



```
print (3 * ' !底家清摸 ' [::-1])
```

厦门大学 郑海山 2019.11.28 西安

```
print(3 * '!底家清摸'[::-1])
```

- Python
- 乘法重载，字符串乘以数字就是将字符串重复多少遍
- 字符串的中括号操作是对字符串进行切片，切片参数3个，start、end、step。步长等于-1就是反转字符串。

```
>>> print(3 * '!底家清摸'[::-1])
摸清家底!摸清家底!摸清家底!
```

RSA 2019

- ▶ 2019年3月4日，RSA 2019，Axonius斩获有着“全球网络安全风向标”之称的创新沙盒的冠军。
- ▶ Axonius 是一家做网络安全资产管理平台（Cybersecurity Asset Management Platform）的公司，主要功能是对用户企业的设备进行管理，包括资产管理、应用管理和补丁管理等。
- ▶ “没技术含量”、“体力活儿”、“开源软件堆一堆”
- ▶ RSA 创新沙箱比赛（RSA Innovation Sandbox Contest）不在于你的技术多么高端，而是看商业模式，是否有投资价值。

RSA 2019

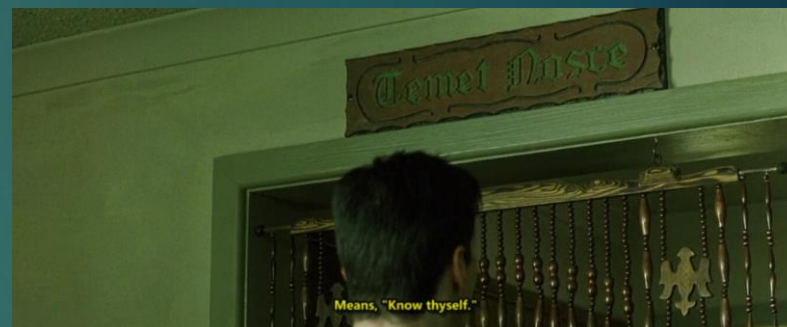
- ▶ When it comes to cybersecurity, what defines better? New tools for building stronger walls? Sharper algorithms for predicting risk? AI and machine learning to help outsmart cybercriminals? That's certainly part of it. Technology always has to move forward. But it's not the only answer.
- ▶ 在网络安全方面，什么是“更好”？是用于建造更坚固墙体的新工具？还是用于风险预测的更精确的算法？亦或是魔高一尺道高一丈的人工智能和机器学习的应用？
- ▶ 不忘初心



You Can't Secure What You Can't See

Axonius网络安全资产管理平台

- ▶ 当听到资产管理的时候，第一印象是资产自动发现或者扫描探测等。但是，Axonius并不是从流量分析，或者主动扫描的方式发现资产，而是对资产进行整合。Axonius的主要技术点在于整合，整合现有安全设备已经监控到的设备。既然是整合现有安全设备已经监控到的，那么它的价值点又是什么？虽然现有的安全产品（比如：EDR、NDR、SIEM等等）多多少少都有自己的资产管理功能，但由于它们受限于某个范围导致资产库是不完整的，他们之间的资产信息形成**竖井**（silo）。
- ▶ 技术剖析 | Axonius为什么能获得 2019 RSAC创新大奖
<https://yq.aliyun.com/articles/693193>
- ▶ RSA2019创新沙盒冠军Axonius，为什么是它？ --走狗是狗哥，安在



The Matrix(1999)

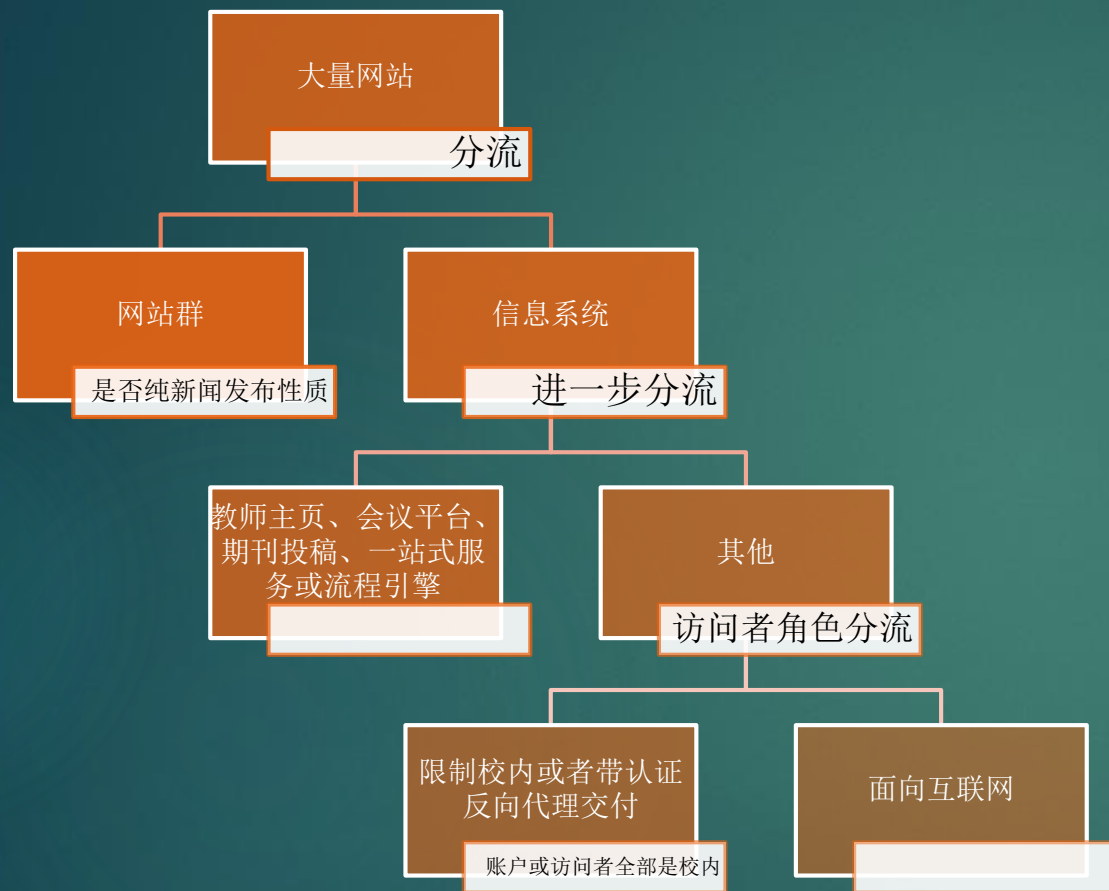
目录

- ▶ 高校常规安全防护手段
- ▶ 摸清家底在厦门大学的实践

高校常规安全防护手段

- ▶ 北大张蓓 《网络与信息安全防护体系建设.pptx》
- ▶ 规划
- ▶ 购买安全设备
- ▶ 购买安全服务
- ▶ 购买信息系统运维服务
- ▶ 网络安全等级保护制度
- ▶ 人的因素：顶层设计、规则、制度、台账。

高校常规安全防护手段：规划



- 分流剥离：按新闻、访问角色剥离部署
- 网站群：《网站群在保障高校网站安全中的重要作用》、《新媒体自媒体等发布平台运营安全相关》
- 教师主页：前台和后台一定要分开。
- 一站式服务或流程引擎：应当无编程，如果有自定义或定制代码每个流程相当于又一个系统。
- 反代：《高等院校Web服务提供IPv6情况随笔》、《5分钟让你的老旧网站支持IPv6、HTTPS、HTTP/2，不能再多了》、《继续说IPv6、HTTPS、HTTP/2，系列完结吧》、《从张焕杰的《校园网站安全防护之Nginx》说开》、《HTTPS是否还会被监听》、《BeyondCorp和高校的落地》

高校常规安全防护手段：购买安全设备

- ▶ 常规：防火墙、IPS、WAF、VPN、堡垒机、日志审计、漏扫、备份
- ▶ 《高校安全设备之买买买攻略》
- ▶ 管理服务器需要VPN拨号+堡垒机，不允许使用任何反向连接的工具，不允许恶意绕过堡垒机和命令行审计，不允许自行打隧道。
- ▶ 东西向防火墙、零信任（Zero-Trust）、微分段（ Micro-segmentation ）、软件定义边界（SDP）
- ▶ 《服务器防火墙设置一网打尽》

高校常规安全防护手段：购买安全设备

- ▶ WAF跟防火墙类似，越靠近被保护对象越好。
- ▶ 规则复杂，对业务影响大。如果能虚拟化给用户自行调整规则是最好，但是要做好隔离，否则一个用户加个死循环正则表达式会把整个WAF打死。
- ▶ WAF更多的是基于规则的匹配。
- ▶ WAF要起作用的部署客户端一定是先跟WAF建立连接，再跟后端建立连接。建议WAF只过非加密流量。
- ▶ 最终的目标是，修改源头，让应用可脱离WAF生存。



Forrest Gump, 1994

高校常规安全防护手段：购买安全服务

- ▶ 安全服务可引入2家，保持多样性，交叉比对，化解工作量。
- ▶ 安全服务包括：上线前安全检查、代码审计、漏洞扫描、渗透测试、配置核查加固、重保服务、安全培训、等保备案、应急响应、威胁情报和安全通告、云检测、安全设备运维等。
- ▶ 渗透测试报告一定要包括：XXX问题不存在，理由。杜绝渗透测试执行不彻底。《年轻人千万不要写代码，基于OWASP Top 10的代码安全》《软件开发最佳实践：代码安全我们需要打什么疫苗》
- ▶ 根据观察，基本上每个系统查下去都有各种中高危问题。每个系统防火墙都不符合最小化原则。

高校常规安全防护手段：购买信息系统运维服务

- ▶ 要求：定期输出运维报告，提交巡检和演练记录
- ▶ 配套：VPN、堡垒机、监控、日志。
- ▶ 监控可以发现一些人无法发现的问题。
- ▶ 《运维的四种境界》、《一键部署Zabbix、Grafana、Icinga、SmokePing监控系统》、《厦门大学：开源监控系统让运维更高效》



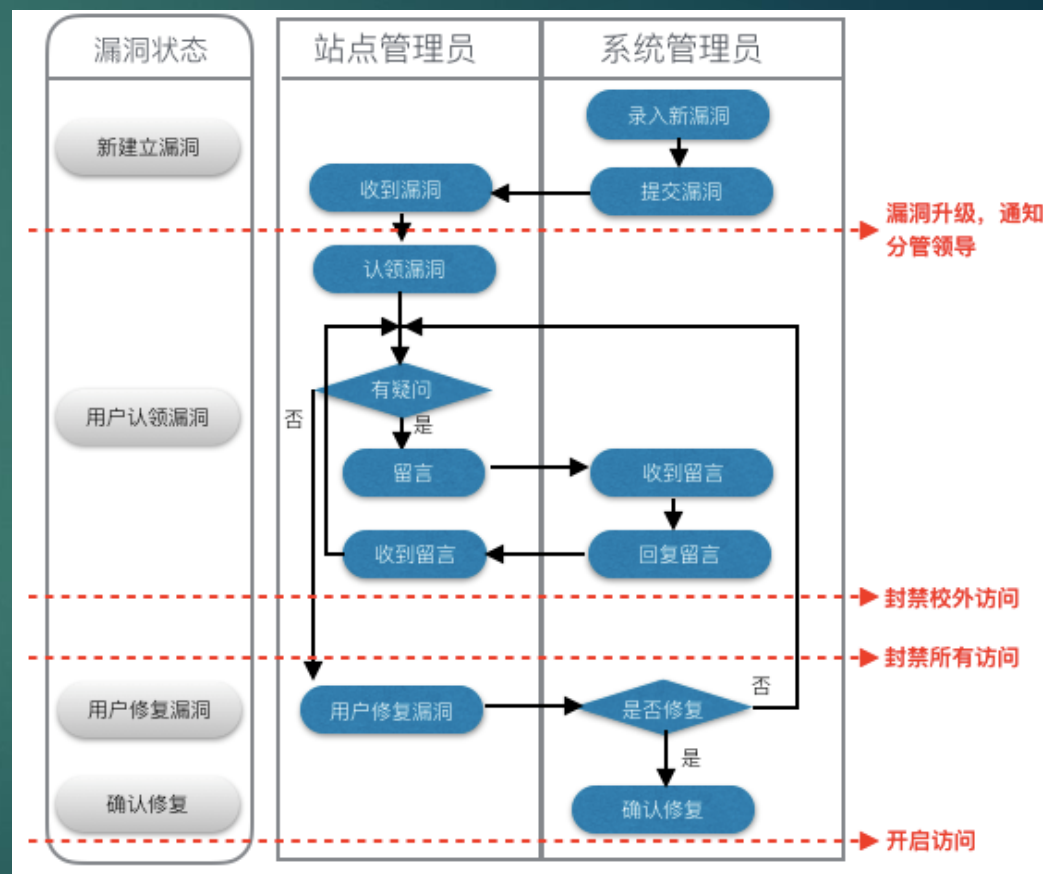
You Can't Secure What You Can't See

备案系统

- ▶ 自研备案系统，所有需要对外提供服务或者有域名的都需要在这个网站上备案联系人和分管领导信息以便可快速应急响应、漏洞全生命周期管理、网址导航、关联分析、读网。
- ▶ 漏洞全生命周期管理：管理各个不同渠道的漏洞，录入，通知，认领，修复，验证，完成。解决以往需要邮件和电话沟通又无法留痕的问题。
- ▶ 江晓莲,郑海山.面向安全漏洞管理的高校备案系统设计与实现[J].网络安全技术与应用,2017,(04):150-152.
- ▶ 郑海山,江晓莲,许卓斌,萧德洪.备案系统记录高校网站安全信用[J].中国教育网络,2018,(Z1):70-73.

备案系统：漏洞全生命周期管理

- ▶ 互联网漏洞平台。在所有较大的互联网漏洞平台申请账户，登记邮件地址。
- ▶ 上级部门通知。区级、市级、省级、部级。
- ▶ 主动恶意代码检测。对信息与网络中心有管理权限的虚拟主机或者虚拟机定期进行恶意代码检测。
- ▶ CVE。
- ▶ 定期查看 WAF 和防火墙日志，找出被 WAF 拦截的地址，识别出可能存在漏洞的站点。
- ▶ 漏洞扫描和渗透测试结果：不纳入，误报和数量太多。



资产建模

- ▶ 资产类型：Web、实体Server、虚拟机、容器、网络设备、IP、URL、客户机、IoT、软件、应用、License、SSL证书、机房、机柜
- ▶ 资产关系复杂：多对多，可变化。服务器有多个IP（IPv4、IPv6（服务、定期变换的隐私IP），内外网，心跳），高可用虚拟IP可以在多个服务器上漂移。服务器有多个域名（虚拟主机）。域名负载均衡在多台服务器上。
- ▶ 反向代理。URL重写，一个URL后面多台服务器，比如Web和数据库分离
- ▶ 安全牛2019/8/16发布《信息资产风险与合规管理 (ITARC) 应用指南》

资产建模

- ▶ 松散耦合
- ▶ 关联分析
- ▶ 差不多先生


关联分析

- ▶ 备案系统数据、堡垒机账户和管理的IP、VPN账户、反代和后端真实服务器、DNS数据、日志集中服务器、监控IP、phpIPAM IP管理数据、VMware（机器名、自定义字段、IP地址）、防火墙、交换机IP/MAC对应、ARP、网段物理位置。
- ▶ 主动探测指纹信息、网络实时HTTP流量分析。
- ▶ 已知的信息（备案系统）和未知的信息（关联出来不在备案系统的）

[illegible]

备案系统数据利用

- ▶ 备案数据一定应当是以数据库形式保存的，可编程调用的。
- ▶ 围绕备案，形成网站全生命周期管理和工作日志：管理员变更情况，年审情况、IP、域名等变更情况。
- ▶ 备案数据可以任意导出成上报需要的数据：IPDB、市局、
ipv6c.cngi.edu.cn



序号	地区	学校数	子网站数	子网站CERNET地址数	子网站CERNET地址百分比	IPv6可达数	IPv6可达百分比	网站可访问数	网站可访问百分比	dnssec	dnssec百分比	IPv6https证书	IPv6https证
	汇总	2,956	56,590	7,971	14.09%	391	13.23%	390	13.19%	14	0.47%	192	
1	安徽	126	2,468	624	25.28%	29	23.02%	29	23.02%	2	1.59%	18	
2	北京	115	3,110	617	19.84%	19	16.52%	19	16.52%	1	0.87%	12	
3	福建	93	1,676	396	23.63%	10	10.75%	10	10.75%	-	-	8	

排序	站点名称	官网	时间	子网站数	子网站CERNET地址数	子网站CERNET地址百分比	IPv4地址	IPv4所属单位	IPv4 AS号	IPv6地址
1	厦门大学	www.xmu.edu.cn	2019-11-26	301	271	90.03%	210.34.0.12	XMU	4538	2001:da8:e800::12

备案系统数据利用：读网

- ▶ 拉网式排查，一个都不能少。
- ▶ 人工读网：专人，结合机器读网，一个个访问备案的网站，记录相关信息，备注进入备案系统，形成工作日志。
- ▶ 机器读网：对每个站点，使用Puppeteer，获取首页的标题、页面下载量、首页原始大小、请求次数、内部链接数、外部链接数、各文件类型大小。统计站点内部链接数。僵尸网站识别：对首页文本进行保存，使用正则表达式分析可能的发布时间。《值班读网》

URL	Title	Error	页面 下载 量 KB	页面 下载 量 MB	首 页 大 小	请 求 次 数	内 部 链 接	外 部 链 接	各文件类型大小
772 http://...u.edu.cn	Home: ...	False	450361K	(448M)	4K	63	8	6	[text/css: '210K', application/javascript: '253K', image/png: '53K', image/jpeg: '143K', video/mp4: '458700K']
678 https://...edu.cn/	站... ..	False	173400K	(169M)	21K	59	48	3	[text/html: '10K', application/javascript: '50K', text/css: '30K', image/jpeg: '35913K', image/png: '3006K', image/gif: '0K', image/svg+xml: '0K', application/font-woff: '95K', video/mpog4: '134232K']
714 http://...u.edu.cn	...	False	108144K	(105M)	29K	46	49	21	[text/html: '35K', text/css: '328K', image/jpeg: '1898K', application/javascript: '130K', image/png: '1K', video/mp4: '105748K']
63 http://...u.edu.cn/		False	87189K	(85M)	391K	92	130	1	[text/html: '33K', image/jpeg: '87000K', image/png: '45K']
174 https://...u.edu.cn/	厦... ..	False	81110K	(79M)	45K	68	76	4	[text/html: '22K', text/css: '27K', application/javascript: '132K', image/jpeg: '605K', image/png: '1632K', image/bmp: '78600K', image/gif: '0K']
168 https://...u.edu.cn/	厦... ..	False	76290K	(76M)	61K	95	248	16	[text/html: '15K', text/css: '34K', application/javascript: '54K', image/jpeg: '74984K', image/png: '3200K', image/gif: '0K', image/svg+xml: '0K']

-
- Four horizontal bar charts are shown, each representing a different percentage. The first bar is orange and labeled '100%'. The second bar is green and labeled '75%'. The third bar is purple and labeled '50%'. The fourth bar is blue and labeled '25%'. Each bar is contained within a black rectangular frame.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	厂商	单位	网站名	URL	联系人姓名	联系人电话	联系人邮件	登记时间	开始时间	结束时间	整改结束时间	二次验证结束时间	厂商对接人	高危漏洞单描述	备注
2			报名系统	http://mu.edu.cn										密码库漏洞 漏洞	安全

关联分析：工程化内容

- ▶ 坑
- ▶ VMware多台服务器IP地址一样：微分段，旧服务器断网不关机。
- ▶ 反向代理：配置了，不启用。
- ▶ 反向代理：必须拿到后端真实IP。被反代后，我们建议用户只对反代开放HTTP端口，对漏扫、探针开放所有端口。探针主动扫描必须带域名，探针需要切换被信任IP和非信任IP。
- ▶ 内网：探针部入，传递数据出来
- ▶ 主动探测：URL多次重定向。多个系统重定向到统一身份认证。
- ▶ 主动探测：多个探测任务耗时不同。获取IP/MAC会丢失数据，需要短期多次取全量
- ▶ 主动探测：错误数据、噪音、伪造Banner

关联分析：工程化内容

- ▶ 每时每刻获取指纹等信息，如何将这些信息存储？
- ▶ 时序数据库。按时间存储。
- ▶ 引入批次的概念，在一次大的批次启动后，可以在批次内将多个主动扫描串起来，形成资产快照。
- ▶ 使用版本控制理念对数据进行折叠：比如对某服务器一年之内端口扫描的一千多次结果，相同进行合并。



向二级学院提供安全能力

- ▶ 《复旦大学：新型信息资产治理平台为二级单位安全赋能》
- ▶ 《厦门大学：让二级学院也拥有漏洞扫描能力》
- ▶ 开放安全能力：漏扫，堡垒机。备份由虚拟化提供。如何将日志、安全设备看到的内容向二级学院开放？
- ▶ 建立校内QQ群，备案网站超过3个，邀请入群
- ▶ 结合安全服务，组织培训，技术交流，情况介绍。

Shodan

Shodan 是一个搜索引擎，用来搜索网络空间中的在线设备

工作原理：Shodan 通过扫描全网设备并抓取解析各个设备返回的 banner 信息。

Shodan新手入坑指南

<https://www.freebuf.com/sectool/121339.html>

《The Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work For You.》by John Matherly


shodan.io/search?query=www.google.com

SHODAN www.google.com Explore Pricing Enterprise Access

Exploits Maps

TOTAL RESULTS
478,961

TOP COUNTRIES



United States	107,908
Brazil	50,629
Russian Federation	27,861
Viet Nam	16,681
Thailand	13,929

TOP SERVICES

HTTP	270,025
HTTPS	197,750
8081	1,968
8880	1,636
8083	722

TOP ORGANIZATIONS

Google	53,499
Amazon.com	12,724
Vietnam Posts and Telecommunications(VNPT)	7,058
Vivo	6,024
3BB Broadband	3,509

TOP OPERATING SYSTEMS

Linux 3.x	466
Windows 7 or 8	72
Linux 2.6.x	21
FreeBSD 8.x	10
Windows XP	4

TOP PRODUCTS

nginx	13,108
Apache httpd	6,635
Connectra Check Point Web Security httpd	6,458
Microsoft IIS httpd	3,199
Jetty	268

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

403 Forbidden
134.39.241.61
work.spsc.edu
Washington State K-20 Telecommunications Network
Added on 2019-11-22 03:36:55 GMT
United States, Olympia
HTTP/1.1 403 Forbidden
Date: Fri, 22 Nov 2019 03:33:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 564
Connection: keep-alive
Location: http://www.google.com/#q=

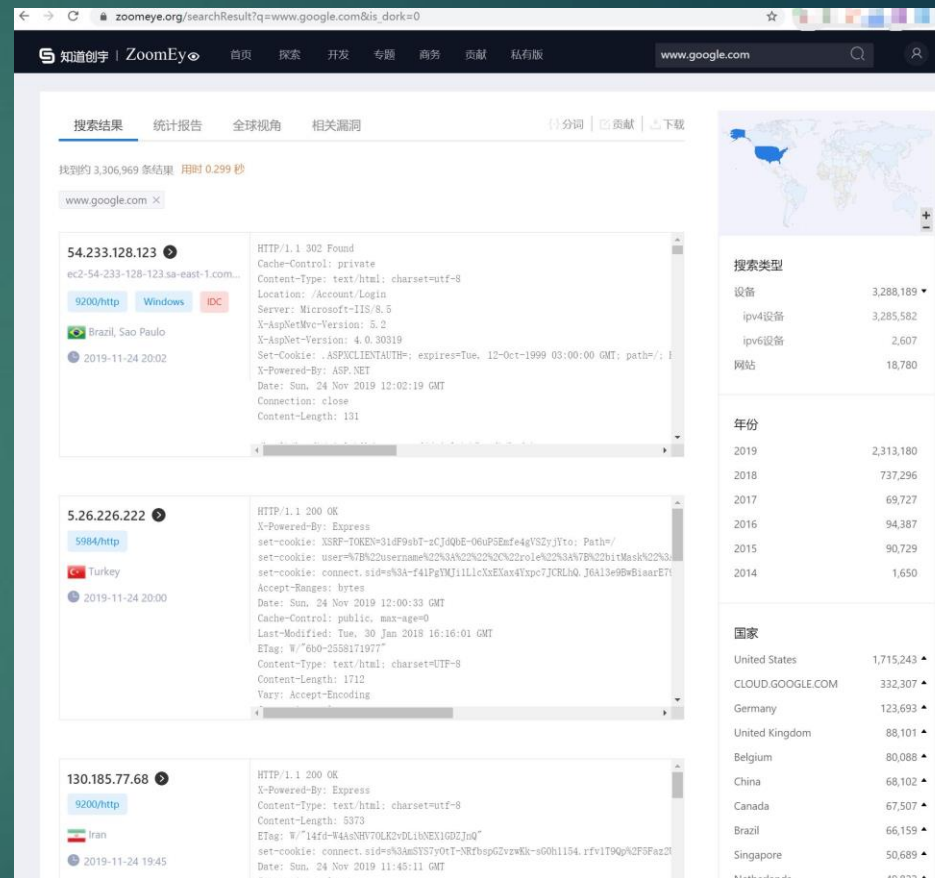
301 Moved
172.217.17.68
ams16a30-in-f68.1e100.net
ams16a30-in-f4.1e100.net
Google
Added on 2019-11-22 03:36:45 GMT
United States
SSL Certificate
Issued By: GTS CA 101
Organization: Google Trust Services
Issued To: www.google.com
Organization: Google LLC
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Fri, 22 Nov 2019 03:33:19 GMT
Expires: Fri, 22 Nov 2019 03:33:19 GMT
Cache-Control: private, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: S...

302 Moved
172.217.17.68
ams16a30-in-f68.1e100.net
ams16a30-in-f4.1e100.net
Google
Added on 2019-11-22 03:37:05 GMT
United States
HTTP/1.1 302 Found
Location: https://www.google.com/?gws_rd=ssl
Cache-Control: private
Content-Type: text/html; charset=UTF-8
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Fri, 22 Nov 2019 03:33:39 GMT
Server: gws
Content-Length: 231
X-XSS-Protection: 0
X-Frame-Options: S...

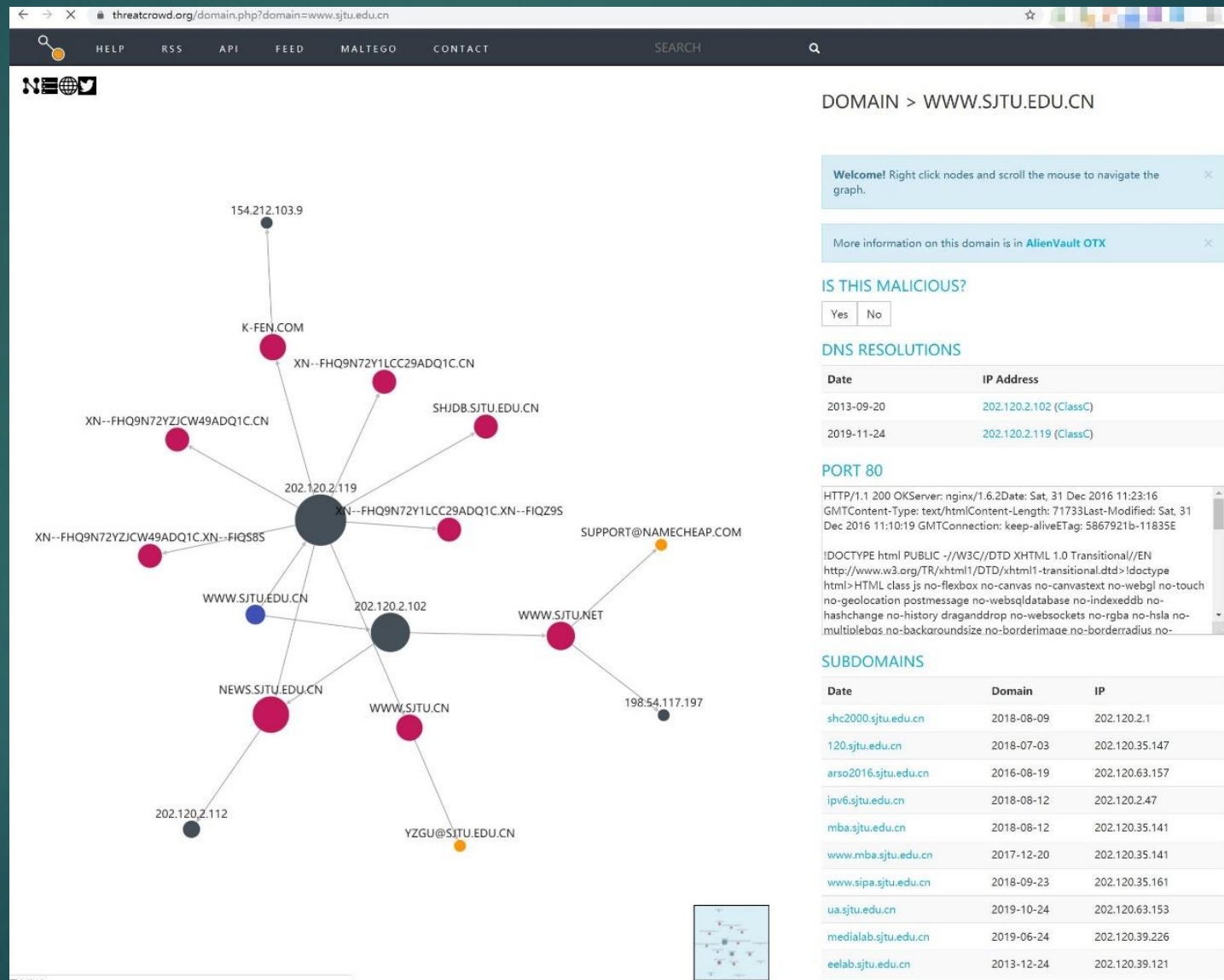
301 Moved
172.217.168.237
ams15a40-in-f13.1e100.net
Google
Added on 2019-11-22 03:37:00 GMT
United States
SSL Certificate
Issued By: GTS CA 101
Organization: Google Trust Services
Issued To: accounts.google.com
Organization: Google LLC
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Fri, 22 Nov 2019 03:33:35 GMT
Expires: Fri, 22 Nov 2019 03:33:35 GMT
Cache-Control: private, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: S...

ZoomEye

- ▶ ZoomEye是一款针对网络空间的搜索引擎，收录了互联网空间中的设备、网站及其使用的服务或组件等信息。
- ▶ ZoomEye 拥有两大探测引擎：Xmap 和 Wmap，分别针对网络空间中的设备及网站，通过 24 小时不间断的探测、识别，标识出互联网设备及网站所使用的服务及组件。研究人员可以通过 ZoomEye 方便的了解组件的普及率及漏洞的危害范围等信息。
- ▶ 虽然被称为“黑客友好”的搜索引擎，但 ZoomEye 并不会主动对网络设备、网站发起攻击，收录的数据也仅用于安全研究。ZoomEye更像是互联网空间的一张航海图。



ThreatCrowd: A Search Engine for Threats



- 
- ▶ 不能让互联网公司更懂我们
 - ▶ 不能让黑客更懂我们
 - ▶ 利用好内网权限和对各个管理系统的管理员权限，建立自己的管理员工具

```
print(''.join(['感', '谢', '聆', '听', '!']))
```



微信公众号：郑海山dump

haishion AT xmu DoT edu dOt cn

<https://dog.xmu.edu.cn>