 可以通过微信“一键断网”进行快速关停。



**方向1：** 互联网访问校内资产

**方向2：** 校内资产访问互联网

自动刷新	10秒	排序方式	连接数	主机组	所有组	关键字搜索		+ 添加	导入	导出	列表	分离	卡片
统一身份认证系统				主页服务器				网上服务大厅					
477	37	0	22.04 ms	329	2166	0	2.78 ms	319	99	0	49.84 ms		
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延		
5.66K	229.93K	2.57M	103.56M	56	21.64M	11.97M	4.21G	338	419.63K	505.29M	120.97G		
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量		
OA服务器				就业系统				教学云主页					
221	151	0	26.40 ms	186	20	0	18.82 ms	106	811	0	4.70 ms		
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延		
2.20K	1.47M	503.77K	214.39M	870	175.58K	1.15M	34.16M	8.35M	128.74K	325.80G	66.97G		
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量		
教务管理系统				资产管理系统				招生系统					
100	8	0	9.70 ms	50	69	2	89.15 ms	21	0	0	5.65 ms		
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延		
1.12K	22.86K	844.11K	17.50M	79.96K	107.96K	767.03M	1.46G	0	0	0	21.45M		
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量		

HW系统Dashboard，可随时查看网络攻防演习系统的连接数、失败率、时延、流量等信息。

实时分析 历史分析

 流入速率 9.78K	 流出速率 1.44M	 PPS 168	连接数 610	 失败率 0%	平均时延 13.76 ms	 流入流量 109.88M	流出流量 5.15G
---	---	--	------------	---	------------------	---	---------------

流量概况 性能概况 协议概况 当前连接

应用	协议	连接	地理位置	时长	客户时延	服务时延	应用时延	上行报文	下行报文	最大包长	流量	HOST	操作
其它HTTP上传	tcp	源: 3.8.162:65254 目: 3.55.244:8081		1	0.11	0.54	13.85	6/12	1/2	1468/702	15218/1404	auth. edu.cn 3...	<a href="#">数据包</a>
WWW	tcp	源: 3.8.162:25666 目: 3.55.246:8081		1	0.06	0.68	1.32	1/2	811/1622	814/1468	1628/2379834	auth. edu.cn 2...	<a href="#">数据包</a>
WWW	tcp	源: 3.8.162:60854 目: 3.55.243:8081		1	0.05	0.32	4.53	1/2	2/4	548/502	1096/1810	auth. t.edu.cn 2...	<a href="#">数据包</a>
WWW	tcp	源: 3.240.159:21875 目: 3.9.161:80		1	0.07	0.05	5.14	1/2	2/4	472/514	944/1966	auth. b. edu.cn 2...	<a href="#">数据包</a>
WWW	tcp	源: 3.8.162:25646 目: 3.55.246:8081		1	0.06	0.74	1.52	1/2	1/2	791/547	1582/1094	auth. t.edu.cn 2...	<a href="#">数据包</a>
WWW	tcp	源: 3.8.162:65382 目: 3.55.244:8081		1	0.05	0.62	1.39	1/2	1/2	936/229	1872/458	auth. pt.edu.cn 3...	<a href="#">数据包</a>
iPhone	tcp	源: 3.8.162:60776 目: 3.55.243:8081		2	0.07	0.29	0.90	1/2	3/6	547/1468	1094/6446	auth. t.edu.cn 2...	<a href="#">数据包</a>
WWW	tcp	源: 3.8.162:25292 目: 3.55.246:8081		2	0.07	0.53	4.05	1/2	2/4	527/421	1054/1648	auth. t.edu.cn 2...	<a href="#">数据包</a>

可以随时查看HW系统的连接信息，发现异常行为。

## 会话流量

IP群组	HW系统	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	80 / 8000-8080	传输协议	任意	应用协议	终端控制		
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	请求域名					
时间范围	2022-05-04 10:49:51 - 2022-05-05 11:49:51		连接类型	所有									
<input type="checkbox"/> 请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传 <sup>i</sup>	下行重传 <sup>i</sup>	重置 <sup>i</sup>	流量 <sup>i</sup>	请求域名	状态	操作
<input type="checkbox"/> 2022-05-04/19:31:32	00-50-56-b...	3.244.211:55800	120.26.2.44:443	浙江杭州	BGP TCP	向日葵远控	0/5	0/10	0/0	1119/11970	client-api.or...		数据包
<input type="checkbox"/> 2022-05-04/20:31:56	00-50-56-8...	3.244.78:59637	114.215.172.2:443	浙江杭州	BGP TCP	向日葵远控	0/5	0/7	0/0	1177/6165	slapi.oray.net		数据包
<input type="checkbox"/> 2022-05-04/21:49:26	00-50-56-b...	55.69:63250	121.40.62.130:443	浙江杭州	BGP TCP	向日葵远控	0/5	2/11	0/0	1123/13186	client-api.or...		数据包
<input type="checkbox"/> 2022-05-04/22:31:32	00-50-56-b...	3.244.211:60257	120.26.2.44:443	浙江杭州	BGP TCP	向日葵远控	0/5	5/12	0/0	1119/14966	client-api.or...		数据包
<input type="checkbox"/> 2022-05-04/23:34:24	00-50-56-b...	3.240.129:58753	121.40.132.43:443	浙江杭州	BGP TCP	向日葵远控	0/128	0/129	0/0	49832/50140	sl-collection...		数据包
<input type="checkbox"/> 2022-05-05/00:52:10	00-50-56-b...	3.240.129:60991	101.37.202.149:443	浙江杭州	BGP TCP	向日葵远控	0/128	1/130	0/0	49832/50504	sl-collection...		数据包
<input type="checkbox"/> 2022-05-05/01:31:32	00-50-56-b...	3.244.211:64734	47.114.97.87:443	阿里云	TCP	向日葵远控	0/5	1/10	0/0	1119/11993	client-api.or...		数据包

可以随时基于终端控制类软件进行查询，发现HW系统产生终端控制的情况。

## 意义

及时发现非法连接，尤其是**伪装的隧道**通讯。

## 作用：

网络攻防演习过程中，攻击方会使用“0day”漏洞进行攻击。这些0day漏洞大多数是基于某个应用的，攻击方会利用这个漏洞上传**加壳的木马程序**，从而获得更多控制权限。为了躲避防火墙的阻断，这些木马采用端口反弹的模式，由服务器主动发起请求，对外进行连接。为了不引起注意和欺骗网络安全设备，很多连接是加密后通过UDP 53，TCP 443这些的端口完成。

如果我们可以**发现和阻断**这些伪装的加密隧道，也可以达到对内网资产保护的目的。

# 未知流量的秘密—真假DNS

会话流量

IP群组	HW系统	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	53	传输协议	UDP	应用协议	未知协议		
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	请求域名					
时间范围	2022-05-05 09:03:39 - 2022-05-05 10:03:39		连接类型	成功									
<input type="checkbox"/> 请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
<input type="checkbox"/> 2022-05-05/09:03:39	00-50-56-8...	3.210.30:57071	111.7.100.67:53	河南郑州...	UDP	未知应用	0/1	0/1	0/0	490/162	-		数据包
<input type="checkbox"/> 2022-05-05/09:03:40	00-50-56-8...	3.210.30:57072	111.7.100.67:53	河南郑州...	UDP	未知应用	0/1	0/1	0/0	490/162	-		数据包
<input type="checkbox"/> 2022-05-05/09:03:42	00-50-56-8...	3.210.30:57074	111.7.100.67:53	河南郑州...	UDP	未知应用	0/1	0/1	0/0	490/162	-		数据包
<input type="checkbox"/> 2022-05-05/09:03:42	00-50-56-8...	3.210.30:57073	111.7.100.67:53	河南郑州...	UDP	未知应用	0/1	0/1	0/0	490/162	-		数据包

Panabit 在协议识别上，不是看端口号，而是看应用层里面的内容，因此，可以发现网络中存在的假冒DNS、假冒HTTPS等流量，从而可以DNS隧道、HTTPS隧道等行为。

事务ID (Transaction ID)	标志 (Flags)
问题计数 (Questions)	回答资源记录数 (Answer RRs)
权威名称服务器计数 (Authority RRs)	附加资源记录数 (Additional RRs)
查询问题区域 (Queries)	
回答问题区域 (Answers)	
权威名称服务器区域 (Authoritative nameservers)	
附加信息区域 (Additional records)	

## DNS 的报文格式。

正常DNS 格式主要分为 3 部分内容，即基础结构部分、问题部分、资源记录部分。其中，事务 ID、标志、问题计数、回答资源记录数、权威名称服务器计数、附加资源记录数这 6 个字段是DNS的报文首部，共 12 个字节。

# 未知流量的秘密—真假DNS

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.9.4	114.114.114.114	DNS	100	Standard query 0x6bd5 A www.baidu.com OPT
2	0.028709	114.114.114.114	10.3.9.4	DNS	147	Standard query response 0x6bd5 A www.baidu.com

- > Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
- > Ethernet II, Src: 00:50:56:b5:2b:2c (00:50:56:b5:2b:2c), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)
- > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4009
- > Internet Protocol Version 4, Src: 10.3.9.4, Dst: 114.114.114.114
- > User Datagram Protocol, Src Port: 42666, Dst Port: 53
- √ Domain Name System (query)
  - Transaction ID: 0x6bd5
  - > Flags: 0x0120 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 1
  - √ Queries
    - > www.baidu.com: type A, class IN
  - > Additional records

正常的DNS 数据包

## 李逵 or 李鬼

基础结构里面包含，事务 ID、标志、问题计数、回答资源记录数、权威名称服务器计数、附加资源记录数这 6 个字段，共 12 个字节。

在每部分都有自己的定义，例如：在问题部分里面包含请求的域名信息。

# 未知流量的秘密—真假DNS

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	3.210.30	111.7.100.67	DNS	490	Standard query 0x0c0b [Malformed Packet]
2	0.016772	111.7.100.67	3.210.30	DNS	162	Standard query 0x0c0b [Malformed Packet]

> Frame 1: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)  
> Ethernet II, Src: 00:50:56:8a:87:ca (00:50:56:8a:87:ca), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4073  
> Internet Protocol Version 4, Src: 3.210.30, Dst: 111.7.100.67  
> User Datagram Protocol, Src Port: 57072, Dst Port: 53  
> Domain Name System (query)  
v [Malformed Packet: DNS]  
v [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]  
[Malformed Packet (Exception occurred)]  
[Severity level: Error]  
[Group: Malformed]

畸形的UDP 53数据包

李逵 or 李鬼

UDP 53数据包，都是DNS请求吗？

由于网络安全设备对UDP 53请求的数据包是放行的，因此，攻击方为了欺骗安全设备，通过UDP 53进行数据传输。

## 添加策略

### 匹配条件

### 执行动作

策略序号	<input type="text" value="100"/>	1~65535,序号小的优先匹配
策略备注	<input type="text" value="阻断DNS隧道"/>	
线路及流向	<input type="text" value="任意"/>	<input type="text" value="任意"/>
首包接口	<input type="text" value="em3"/>	
源接口	<input type="text" value="任意"/>	<input type="text" value="任意"/>
内网地址: 端口	<input type="text" value="IP群组"/>	<input type="text" value="HW系统"/>
外网地址: 端口	<input type="text" value="任意"/>	<input type="text" value="53"/>
协议	<input type="text" value="UDP"/>	<input type="text" value="未知协议"/>

80或80-8000,0表示任意端口

[选择协议](#)

### 管控策略:

对于HW系统访问外网地址的UDP 53端口的未知协议进行阻断操作

# 未知流量的秘密—真假HTTPS



会话流量

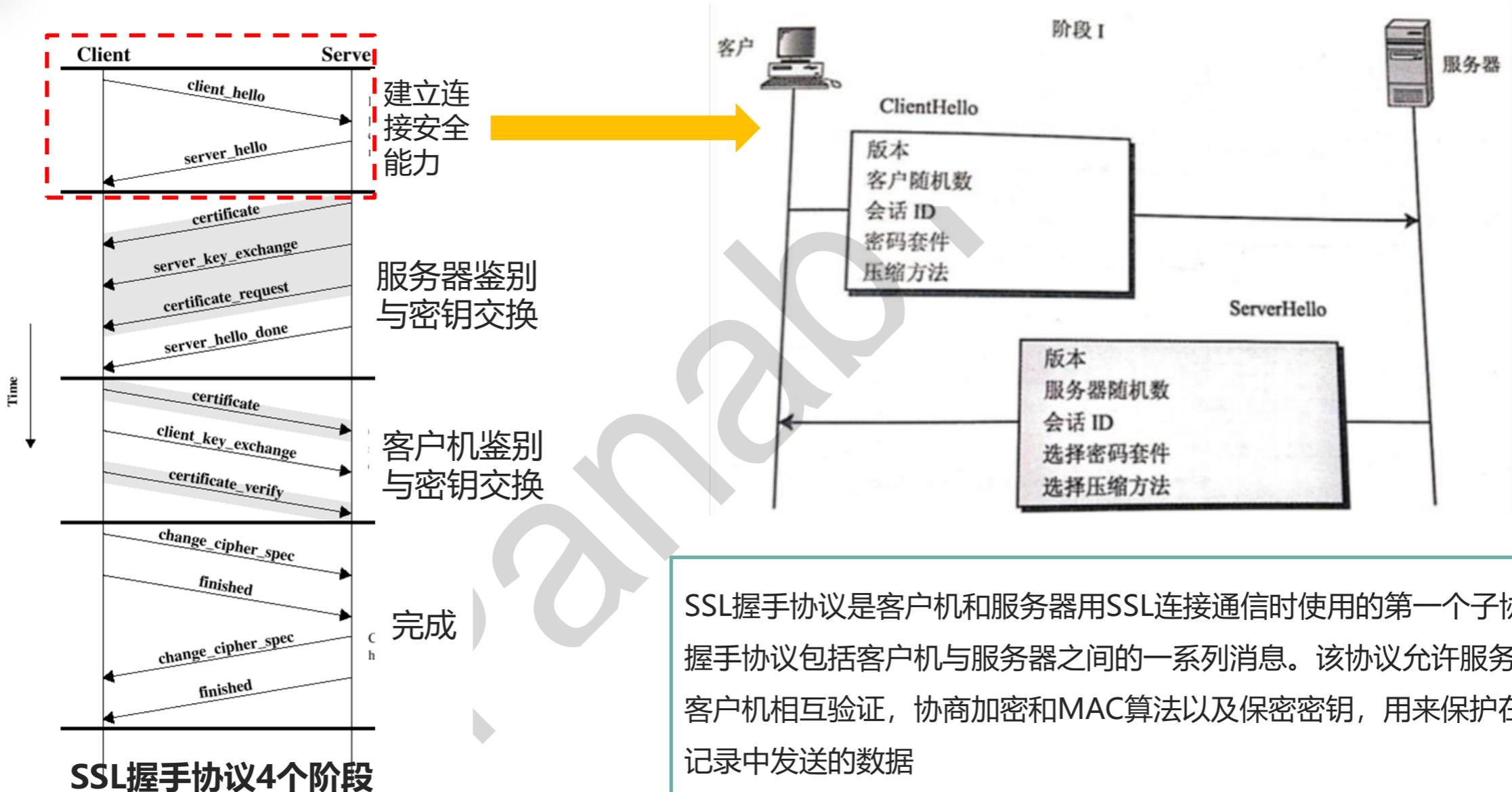
IP群组	HW系统	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	443	传输协议	TCP	应用协议	未知协议
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	国外	请求域名			
时间范围	2022-04-30 10:00:40 - 2022-05-01 11:00:40		连接类型	所有							

<input type="checkbox"/>	请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
<input type="checkbox"/>	2022-04-30/10:02:28	cc-d3-9d-9...	52.85:51193	40.90.184.82:443	新加坡	TCP	未知应用	0/0	0/0	1/0	0/3105	-		数据包
<input type="checkbox"/>	2022-04-30/10:02:28	cc-d3-9d-9...	52.85:51192	40.90.184.82:443	新加坡	TCP	未知应用	0/0	0/0	0/0	634/2936	-		数据包
<input type="checkbox"/>	2022-04-30/10:02:33	00-50-56-b...	9.30:59667	52.140.118.28:443	印度	TCP	未知应用	0/0	0/0	0/0	879/1059	-		数据包
<input type="checkbox"/>	2022-04-30/10:23:40	00-0c-29-c...	10.9:54300	208.91.0.89:443	美国	TCP	未知应用	0/0	0/0	0/0	410/1827	-		数据包
<input type="checkbox"/>	2022-04-30/10:04:53	00-50-56-b...	200.6:59067	52.139.250.253:443	新加坡	TCP	未知应用	6/47	1/46	1/0	6145/13846	-		数据包
<input type="checkbox"/>	2022-04-30/11:00:15	00-50-56-b...	181.86:3814	72.247.61.28:443	日本	TCP	未知应用	0/1	0/3	1/0	184/2141	-		数据包
<input type="checkbox"/>	2022-04-30/10:49:08	cc-d3-9d-9...	52.85:51225	20.44.10.122:443	美国	TCP	未知应用	0/0	0/0	0/0	1029/3710	-		数据包
<input type="checkbox"/>	2022-04-30/12:11:43	00-50-56-b...	9.75:51830	40.77.226.250:443	爱尔兰	TCP	未知应用	0/0	0/0	0/0	0/1246	-		数据包
<input type="checkbox"/>	2022-04-30/13:08:05	00-50-56-b...	181.92:51937	20.189.173.2:443	美国	TCP	未知应用	0/0	0/0	0/0	1029/109	-		数据包

Panabit 在协议识别上，不是看端口号，而是看应用层里面的内容，因此，可以发现网络中存在的假冒DNS、假冒HTTPS等流量，从而可以DNS隧道、HTTPS隧道等行为。

# 未知流量的秘密—真假HTTPS



SSL握手协议是客户机和服务器用SSL连接通信时使用的第一个子协议，握手协议包括客户机与服务器之间的一系列消息。该协议允许服务器和客户机相互验证，协商加密和MAC算法以及保密密钥，用来保护在SSL记录中发送的数据

# 未知流量的秘密—真假HTTPS

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.8.162	10.91.129.22	TCP	78	43086 8443 [SYN] Seq=0 Win=29200
2	0.001017	10.91.129.22	10.3.8.162	TCP	78	8443 43086 [SYN, ACK] Seq=0 Ack=1
3	0.001115	10.3.8.162	10.91.129.22	TCP	70	43086 8443 [ACK] Seq=1 Ack=1 Win=
4	0.001121	10.3.8.162	10.91.129.22	TLSv1	296	Client Hello
5	0.002008	10.91.129.22	10.3.8.162	TCP	70	8443 43086 [ACK] Seq=1 Ack=227 Wi
6	0.002878	10.91.129.22	10.3.8.162	TLSv1.2	156	Server Hello
7	0.002878	10.91.129.22	10.3.8.162	TLSv1.2	76	Change Cipher Spec
8	0.002918	10.3.8.162	10.91.129.22	TCP	70	43086 8443 [ACK] Seq=227 Ack=87 W
9	0.002920	10.91.129.22	10.3.8.162	TLSv1.2	139	Encrypted Handshake Message

Length: 221

## Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 217

Version: TLS 1.2 (0x0303)

Random: e1aca5f61b96460381a7942cb4b3c7a5abfcc1861fbd03226f3fc1afe06ce346

Session ID Length: 32

Session ID: 626d5ca918d564488bec280bd9979a4fe650846d0398c0c3a2b6b2ed178d9419

Cipher Suites Length: 56

Cipher Suites (28 suites)

Compression Methods Length: 1

Compression Methods (1 method)

## 正常HTTPS

正常HTTPS通讯时候，客户端和服务端需要有TLS/SSL握手4个阶段，用于密钥交换。

例如：在Client Hello报文中包含版本、客户端随机数、密码套件等信息。

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.181.86	183.201.219.38	TLSv1.2	156	Application Data
2	0.003498	10.3.181.86	183.201.219.38	TLSv1.2	154	Application Data
3	0.005429	10.3.181.86	183.201.219.38	TLSv1.2	158	Application Data
4	0.018210	183.201.219.38	10.3.181.86	TCP	64	443 数据 32007 [ACK] Seq=1 Ack=99 Win=178 Len=0
5	0.018936	183.201.219.38	10.3.181.86	TLSv1.2	256	Application Data
6	0.019019	183.201.219.38	10.3.181.86	TLSv1.2	256	Application Data

> Frame 1: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)  
> Ethernet II, Src: 00:50:56:b5:6c:ba (00:50:56:b5:6c:ba), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4072  
> Internet Protocol Version 4, Src: 10.3.181.86, Dst: 183.201.219.38  
> Transmission Control Protocol, Src Port: 32007, Dst Port: 443, Seq: 1, Ack: 1, Len: 98  
Transport Layer Security  
 TLSv1.2 Record Layer: Application Data Protocol: http-over-tls  
 Content Type: Application Data (23)  
 Version: TLS 1.2 (0x0303)  
 Length: 93  
 Encrypted Application Data: 0000000000000000648440538eeaa54aa32838f51364cf1953b95ffda05500d9ce15a304d  
 [Application Data Protocol: http-over-tls]

```
0000  88 df 9e 39 2a 01 00 50 56 b5 6c ba 81 00 0f e8  ...9*..PV .l....
0010  08 00 45 00 00 8a 15 70 40 00 80 06 92 b4 0a 03  ..E...p@ .....
0020  b5 56 b7 c9 db 26 7d 07 01 bb 4c dc f9 de 78 63  .V...&!... .L...xc
```

**非正常HTTPS**

这个TCP协议目标端口为443的数据包，第一个报文就直接是应用数据，没有SSL握手的过程。

也就是说，客户端和服务端没有经过密钥协商，但已经知道对方是可信的。

相当于一个间谍没有对暗号就开始传送情报。

匹配条件	执行动作
策略序号	200 <small>1~65535,序号小的优先匹配</small>
策略备注	阻断HTTPS隧道
线路及流向	任意 任意
首包接口	em3
源接口	任意
内网地址: 端口	IP群组 HW系统 : 30或81
外网地址: 端口	任意 : 443
协议	TCP 未知协议 <a href="#">选择</a>

## 管控策略:

对于HW系统访问外网地址的TCP 433端口的未知协议进行阻断操作



03

如何溯源给防守方加分?

# 攻防演习，防守方加分项目

类别	得分标准	赋值规则	赋值上线	备注
发现类	发现攻击者进入逻辑隔离业务内网区事件	100分/次	1000分	提供的证据必须与攻击方提供的证据相吻合的 <b>详细分析报告</b> (时间、IP、日志、处置结果等)
消除类	处置异常账号	普通用户：应用层5分，系统层10分，数据库10分，网络设备25分。管理员用户：得分*2	500分	提供包含 <b>确凿证据的详细分析报告</b> (创建时间、访问日志、登录日志、处置结果等)，由裁判组研判后给分
应急处理类	积极配合应急组工作，根据线索能快速准确定位危害系统， <b>能提供充分的日志记录，配合执法机关有效固定证据完成勘验</b>	能高效配合完成应急工作的，得分300；配合一般的，得分200；差的-100	/	最高300分，最低-100分
追踪溯源类	对网络攻击事件的进行成功溯源， <b>提交有效证据材料构成证据链</b> ，还原完整攻击路径，证实攻击者的攻击行为	境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客	/	提供包含 <b>确凿证据</b> 的详细分析报告 (时间、平台截图、访问日志、告警详情等)

PS: 加分项目不止这几个，这里只是摘抄几个举例说明。

# 攻防演习，全流量数据留存可以作什么？

会话流量

源IP 任意IP 源端口 80 / 8000-8080 单个IP 10.3.8.211 目标端口

源IP ISP 任意 目标IP ISP 任意 源IP区域 任意 目标IP区域

时间范围 2022-04-19 08:29:41 - 2022-04-19 09:29:41 连接类型 所有

请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57039	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57037	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57030	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.21561	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57033	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.2.48.59.57036	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57029	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57028	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57015	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57017	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.48.59.57021	10.3.8.211:80		TCP	SYN_ACK
<input type="checkbox"/> 2022-04-19/08:29:41	10.2.48.59.57025	10.3.8.211:80		TCP	SYN_ACK

通过全流量的数据留存，发现从外网对内网一台服务器的端口扫描  
(很不幸，端口扫描不是加分项)

源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传/包数	下行重传/包数	重置 <sup>i</sup>	流量 <sup>i</sup>
9/08:29:41	55.30:39522	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	55.30:39524	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	55.30:39523	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39525	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39526	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	55.30:39527	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39529	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39530	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39528	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39538	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39537	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39536	10.3.240.5:1433	TCP	MSSQL	1/2	1/2	0/0	584/388

通过全流量的数据留存，发现从外网对内网一台数据库服务器的流量非常有规律。  
这个是啥原因呢？有可能是加分项目吗？

# 全流量数据留存+报文分析

报文解析 报文交互 元数据 报文播放

报文显示过滤器

4	0.000323	10.3.240.5	10.3.55.30	TCP	78	[TCP Out-Of-Order] 1433 数据 51294
5	0.000415	10.3.240.5	10.3.55.30	TCP	70	51294 数据 1433 [ACK] Seq=1 Ack=1
6	0.000416	10.3.240.5	10.3.55.30	TCP	70	[TCP Dup ACK 5#1] 51294 数据 1433
7	0.000617	10.3.240.5	10.3.55.30	TDS	292	TDS7 login
8	0.000630	10.3.240.5	10.3.55.30	TCP	292	[TCP Retransmission] 51294 数据 1433
9	0.001315	10.3.240.5	10.3.55.30	TDS	194	Response
10	0.001316	10.3.240.5	10.3.55.30	TCP	70	1433 数据 51294 [FIN, ACK] Seq=1280000000
11	0.001330	10.3.240.5	10.3.55.30	TCP	194	[TCP Out-Of-Order] 1433 数据 51294

Packet Number: 1

Window: 0

▼ TDS7 Login Packet

> Login Packet Header

> Lengths and offsets

Client name: F...XTBGYY

Username: byoaselect

Password: byoaselect

App name: jTDS

Server name: 10.3.240.5

Library name: S

Database name: RDSYS...710013

```
00b0 54 00 42 00 47 00 59 00 59 00 62 00 79 00 6f 00  T.B.G.Y.Y .b.y.o.
00c0 61 00 73 00 65 00 6c 00 65 00 63 00 74 00 83 a5  a.s.e.l.e.c.t...
00d0 32 a5 53 a5 b3 a5 92 a5 f3 a5 63 a5 f3 a5 93 a5  2.S.....c....
00e0 e2 a5 6a 00 54 00 44 00 53 00 31 00 30 00 2e 00  ..j.T.D.S .l.o...
00f0 33 00 2e 00 32 00 34 00 30 00 2e 00 35 00 6a 00  3...2.4.0 ...5.j.
0100 54 00 44 00 59 00 59 00 44 00 59 00 59 00  T.D.S.D.S.V.S
```

## NTM分析

外网某IP对数据库进行进行**连续**的登录操作。

登录的用户名为 “byoaselect”

报文解析 报文交互 元数据 报文播放

报文显示过滤器

4	0.000323	10.3.240.5	55.30	TCP	78	[TCP Out-Of-Order
5	0.000415	55.30	10.3.240.5	TCP	70	51294 款 1433 [
6	0.000416	55.30	10.3.240.5	TCP	70	[TCP Dup ACK 5#1]
7	0.000617	55.30	10.3.240.5	TDS	292	TDS7 login
8	0.000630	55.30	10.3.240.5	TCP	292	[TCP Retransmissi
9	0.001315	10.3.240.5	10.3.5	TDS	194	Response
10	0.001316	10.3.240.5	10.3.5	TCP	70	1433 款 51294 [
11	0.001330	10.3.240.5	10.3.5	TCP	194	[TCP Out-Of-Order

Token - Error

Token length: 104  
SQL Error Number: 18456  
State: 1  
Class (Severity): 14  
Error message length: 21 characters  
Error message: 攀儿桐 byoaselect 鋼海緯澶辨觸鉅  
Server name length: 25 characters  
Server name: WIN-6F1CSPSJSQM\MSSQL2018  
Process name length: 0 characters  
Line number: 1

Token - Done

```
0050 00 18 48 00 00 01 0e 15 00 28 75 37 62 20 00 27 ..H.....(u7b.'
0060 00 62 00 79 00 6f 00 61 00 73 00 65 00 6c 00 65 .b.y.o.a.s.e.l.e
0070 00 63 00 74 00 27 00 20 00 7b 76 55 5f 31 59 25 .c.t.'..{vU_1Y%
0080 84 02 20 10 57 00 40 00 40 00 24 00 36 00 46 00 O W T N - 6 F
```

## NTM分析

外网某IP对数据库进行进行**连续**的登录操作。数据库服务器进行响应，提示token 错误，同时，返回错误提示。

## 加分项目：

加分类别：发现类

加分标准：发现账号异常

加分：数据库账号10分，上限为500分



报文解析 报文交互 元数据 报文播放

报文显示过滤器

15	0.005422	242.47	10.112.48.129	MySQL	135	Request Query
16	0.006288	10.112.48.129	242.47	MySQL	183	Response
17	0.006590	242.47	10.112.48.129	MySQL	136	Request Query
18	0.007432	10.112.48.129	242.47	MySQL	184	Response
19	0.007736	242.47	10.112.48.129	MySQL	136	Request Query
20	0.008592	10.112.48.129	242.47	MySQL	183	Response

> Frame 17: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)  
> Ethernet II, Src: d0:94:66:67:17:8d (d0:94:66:67:17:8d), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4068  
> Internet Protocol Version 4, Src: 242.47, Dst: 10.112.48.129  
> Transmission Control Protocol, Src Port: 46710, Dst Port: 3306, Seq: 302, Ack: 413, Len: 66

MySQL Protocol

Packet Length: 62

Packet Number: 0

Request Command Query

Command: Query (3)

Statement: select skill\_order from knowledgePoint where skill\_id = '111'

```
0000  88 df 9e 39 2a 01 d0 94 66 67 17 8d 81 00 0f e4  ...9*...f g.....
0010  08 00 45 00 00 76 16 2d 40 00 40 06 ed 31 0a 03  ..E..v.-@ .@.1..
0020  f2 2f 0a 70 30 81 b6 76 0c ea d8 0c f5 b6 5d db  ./..p0..v. ....].
0030  cd 9c 80 18 00 ed de e1 00 00 01 01 08 0a 2d 2a  ..... -*
0040  b9 6b 92 38 ac 40 3e 00 00 00 03 73 65 6c 65 63  .k.8.>.. ..selec
0050  74 20 73 6b 69 6c 6c 5f 6f 72 64 65 72 20 66 72  t skill_o rder fr
```

## NTM分析

外网某IP对数据库进行进行root登录操作。登录成功后，进行数据库相关操作。

## 加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客

报文解析 报文交互 **元数据** 报文播放

展示方式 按属性

- > command
- > charset
- > warnings
- > version
- √ user
  - ⊕ 报文6 root
- > unused
- > thread\_id
- > response\_code
- > request
- √ query
  - ⊕ 报文9 SET AUTOCOMMIT = 0
  - ⊕ 报文11 BEGIN
  - ⊕ 报文13 select 铜斤拷铜斤拷铜斤拷, 铜斤拷铜斤拷铜斤拷铜斤拷 from timu where id = 15
  - ⊕ 报文15 select skill\_order from knowledgePoint where skill\_id = '347'
  - ⊕ 报文17 select skill\_order from knowledgePoint where skill\_id = '851'
  - ⊕ 报文19 select skill\_order from knowledgePoint where skill\_id = '863'
  - ⊕ 报文21 select skill\_order from knowledgePoint where skill\_id = '142'
  - ⊕ 报文23 select skill\_order from knowledgePoint where skill\_id = '817'
  - ⊕ 报文25 select skill\_order from knowledgePoint where skill\_id = '167'
  - ⊕ 报文27 select skill\_order from knowledgePoint where skill\_id = '796'
  - ⊕ 报文29 COMMIT

## NTM分析

通过元数据分析，将同一会话里面的报文进行数据还原，还原相关操作的细节。

## 加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客

会话流量



源IP	任意IP	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	80 / 8000-8080	传输协议	任意	应用协议	任意协议
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	请求域名			
时间范围	2022-05-05 13:03:44 - 2022-05-05 14:03:44		连接类型	所有							

请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-05/13:03:44	00-50-56-b...	3.8.162.64336	1.53.100:80		TCP	WWW	1/2	26/52	0/0	1682/10628	www.b...e...		数据包
2022-05-05/13:03:44	00-50-56-b...	3.8.162.2732	1.129.64:80		TCP	伪IE下载	0/1	0/17	0/0	1014/24524	cucloud....		数据包
2022-05-05/13:03:44	00-50-56-b...	8.162:5110	1.129.30:80		TCP	WWW	0/2	0/2	0/0	1619/701	iucloud.b...		数据包
2022-05-05/13:03:44	00-50-56-b...	22.0.233:55012	3.9.85:80		TCP	其它HTTP上传	0/1	0/1	0/0	275/195	3.9.85 304		数据包

**报文播放**，又称报文回放。是指通过全流量数据留存后，按照一定的筛选条件，将符合条件的报文从NTM的某个接口播放出去，用于模拟真实流量，它具有真实流量的全部特征。

**用途：**安全取证、压力测试、故障分析、第三方系统联动等。

# 全流量数据留存+报文播放

时间范围: 2022-05-01 11:14:53 - 2022-05-01 12:14:53 | 连接类型: 所有

请求时间	MAC	源IP	目标IP	目标...	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42740	53.100:80		TCP	WWW	1/2	2/4	0/0	1190/4104	www...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42952	53.100:80		TCP	WWW	1/2	1/2	0/0	1866/1678	www...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42912	53.100:80		TCP	WWW	1/2	42/84	0/0	1920/61318	www.b...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42910	53.100:80		TCP	WWW	1/2	39/78	0/0	1920/52766	www...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42908	53.100:80		TCP	WWW	1/2	21/42	0/0	1982/63414	www.b...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42924	53.100:80		TCP	WWW	1/2	2/4	0/0	1884/4452	www...t.edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42928	53.100:80		TCP	WWW	1/2	53/106	0/0	1972/28238	www...t.edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42938	53.100:80		TCP	WWW	1/2	9/18	0/0	1888/25300	www.b...edu.cn 200	数据包	数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42936	53.100:80		TCP	WWW	1/2	11/22	0/0	1878/31730	www.f...edu.cn 200	数据包	数据包



NTM



报文播放



杀毒&IDS



已知病毒&木马审计系统

# 全流量数据留存+报文播放

请求时间	MAC	源IP	目标IP	目标...	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42740	53.100:80		TCP	WWW	1/2	2/4	0/0	1190/4104	www...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42952	53.100:80		TCP	WWW	1/2	1/2	0/0	1866/1678	www...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42912	53.100:80		TCP	WWW	1/2	42/84	0/0	1920/61318	www.b...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42910	53.100:80		TCP	WWW	1/2	39/78	0/0	1920/52766	www...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42908	53.100:80		TCP	WWW	1/2	21/42	0/0	1982/63414	www.b...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42924	53.100:80		TCP	WWW	1/2	2/4	0/0	1884/4452	www...t.edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42928	53.100:80		TCP	WWW	1/2	53/106	0/0	1972/28238	www...t.edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	...162.42938	53.100:80		TCP	WWW	1/2	9/18	0/0	1888/25300	www.b...edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42936	53.100:80		TCP	WWW	1/2	11/22	0/0	1878/31730	www.f...edu.cn 200		数据包



NTM



报文播放



沙箱



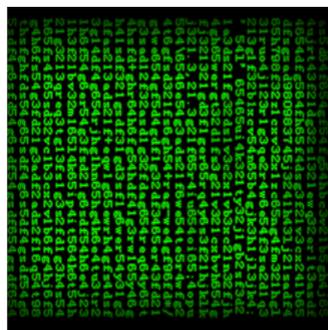
未知病毒&木马分析系统

# 全流量数据留存+报文播放

请求时间	MAC	源IP	目标IP	目标...	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42740	53.100:80		TCP	WWW	1/2	2/4	0/0	1190/4104	www. edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42952	53.100:80		TCP	WWW	1/2	1/2	0/0	1866/1678	www. edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42912	53.100:80		TCP	WWW	1/2	42/84	0/0	1920/61318	www. edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42910	53.100:80		TCP	WWW	1/2	39/78	0/0	1920/52766	www. edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42908	53.100:80		TCP	WWW	1/2	21/42	0/0	1982/63414	www. edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42924	53.100:80		TCP	WWW	1/2	2/4	0/0	1884/4452	www. t.edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42928	53.100:80		TCP	WWW	1/2	53/106	0/0	1972/28238	www. t.edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42938	53.100:80		TCP	WWW	1/2	9/18	0/0	1888/25300	www. b.edu.cn 200		数据包
2022-05-01/11:14:53	00-50-56-80-f9-da	3.8.162.42936	53.100:80		TCP	WWW	1/2	11/22	0/0	1878/31730	www. f.edu.cn 200		数据包



NTM



报文播放



威胁情报



威胁情报  
审计系统

- 挖矿分析
- 恶意木马分析
- 勒索软件分析
- APT分析
- 暗网访问分析
- C&C攻击分析
- .....



2022

可视化网络领导者

**THANK YOU**