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

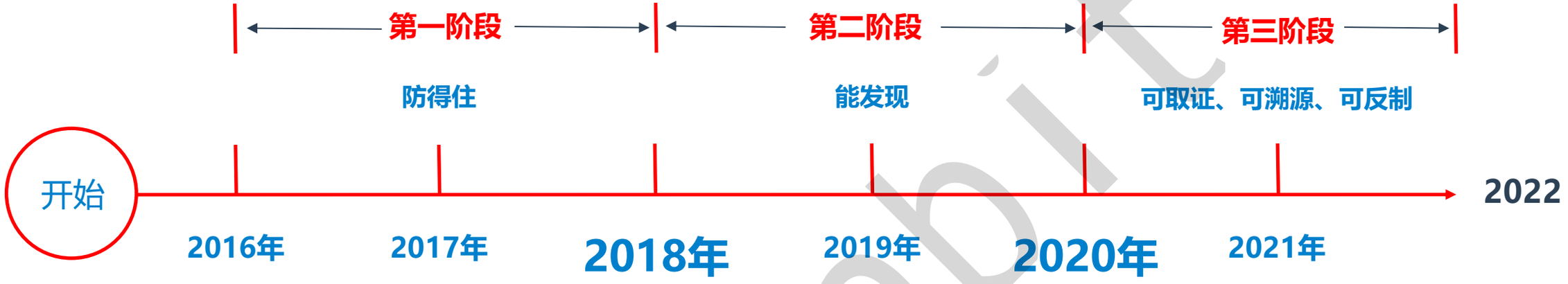
网络安全攻防演习简介

什么是攻防演习

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



防守对策	防守对策	防守对策
1.使用大量的硬性防守手段； 2.下线风险的业务系统； 3.封堵大量的IP地址； 4.畸形的防守手段；	1.使用大量的硬性防守手段； 2.下线风险的业务系统； 3.封堵大量的IP地址； 4.畸形的防守手段； 5.使用大量的安全设备；	1.使用大量的硬性防守手段；× 2.下线风险的业务系统；× 3.封堵大量的IP地址；× 4.畸形的防守手段；× 5.使用大量的安全设备；√

教育行业网络安全攻防演习— 2022

Panabit®

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

网络安全攻防演习—攻击方常用手段

攻击方常用手段

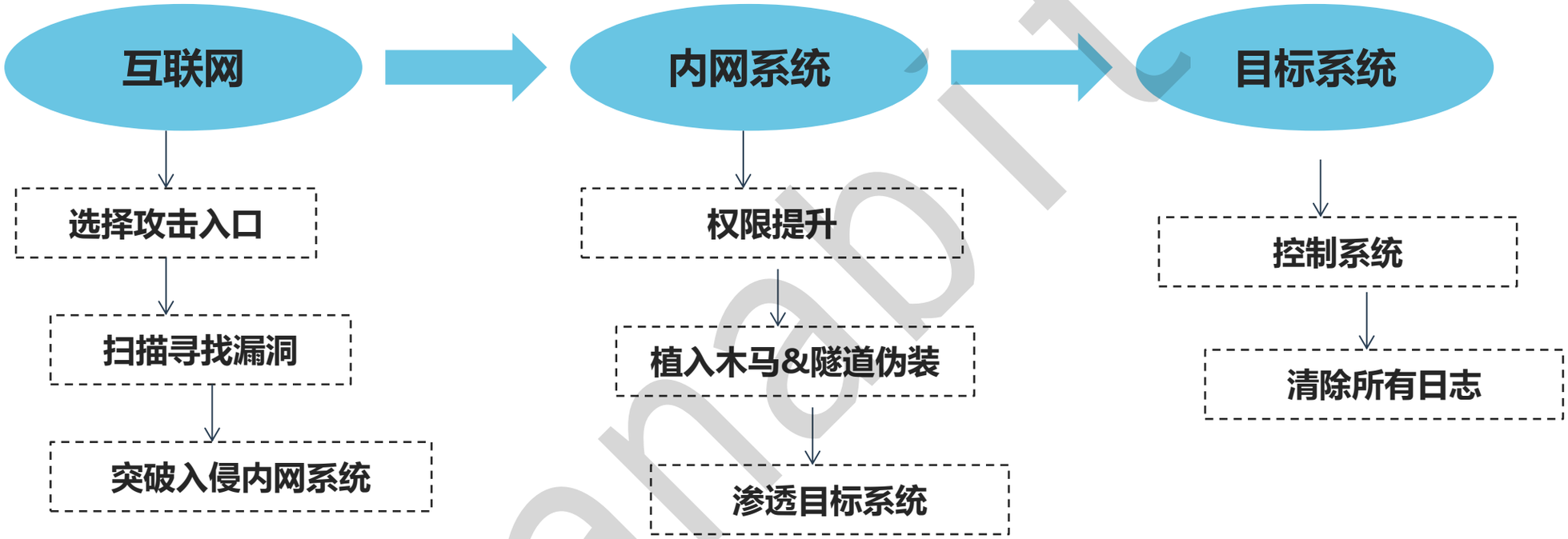
探测：通过扫描，暴力破解，钓鱼，嗅探等方式发现防守方的漏洞和弱点。

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，同时所有删除操作日志。

网络安全攻防演习— 攻击方思路



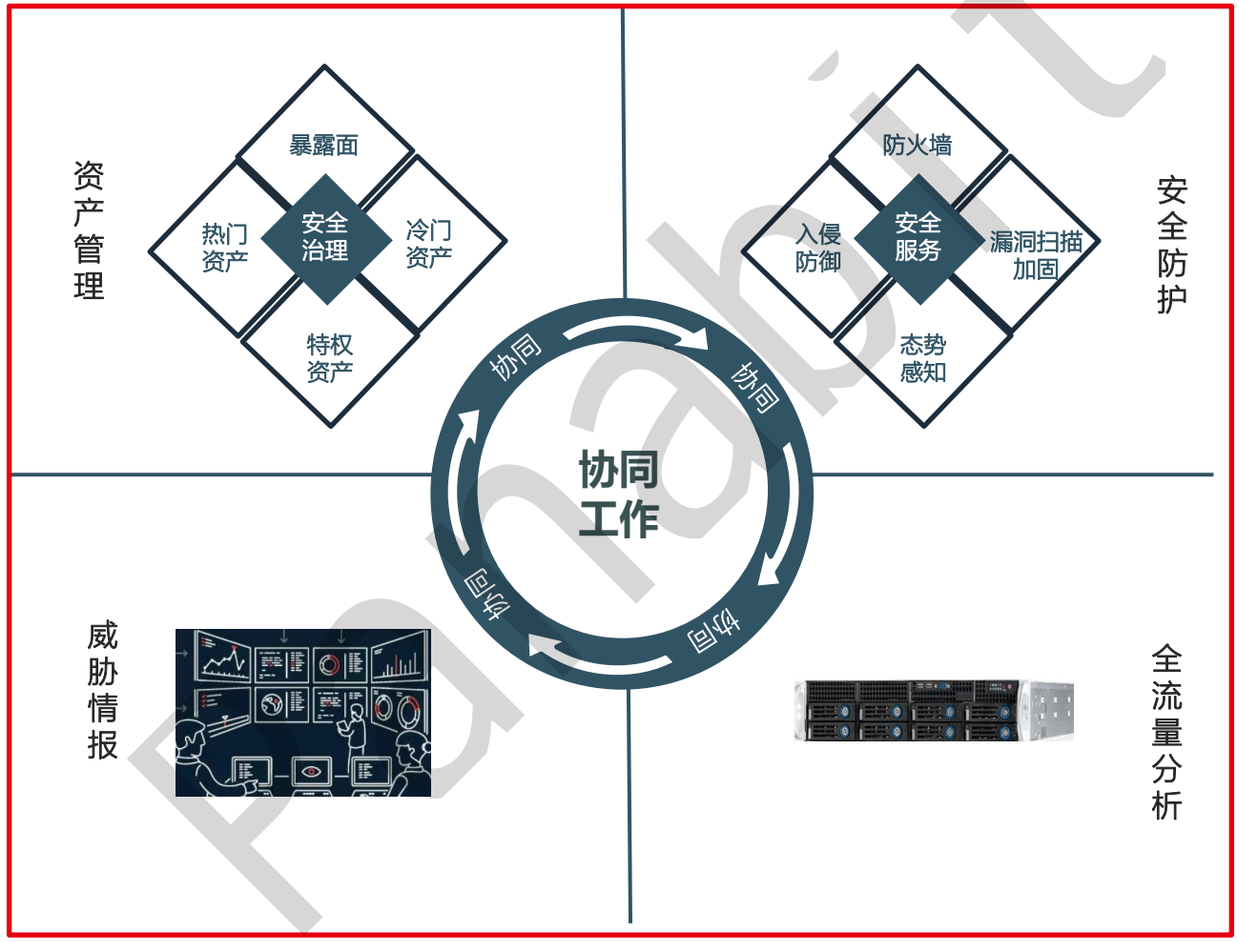
互联网突破口选择原则：选择防护意识薄弱系统，存在高危漏洞系统，第三方供应商，运维服务供应商，新型应用架构业务系统等。

网络安全攻防演习— 防守方思路

Panabit®

标注重点资产
关闭冷门资产
管控特权终端
最小暴露面

恶意木马阻断
勒索软件阻断
APT分析阻断
C&C攻击阻断
HW相关阻断



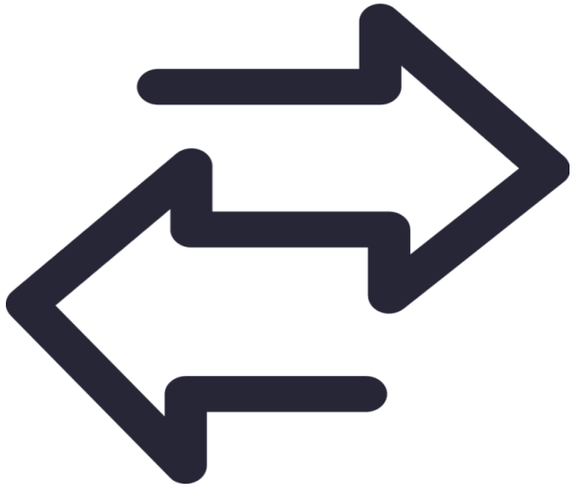
通过各种安全产品和安全服务，最大程度保护重点资产

流量异常发现
DNS隧道分析
流量播放分析
攻击证据提取

02

梳理资产，减少暴露面

防守方全方位资产管理



方向1：互联网访问校内资产

方向2：校内资产访问互联网

资产管理—互联网访问校内

意义

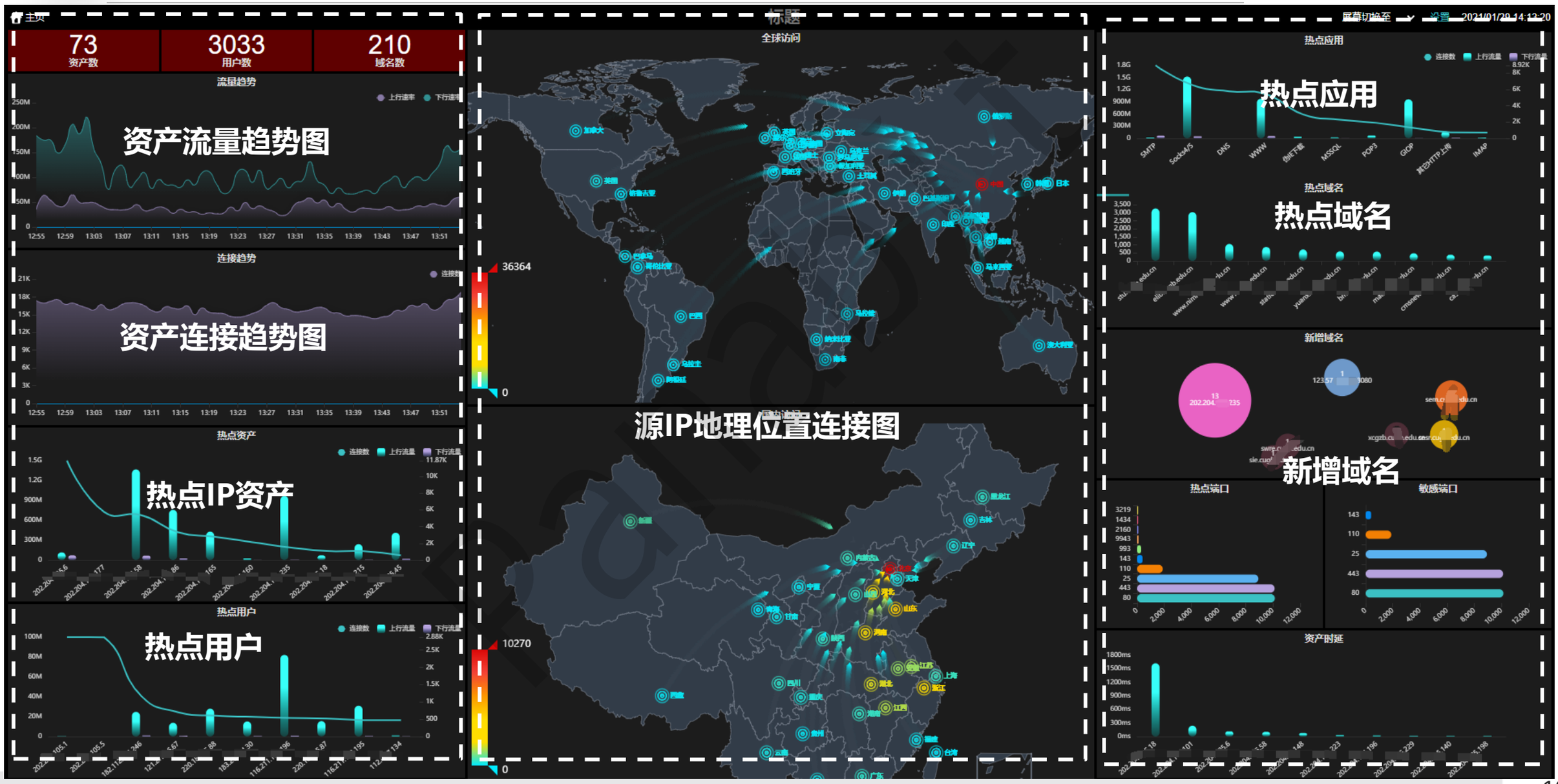
检测资产暴露面，及时发现暴露资产，确保资产暴露最小化。

作用：

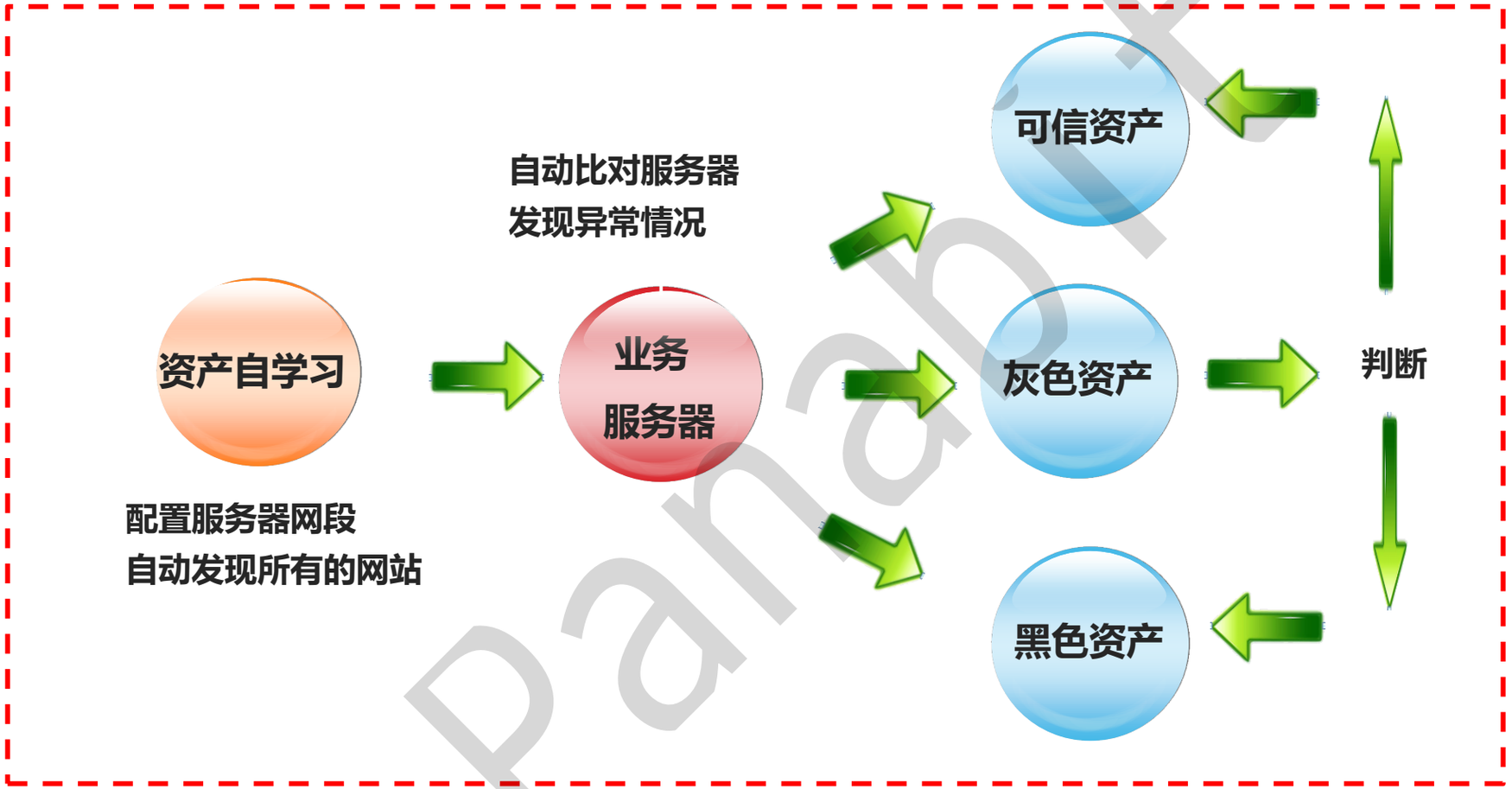
网络攻防演习是针对于**全程可控、可审计**的实战攻击。因此，做好资产梳理，达到资产暴露最小化目的，便于我们下一步的监控和审计。

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**。

资产管理—资产大屏



防守方资产管理



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

Panabit®

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.b edu.cn	172352	63338	108926	88	105583	514	2722	0
2	service.b .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.b .edu.cn	36334	512	5201	30621	0	5199	1	0
5	apiucloud. .edu.cn	35796	406	34932	458	32923	0	1956	3
6	ucloud.b edu.cn	24028	904	22235	889	18476	3360	384	0
7	huorong.b 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.b edu.cn	12117	1228	10889	0	270	10554	51	0
10	oa.bu du.cn	9293	138	9022	133	6321	10	2690	0
11	teac t.edu.cn	8514	242	[illegible]	3	4914	325	214	2383
12	news.b .edu.cn	8216	3212	5002	2	3729	261	1011	0
13	imgservice.b edu.cn	7433	434	6990	9	6924	36	27	0
14	reservation.b 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. .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

< 1 2 3 4 5 > 到第 1 页 确定 总共 464 1

资产数量

资产管理— 非授权访问告警

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。

资产管理—资产管控

对象列表 登录日志 操作日志

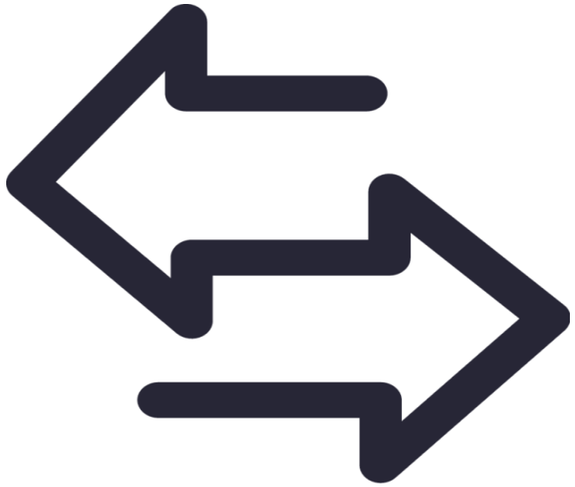
序号	用户	操作时间	内容
1		2019/04/25 09:25:20	联网 设备/TEST11111111 对象/www.abc.cn 用户/
2		2019/04/24 16:09:44	断网 设备/TEST11111111 对象/www.abc.cn 用户/
3		2019/04/22 15:54:24	断网 设备/wp2018072510 对象/www.abc.edu.cn
4		2019/04/22 15:53:36	联网 设备/wp2018072510 对象/oa.abc.wdu.cn 用
5		2019/04/22 15:51:55	联网 设备/wp2018072510 对象/www.abc.edu.cn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

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**。

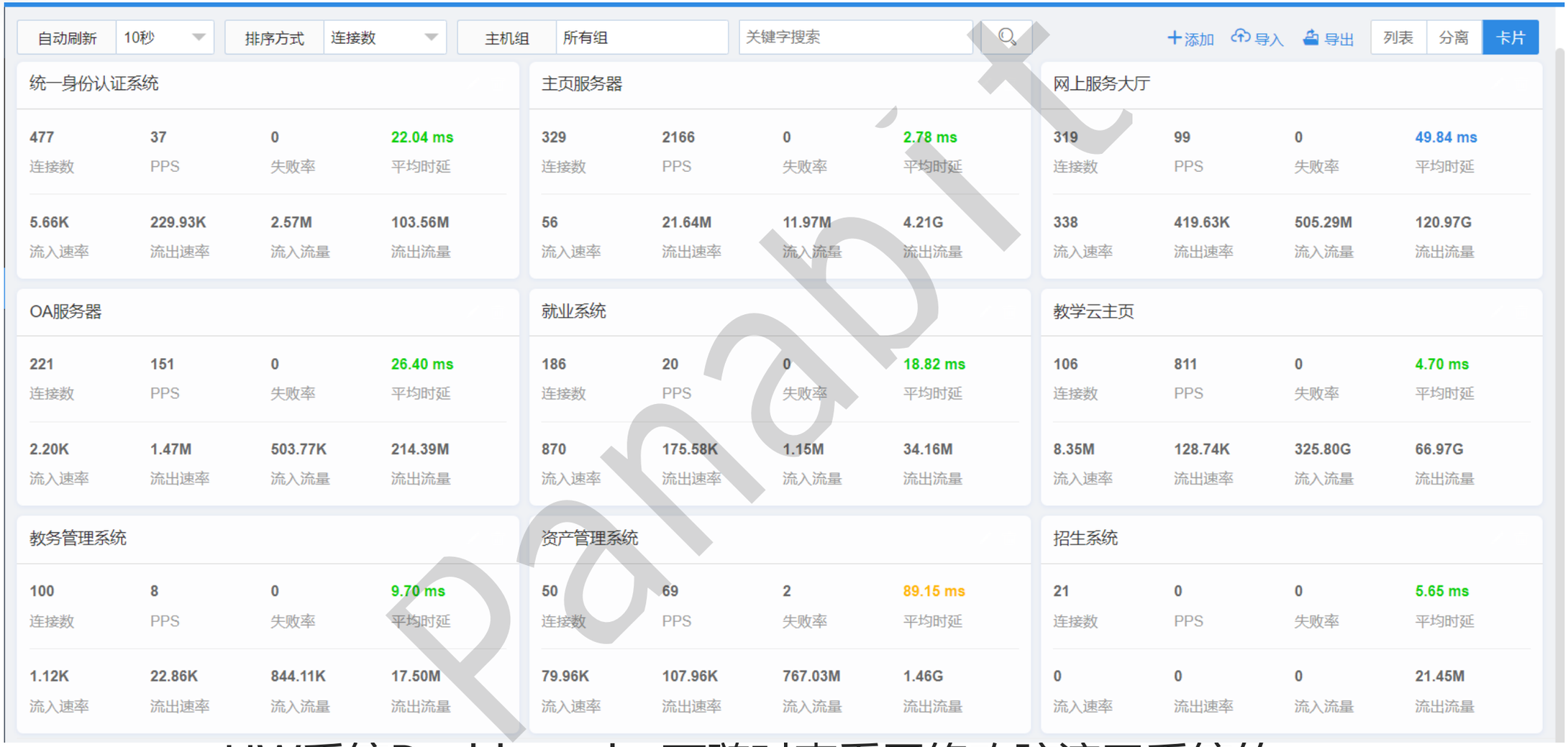
实战：校园网卡顿NTM分析



方向1：互联网访问校内资产

方向2：校内资产访问互联网

资产管理—资产可视化



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。

资产管理—资产可视化

实时分析　历史分析

流入速率	流出速率	PPS	连接数	失败率	平均时延	流入流量	流出流量
9.78K	1.44M	168	610	0 %	13.76 ms	109.88M	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…	数据包
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…	数据包
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…	数据包
WWW	tcp	源 3.240.159:21875 目 .9.161:80		1	0.07	0.05	5.14	1/2	2/4	472/514	944/1966	auth.b edu.cn|2…	数据包
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…	数据包
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…	数据包
iPhone	tcp	源 0.3.8.162:60776 目 0.3.55.243:8081		2	0.07	0.29	0.90	1/2	3/6	547/1468	1094/6446	auth. .edu.cn|2…	数据包
WWW	tcp	源: 3.8.162:25292 目:1 3.55.246:8081		2	0.07	0.53	4.05	1/2	2/4	527/421	1054/1648	auth. t.edu.cn|2…	数据包

可以随时查看HW系统的连接信息，发现异常行为。

资产管理— 不该发生的应用

Panabit®

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

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
2022-05-04/19:31:32	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
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
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
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
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
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
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。

资产管理— 未知流量里面的秘密

Panabit®

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

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DNS

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

Panabit®

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
v Domain Name System (query)
    Transaction ID: 0x6bd5
  > Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  v 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

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。

资产管理—DNS管控

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

27

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

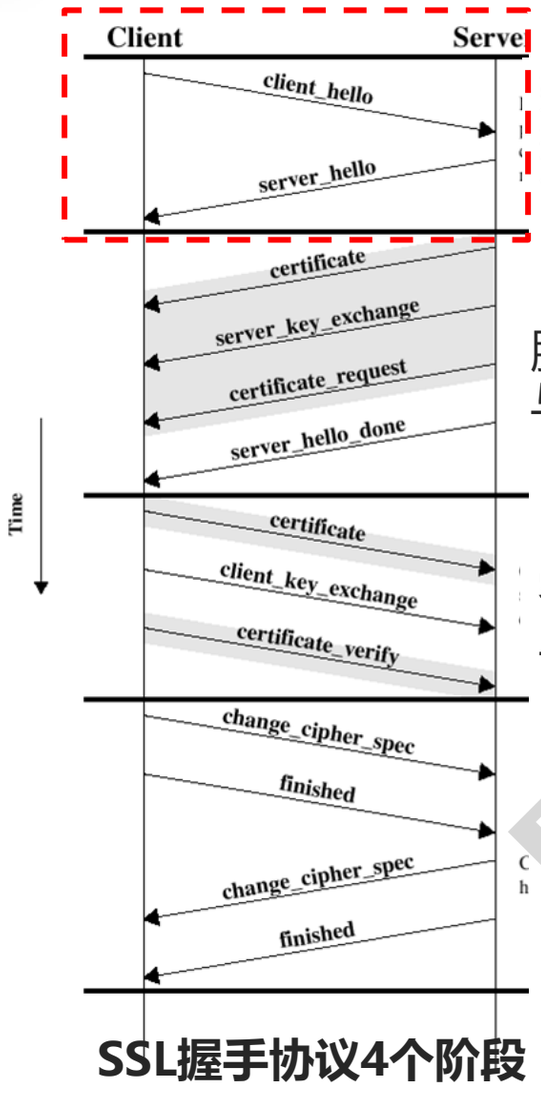
源IP ISP 任意 | 目标IP ISP 任意 | 源IP区域 任意 | 目标IP区域 国外 | 请求域名

时间范围 2022-04-30 10:00:40 - 2022-05-01 11:00:40 | 连接类型 所有

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
2022-04-30/10:02:28	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
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
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
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
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
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
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
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
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



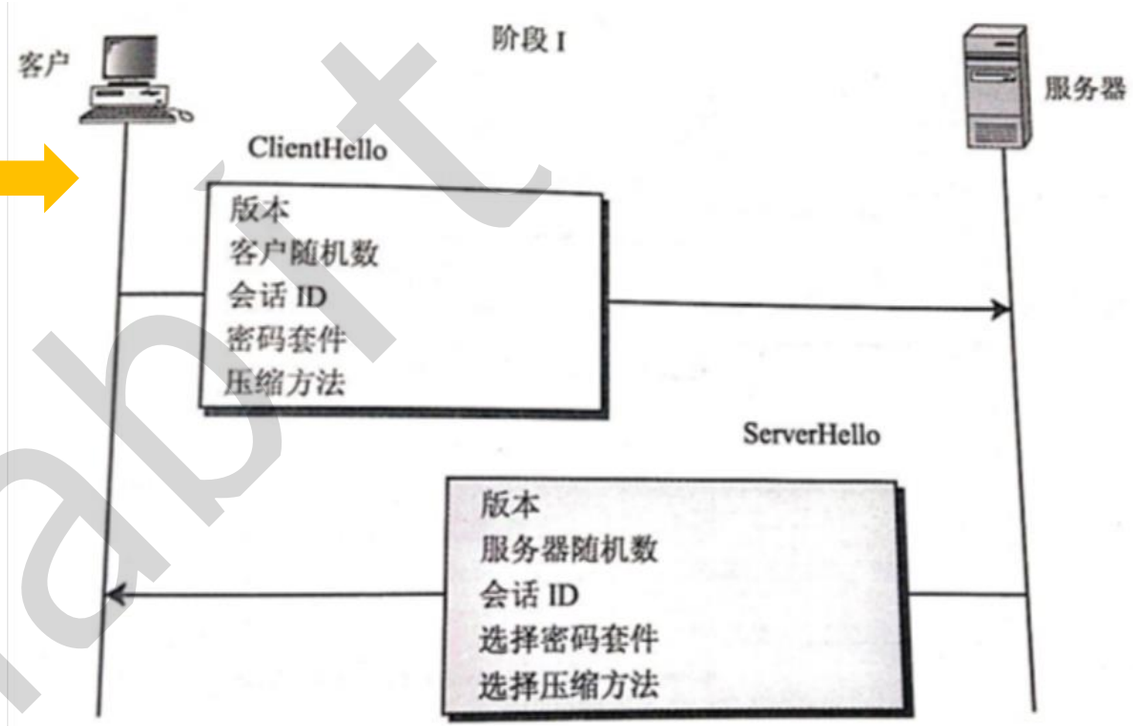
建立连接安全能力

服务器鉴别与密钥交换

客户机鉴别与密钥交换

完成

SSL握手协议4个阶段



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 鈥 8443 [SYN] Seq=0 Win=29200
2	0.001017	10.91.129.22	10.3.8.162	TCP	78	8443 鈥 43086 [SYN, ACK] Seq=0 Ack=1
3	0.001115	10.3.8.162	10.91.129.22	TCP	70	43086 鈥 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 鈥 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 鈥 8443 [ACK] Seq=227 Ack=87 W
9	0.002920	10.91.129.22	10.3.8.162	TLSv1.2	139	Encrypted Handshake Message

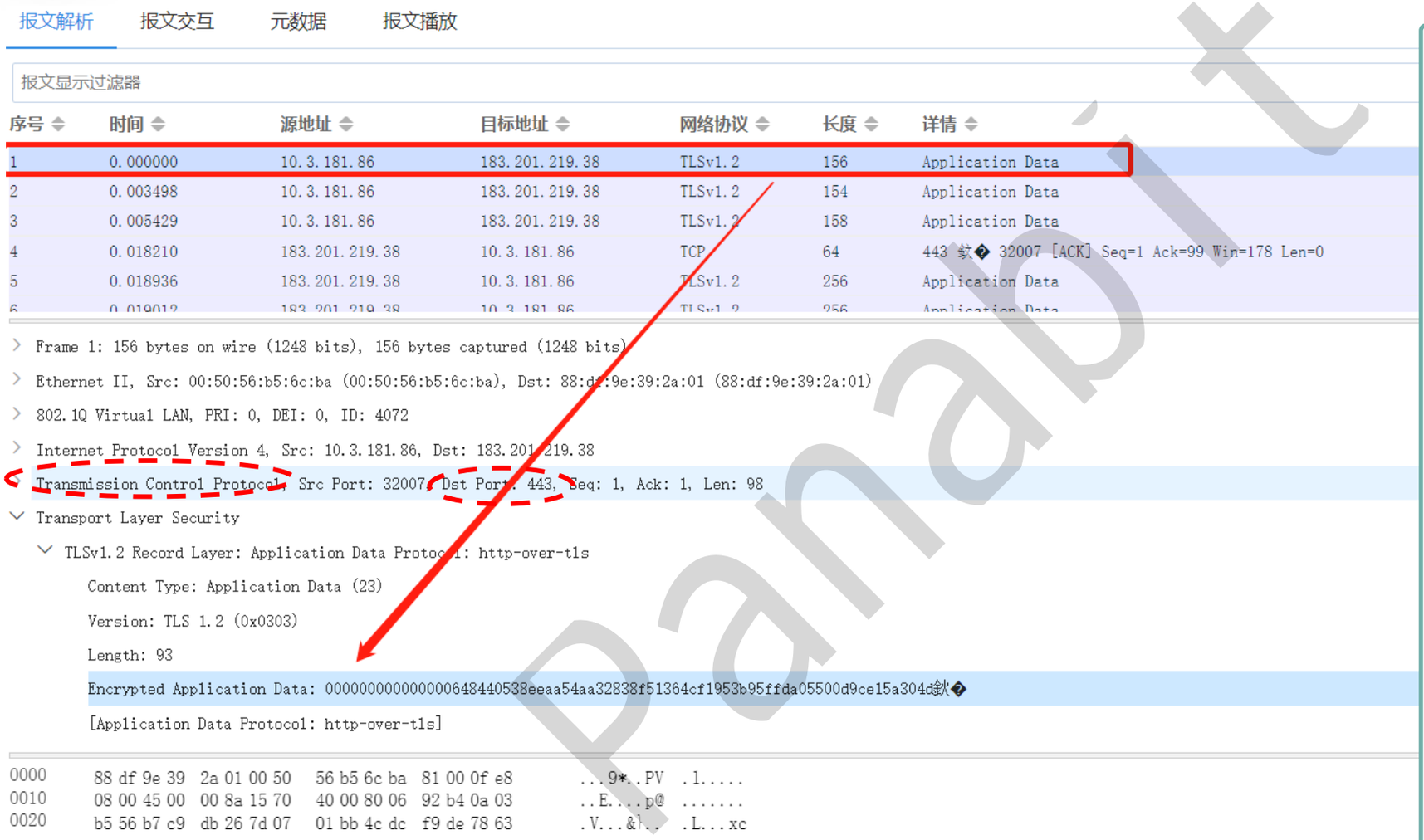
```
Length: 221
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 217
    Version: TLS 1.2 (0x0303)
    Random: e1aca5f61b96460381a7942cb4b3c7a5abfcc1861fbd03226f3fc1afe06ce346
    Session ID Length: 32
    Session ID: 626d5ca918d564488bec280bd9979a4fe650846d0398c0c3a2b6b2ed178d9419
    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，客户端和服务器端需要有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。

未知流量的秘密— 真假HTTPS



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，客户端和服务器没有经过密钥协商，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。

资产管理—HTTPS加密隧道阻断

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

32

03

如何溯源给防守方加分？

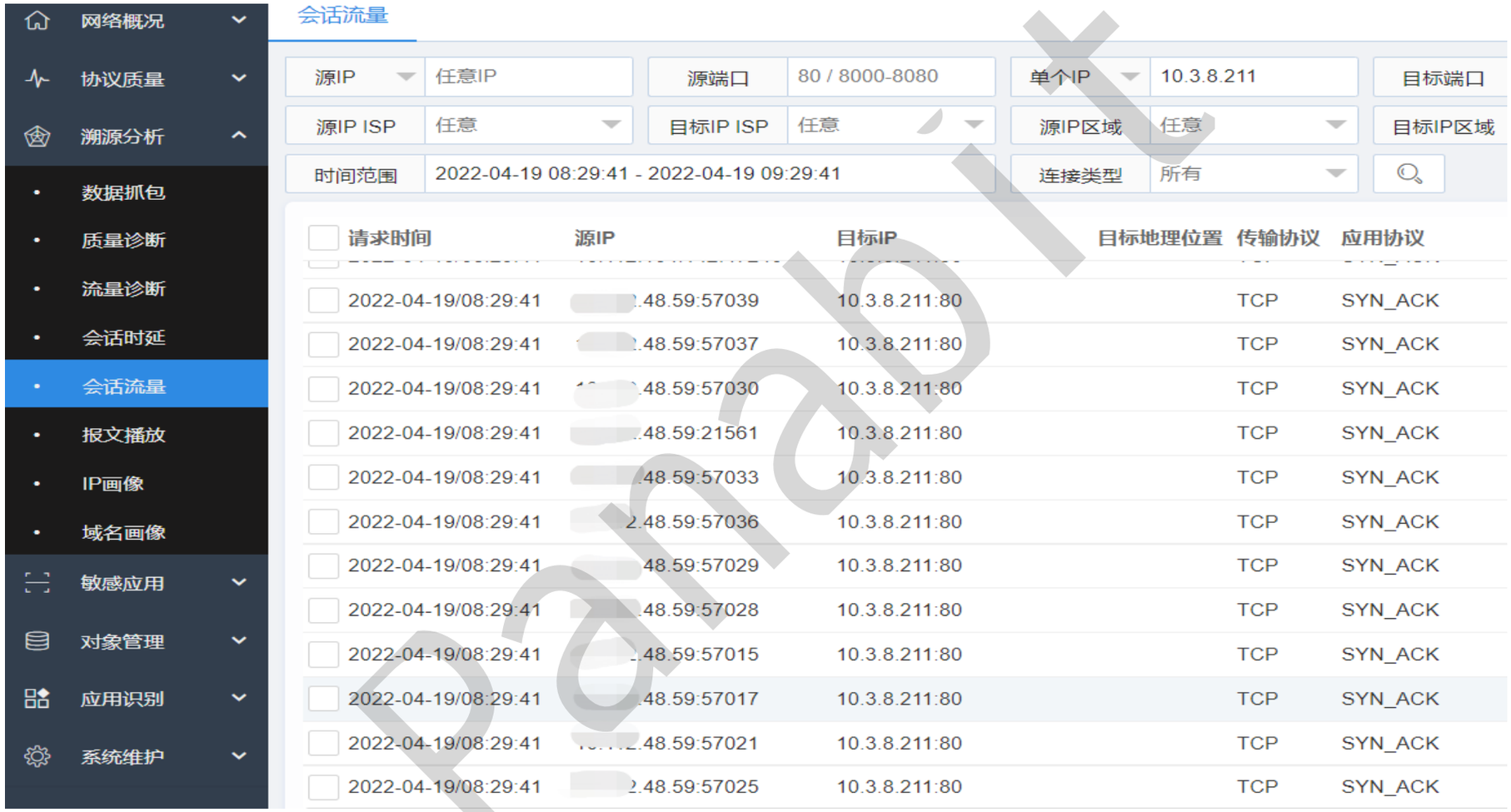
攻防演习，防守方加分项目

Panabit®

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**详细分析报告**（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**含确凿证据的详细分析报告**（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，**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**	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，**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	境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客	/	提供包含确凿证据的详细分析报告（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？



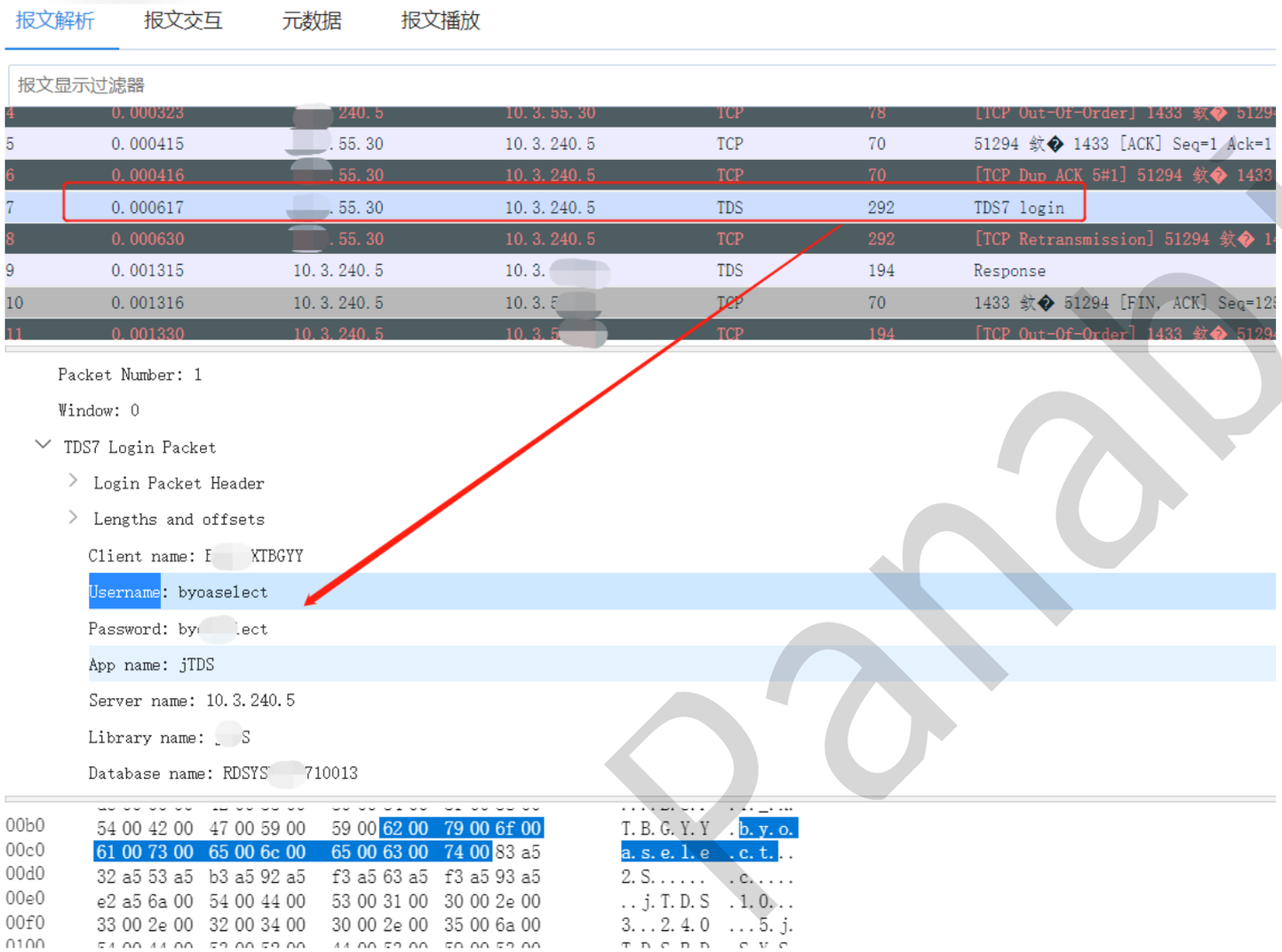
通过全流量的数据留存，发现从外网对内网一台服务器的端口扫描
（很不幸，端口扫描不是加分项）

全流量数据留存+报文分析

	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	流量
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	5.30:39524	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	5.30:39523	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39525	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39526	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39527	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	3.55.30:39536	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

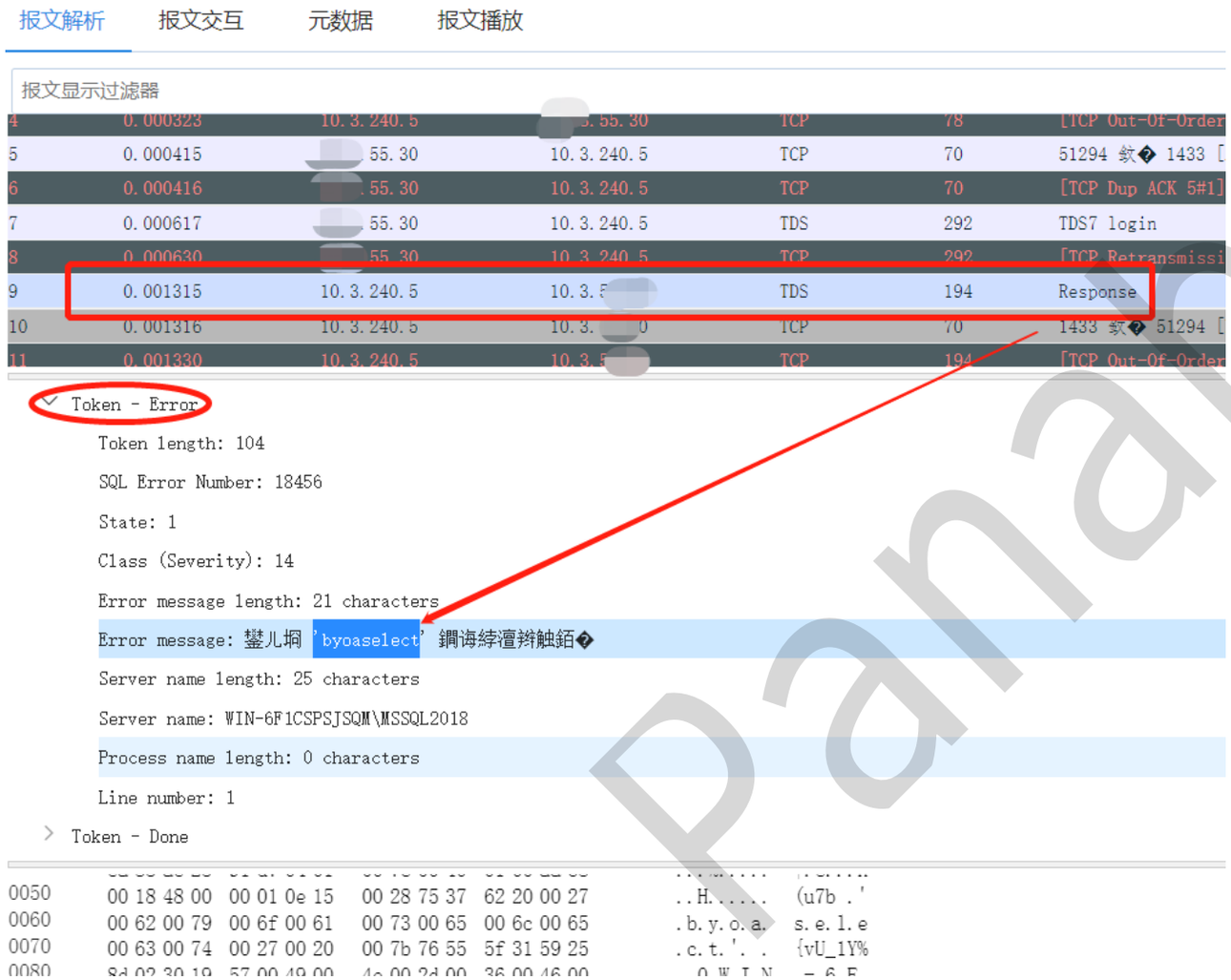


NTM分析

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”

全流量数据留存+报文分析



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。

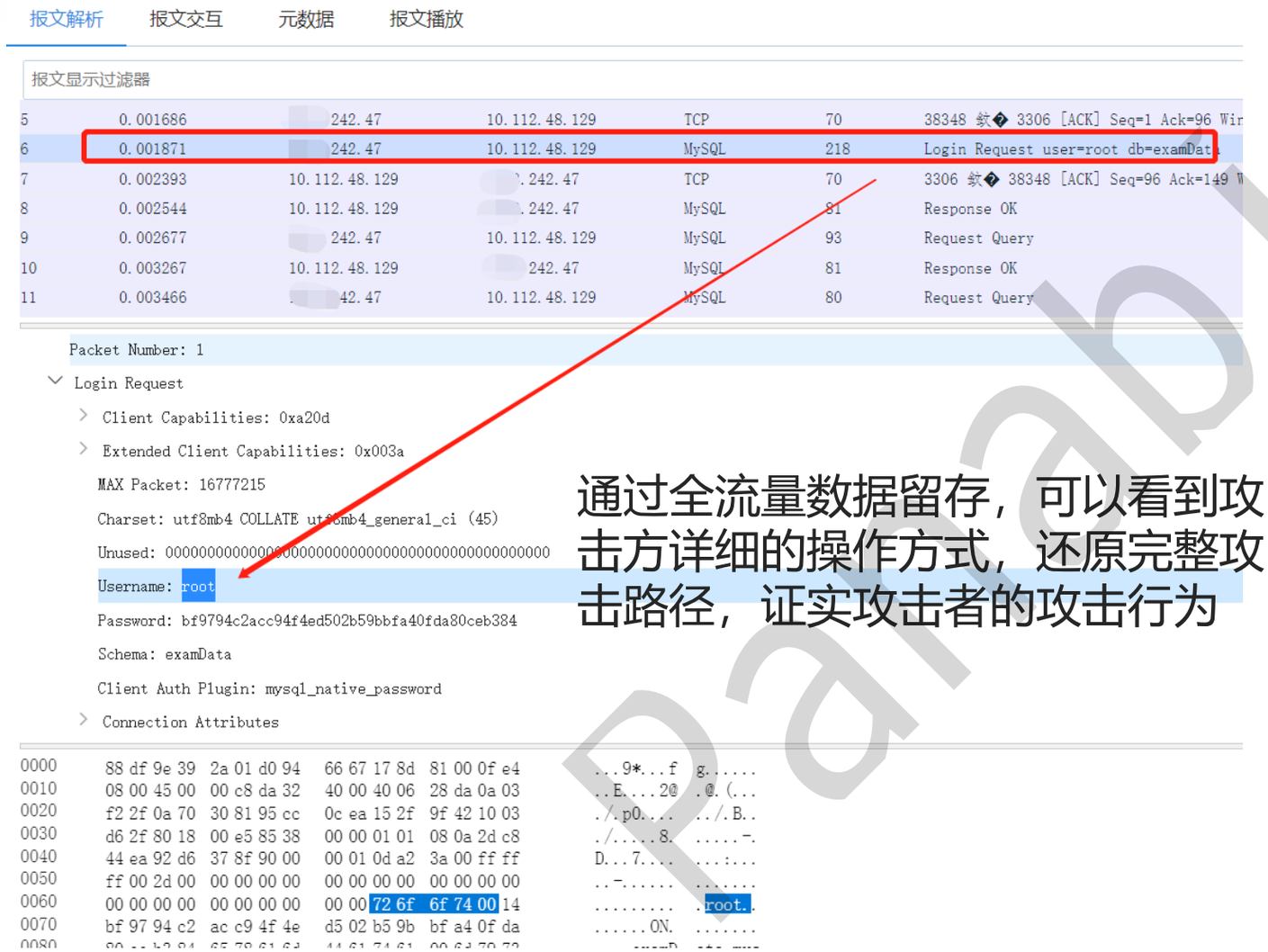
加分项目：

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

全流量数据留存+报文分析



通过全流量数据留存，可以看到攻击方详细的操作方式，还原完整攻击路径，证实攻击者的攻击行为

NTM分析

外网某IP对数据库进行进行**root**登录操作。并且登录成功。

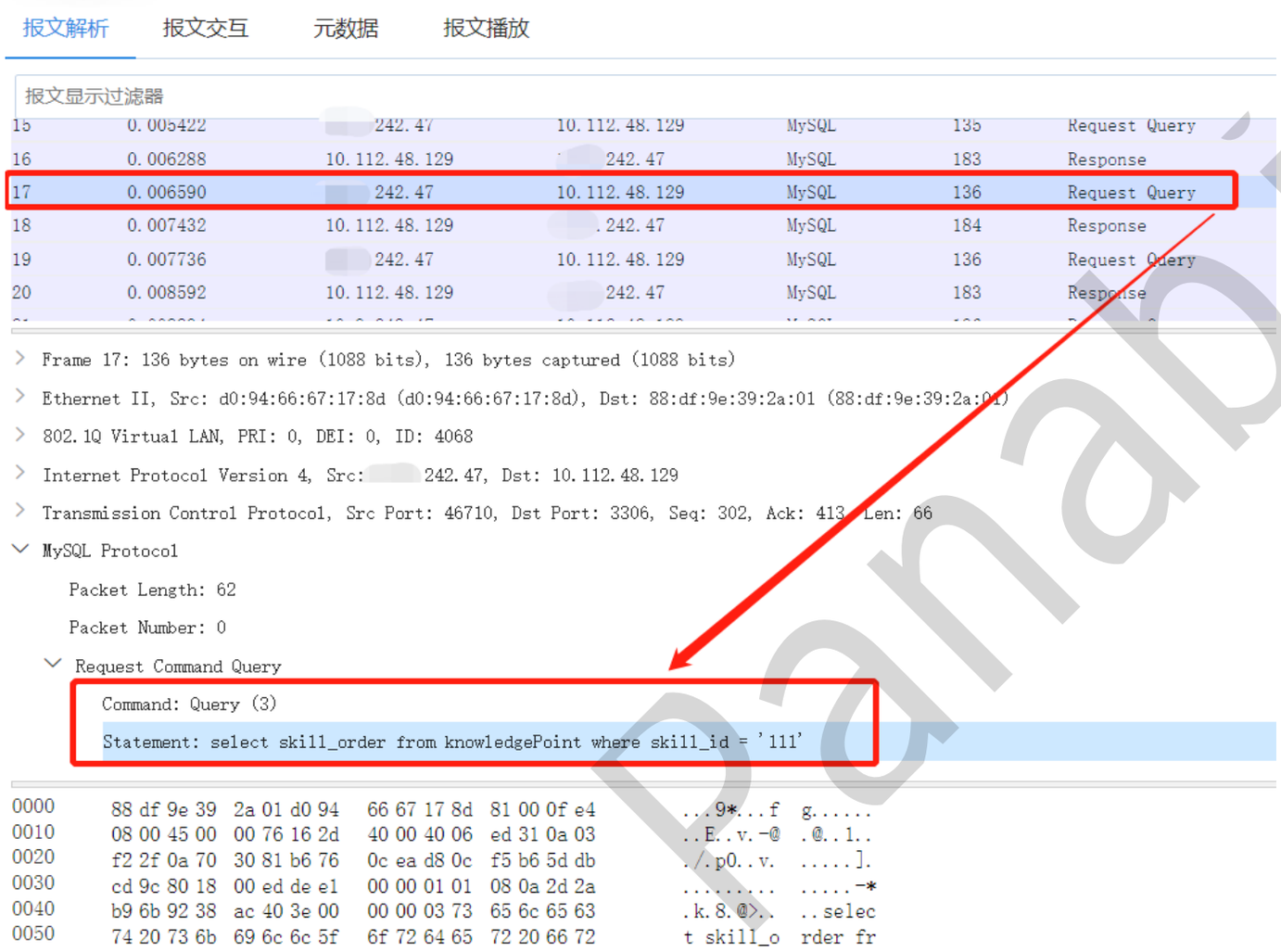
加分项目：

加分类别：发现类

加分标准：发现账号异常

加分：账号异常，加分上限为500分

全流量数据留存+报文分析



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。

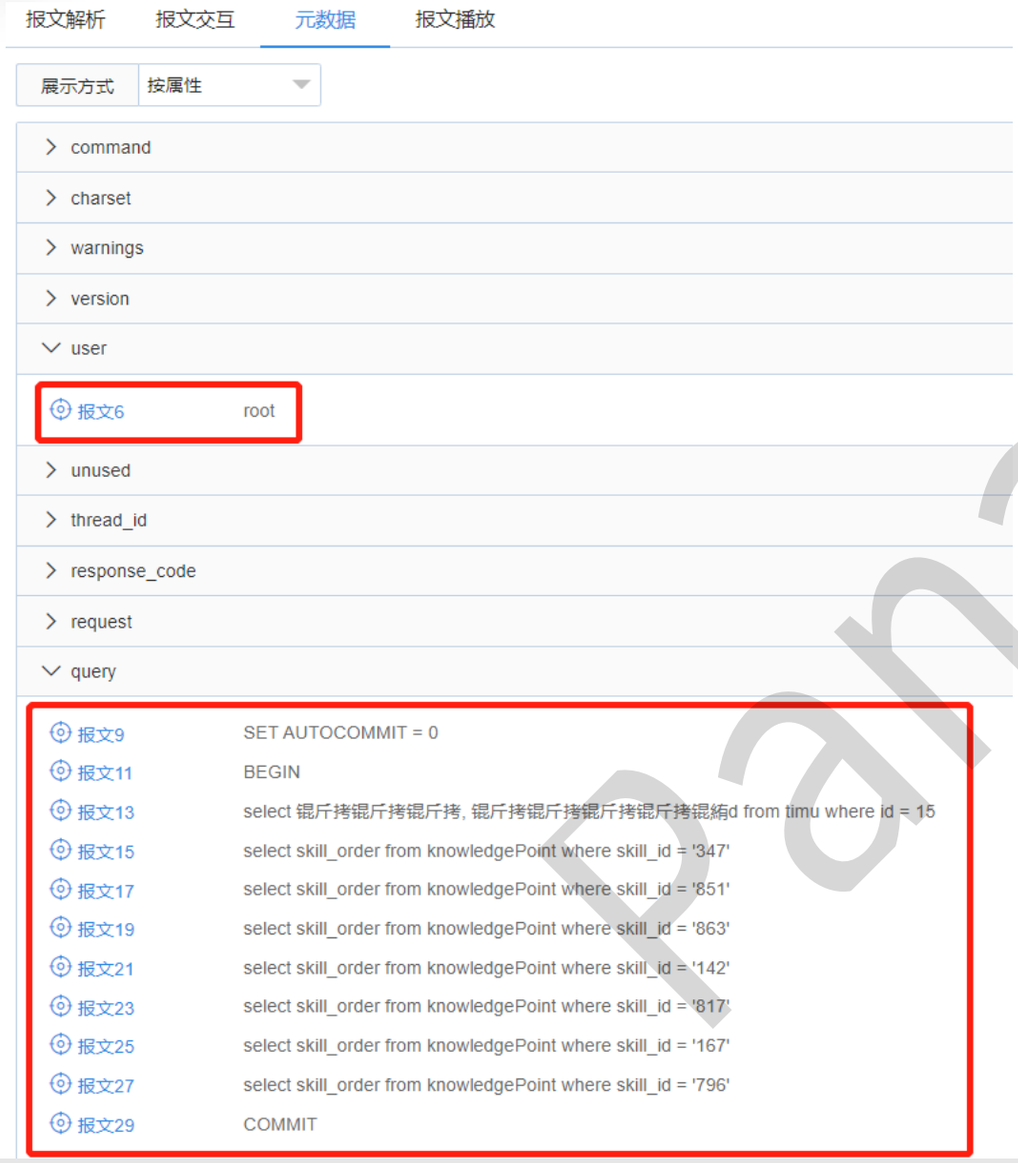
加分项目：

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

全流量数据留存+报文分析



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

全流量数据留存+报文播放

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。

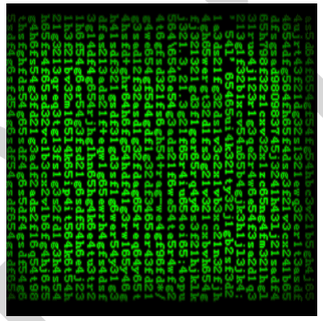
用途：安全取证、压力测试、故障分析、第三方系统联动等。

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
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.h 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.h 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. edu.cn|200		数据包

NTM



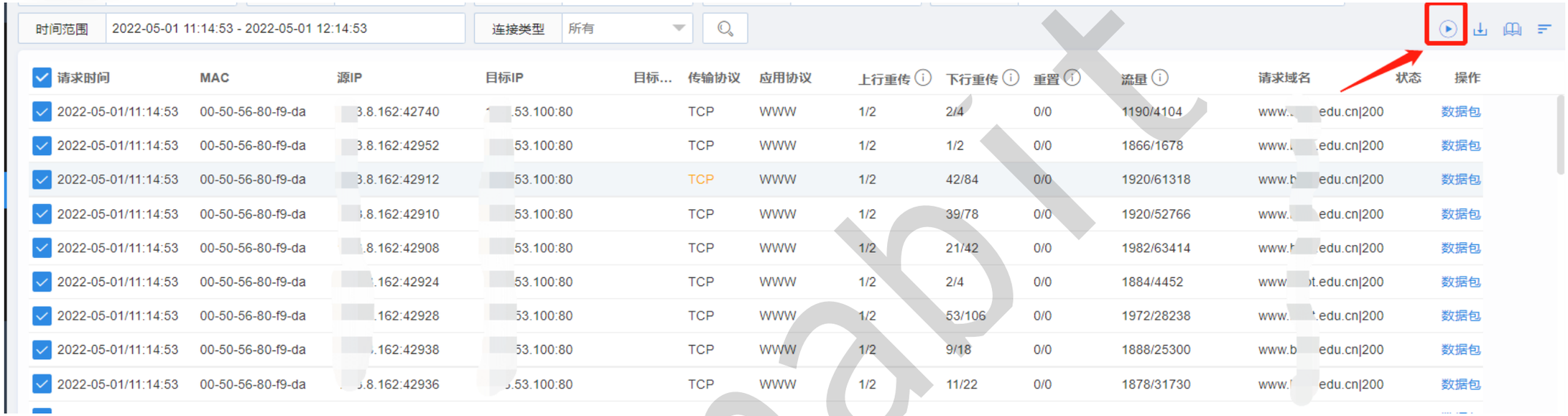
报文播放

杀毒&IDS

=

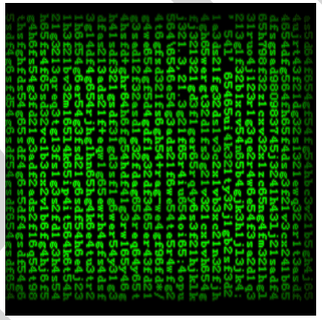
已知病毒&木马审计系统

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.h 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.h 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. edu.cn|200		数据包

NTM



报文播放

沙箱

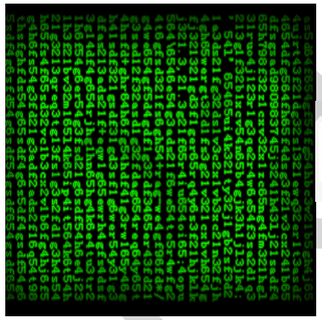
未知病毒&木马分析系统

全流量数据留存+报文播放

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
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.h 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.h 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. 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