Kali系统工具使用

渗透测试环境搭建 第2课

360
网络安全学院

教学目标

- 掌握Kali下小工具以及命令的使用

参考资料：《Kali Linux渗透测试的艺术》

https://tools.kali.org/tools-listing

目录

Chrome浏览器的使用及简单linux使用

360网络安全学院

- chrome运行问题
- 修改用户密码
- Vim的使用

Chrome浏览器的使用

360网络安全学院

- chrome不能以特权用户身份运行
  - 创建一个新用户chromeuser
  - useradd –d /usr/chromeuser -m chromeuser

```
root@kali:~# google-chrome
[7236:7236:0222/214411.976367:ERROR:zygote_host_impl_linux.cc(90)] Running as ro
ot without --no-sandbox is not supported. See https://crbug.com/638180.
```

Chrome浏览器的使用

- 命令su chromeuser -c google-chrome出错
  - 原因：chromeuser无权在root登陆的可视化界面内展开图形程序
  - 解决方案：以root用户身份解除限制
  - xhost +

```
root@kali:~# su chromeuser -c google-chrome
No protocol specified
(google-chrome:7416): Gtk-WARNING **: cannot open display: :1
```

```
root@kali:~# xhost +
access control disabled, clients can connect from any host
```

修改用户密码

- root用户下：passwd [用户名]——修改其他用户密码
- 比如：passwd chromeuser
- 任意用户：passwd 修改自己的密码

Vim的使用

- 命令：vim [文件名]
- 作用：查看或编辑该文件，如果文件不存在则在保存文件时文件会被创建

Vim的使用

360 网络安全学院

- Vim的三种模式
- 1、normal mode
- 2、insert mode
- 3、command-line mode

Vim的使用

360 网络安全学院

- 输入“vim [文件名]”后进入normal mode
- 左下角显示“—插入--”或“--insert--”代表vim正在insert mode下
- Insert mode下按esc返回normal mode
- Normal mode下按“:”进入command-line mode

Vim的使用

360 网络安全学院

- 简单使用指南：
- 1、vim [文件名]打开文件进行预览
- 2、按“i”对文件进行编辑
- 3、编辑完成后按“esc”退回预览
- 4、“:wq”保存文件并退出vim

Kali Linux前期信息收集工具

Kali Linux前期信息收集工具

- whois
- dmitry
- 域名枚举-dnsenum
- 子域名爆破-subDomainsBrute
- 指纹识别-whatweb
- 网站目录扫描-dirsearch

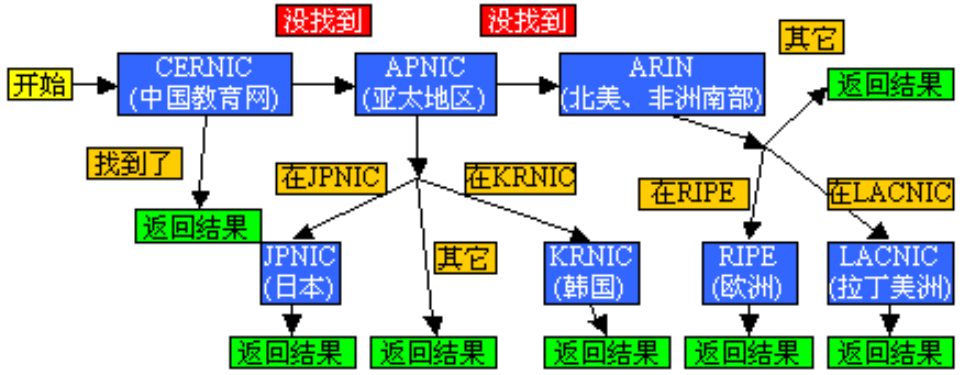
Kali Linux工具分类

360网络安全学院

- 信息收集（Information gathering）
- 无线攻击（Wireless Attacks）
- 密码破解 （Password Attacks）
- 压力测试（Stress Testing）
- 取证工具（Forensics Tools）
- 逆向工程（Reverse Engineering）
- 硬件攻防（Hardware Hacking）
- 漏洞挖掘（Vulnerability Analysis）
- Web应用（Web Applications）
- 漏洞利用工具（Exploitation Tools）
- 嗅探和欺骗（Sniffing & Spoofing）
- 后门维持（Maintaining Access）
- 情报分析（Reporting Tools）

whois

- whois是用来查询域名的IP以及所有者等信息的传输协议。简单说，whois就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册
- RFC812定义了一个非常简单的Internet信息查询协议——WHOIS协议。其基本内容是，先向服务器的TCP端口43建立一个连接，发送查询关键字并加上回车换行，然后接收服务器的查询结果。）



whois

360 网络安全学院

- whois [域名]——快速查询whois

```
root@Kali:~# whois 360.cn
Domain Name: 360.cn
ROID: 20030311s10001s00024165-cn
Domain Status: clientDeleteProhibited
Domain Status: clientTransferProhibited
Registrant ID: ename_g83uqdpzra
Registrant: 北京奇虎科技有限公司
Registrant Contact Email: domainmaster@360.cn
Sponsoring Registrar: 厦门易名科技股份有限公司
Name Server: dns1.360safe.com
Name Server: dns2.360safe.com
Name Server: dns3.360safe.com
Name Server: dns7.360safe.com
Name Server: dns8.360safe.com
Name Server: dns9.360safe.com
Registration Time: 2003-03-17 12:20:05
Expiration Time: 2019-03-17 12:48:36
DNSSEC: unsigned
```

dmitry

- Dmitry（Deepmagic Information Gathering Tool）是一个由C语言编写的UNIX/(GNU)Linux命令行工具，它可用于收集主机相关信息，比如子域名、Email地址、系统运行时间信息，它是一个简单的信息收集集成工具
  - 根据IP（或域名）来查询目标主机的Whois信息
  - 在Netcraft.com的网站上挖掘主机信息
  - 查找目标域中用的子域
  - 对目标主机进行Email地址搜索，查找目标域的电子邮件地址
  - 对目标主机进行TCP端口扫描（Portscan），探测目标主机上打开的端口、被屏蔽的端口和关闭的端口

dmitry

360 网络安全学院

```
root@Kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered
ts
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

```
root@Kali:~# dmitry -iwnsepfb www.so.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:111.206.81.174
HostName:www.so.com

Gathered Inet-whois information for 111.206.81.174
---------------------------------


inetnum:        111.0.0.0 - 111.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------------
```

域名枚举-dnsenum

- dnsenum [options] <domain>
- 可使用-f指定用于子域名爆破的字典

```
root@kali:~/Desktop/subDomainsBrute-master/dict# proxychains dnsenum -f subnames
.txt baidu.com
ProxyChains-3.1 (http://proxychains.sf.net)
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----   baidu.com   -----
```

子域名爆破-subDomainsBrute

360 网络安全学院

- 特点：自带了一个常用字典
- 可使用-f指定用于子域名爆破的字典

```
root@kali:~/Desktop/subDomainsBrute-master# python subDomainsBrute.py baidu.com
[+] Validate DNS servers
[+] Server 182.254.116.116  < OK >   Found 1
[+] 1 available DNS Servers found in total
[+] Init 6 scan process.
[*] 12 found, 16059 scanned in 180.8 seconds, 88 groups left                ^[
```

指纹识别-whatweb

360 网络安全学院

- 识别网站指纹
- 方便易用

```
root@kali:~/Desktop/subDomainsBrute-master# whatweb https://www.360.cn
https://www.360.cn [200 OK] Country[CHINA][CN], HTML5, HTTPServer[nginx], IP[36.
110.213.49], JQuery, Lightbox, Script[text/template], Title[360官网 - 360安全软
件 - 360智能硬件 - 360智能家居 - 360企业服务], nginx
```

网站目录扫描-dirsearch

360 网络安全学院

- 网址：https://github.com/maurosoria/dirsearch
- 快速扫描网站目录
- 能发现常见的备份文件泄露

```
root@kali:~/Desktop/dirsearch-master# python3 dirsearch.py -u 360.cn -e php

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: php | Threads: 10 | Wordlist size: 5961

Error Log: /root/Desktop/dirsearch-master/logs/errors-18-02-22_23-44-01.log

Target: 360.cn

[23:44:07] Starting:
[23:44:15] 400 -  166B  - /%2e%2e/google.com
[23:44:15] 301 -  178B  - /php  ->  http://www.360.cn/php
```

Nmap的简单使用

Nmap的简单使用

- Nmap简单演示
- -p 指定端口
- -sI TCP空闲扫描

Nmap简单演示

360 网络安全学院

- 典型使用

```
root@kali:~/Desktop/subDomainsBrute-master/dict# nmap 360.cn

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-22 23:55 UTC
Nmap scan report for 360.cn (221.181.72.140)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 50.41 seconds
```

-p指定端口

360 网络安全学院

- 该命令用于指定扫描端口或端口范围

```
root@kali:~/Desktop/subDomainsBrute-master/dict# nmap -p 80 360.cn

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-22 23:59 UTC
Nmap scan report for 360.cn (36.110.213.49)
Host is up (0.0061s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

总结

360 网络安全学院

- Chrome浏览器的使用
- Vim的使用
- Kali Linux小工具的使用

谢谢

360
网络安全学院