服务扫描

作者：someone38063
原文链接：https://ld246.com/article/1558858386949
来源网站：链滴

服务扫描

- 识别开放端口上运行的应用
- 识别目标操作系统
- 提高攻击效率
- Banner捕获
- 服务识别
- 操作系统识别
- SNMP分析
- 防火墙识别

服务扫描

- Banner
- 软件开发商
- 软件名称
- 服务类型
- 版本号
- 直接发现已知的漏洞和弱点
- 连接建立后直接获取Banner
- 另类服务识别方法
- 特征行为和响应字段
- 不同的响应可用于那个与识别底层操作系统

SNMP

- 简单网络管理协议
- Community Strings
- 信息查询或重新配置
- 识别和绕过防火墙筛选

服务扫描————Banner

nc -nv ip port

Python socket

• socket模块用于连接网络服务

• import socket

• bangrab = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

• bangrab.connect(("192.168.1.1",21))

•bangrab.recv(4096) //recv()接收数据

>'220(vsftpd 2.3.4)\r\n'

• bangrab.close() //关闭对象

• exit()

• 有些系统或软件Banner不允许抓取，recv函数无返回将挂起

• ./ban_grab.py 192.168.1.1 1 100

---

banner_grab.py

```
#!/usr/bin/python
import socket
import select
import sys

if len(sys.argv) != 4:
print "Usage ./banner_grab.py [target-ip] [first port] [last port]"
print "Example ./banner_grab.py 192.168.1.1 1 100"
print "EXample will grab banners for TCP ports 1 though 100 on 192.168.1.1"
exit()
ip = sys.argv[1]
start = int(sys.argv[2])
```

```
end = int(sys.argv[3])

for port in range(start,end):
try:
bangrab = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
bangrab.connect((ip,port))
ready = select.select([bangrab],[],[],1)
if ready[0]:
print "TCP Port" + str(port) + "-" + bangrab.recv(4096)
bangrab.close()
except:
pass
```

服务扫描————Banner

- dmitry -p 172.16.36.135
- dmitry -pb 172.16.36.135

- nmap -sT 1.1.1.1 -p 22 --script=banner

服务扫描————Banner

- amap -B 172.16.36.135 21
- amap -B 172.16.36.135 1-65535
- amap -B 172.16.36.135 1-65535 | grep on

服务扫描————服务识别

- Banner信息抓取能力有限

- nmap响应特征分析识别服务
- 发送系列复杂的嗅探
- 依据响应特征signature

nc -nv ip port

nmap ip -p port -sV

- amap 192.168.1.134 80
- amap 172.16.36.135 20-30
- amap 172.16.36.135 20-30 –q
- amap 172.16.36.135 20-30 -qb

操作系统识别

- 操作系统识别技术
- 种类繁多
- 好产品采用多种技术组合
- TTL起始值
- WIndows：128（65~128）
- Linux/Unix：64（1-64）
- 某些UNix：255

nmap使用多种技术识别操作系统

- nmap 192.168.1.1 -O
- 系统服务特征

- xprobe2 1.1.1.1
- 结果有误差

- 被动操作系统识别
- IDS
- 抓包分析
- 被动扫描
- p0f：监听流量，分析数据包，猜测目标操作系统（命令：p0f）

- 结合ARP地址欺骗识别全网OS

SNMP扫描

snmp：（简单网络管理协议），服务端一般为UDP161，客户端162端口；明文传输

- snmp
- 信息的金矿
- 经常被错误配置
- public/private/manager
- MIB Tree
- SNMP Management Information Base (MIB)
- 树形的网络设备管理功能数据库
- 1.3.6.1.4.1.77.1.2.25
- onesixtyone 1.1.1.1 public
- onesixtyone -c dict.txt -i hosts -o my.log -w 100（i：主机列表文件）

- snmpwalk 192.168.20.199 -c public -v 2c (c：community，v：smp版本)
- 用户
- snmpwalk -c public -v 2c 1.1.1.1 1.3.6.1.4.1.77.1.2.25（oid）
- snmpcheck -t 192.168.20.199
- snmpcheck -t 192.168.20.199 -c private -v 2
- snmpcheck -t 192.168.20.199 -w

Server Message Block协议（服务器消息块）

常用端口139、445

- 微软历史上出现安全问题最多的协议
- 实现复杂
- 默认开放
- 文件共享
- 空会话未身份认证访问（SMB1）
- 密码策略
- 用户名
- 组名

- 机器名
- 用户、组SID

版本	操作系统
SMB1	Windows 2000/xp/Windows 2003
SMB2	Windows Vista SP1/Windows 2008
SMB2.1	Win 7/Windows 2008 R2
SMB3	Win 8/Windows 2012

- nmap -v -p139,445 192.168.60.1-20
- nmap 192.168.60.4 -p139,445 --script=smb-os-discovery.nse
- nmap -v -p139,445 --script=smb-check-vulns --script-args=unsafe=1 1.1.1.1
- nbtscan -r 192.168.60.0/24
- enum4linux -a 192.168.60.10

- nc -nv 1.1.1.1 25 • VRFY root
- nmap smtp.163.com -p25 --script=smtp-enum-users.nse --script-args=smtp-enumusers.methods={VRFY}
- nmap smtp.163.com -p25 --script=smtp-open-relay.nse
- smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
- ./smtp.py

SMTP扫描

通常运行在25端口

- nc -nv 1.1.1.1 25
- VRFY root
- nmap smtp.163.com -p25 --script=smtp-enum-users.nse --script-args=smtp-enumusers.methods={VRFY}
- nmap smtp.163.com -p25 --script=smtp-open-relay.nse
- smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1

smtp.py

```
 #!/usr/bin/python
import socket
import sys
if len(sys.argv) != 2:
print "Usage smtp.py ,<username>"
sys.exit(0)
s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect = connect(("192.168.1.1",25))
banner = s.recv(1024)
print banner
s.send("VRFY" + sys.argv[1] + '\r\n')
result = s.recv(1024)
print result
s.close()
```

##防火墙识别

- 通过检查回包，可能是别端口是否经过防火墙过滤
- 设备多种多样，结果存在一定误差

Send	Response	Type
SYN	NO	Filtered
ACK	RST	Filtered
Syn	SYN+ACK/SYN+RST	Filter d
ACK	NO	Filtered
SYN	SYN+ACK/SYN+RST	Unfil ered / OPEN
ACK	RST	Unfiltered / OPEN
SYN	NO	CLosed
ACK	NO	CLosed

防火墙识别

- nmap有系列防火墙过滤检测功能
- nmap -sA 192.168.1.1 -p 22

负载均衡识别

分为广域网负载均衡和服务器负载均衡

- 广域网负载均衡原理为DNS轮询，一个域名解析到多个IP；智能DNS，链路质量判断

• HTTP-Loadbalancing

• Nginx

• Apache

● loading balancing detector

• lbd www.baidu.com

• lbd mail.163.com

WAF识别

● WEB应用防火墙

• wafw00f -l （l：列出能检测的WAF）

• wafw00f http://www.microsoft.com

• nmap www.microsoft.com --script=http-waf-detect.nse

nmap的常用参数

主机发现

* iR（num hosts）：choose random target

* --exclude [host1] [host2]：不扫这些地址/网络

* sL：相当于计算子网掩码功能

* Pn：有防火墙的时候应用，扫主机

* PS/PA/PU/PY：分别为TCP：SYN/ACK、UDP、SCTP发现端口

* PE/PP/PM：icmp echo、timestamp、netmask

* PO：ip扫描

* n：不做dns解析

* --dns-server：用指定的dns服务器

* --traceroute：路由追踪

端口发现

nmap默认用syn扫描

* sU：UDP扫描

* sI [zombie host]：Idle scan

* b [ftp relay host]：ftp bounce scan

* -p U: :UDP -p T: :TCP

* F：fast mode，

* r：连续扫描

服务扫描

* sV：nmap利用集成的特征库进行匹配

##Firewall/IDS EVASION AND SPOOF

* D [decoy1] [decoy2] [decoy3]...:伪造更多的IP地址去扫描目标，从而隐蔽自己的地址

* S [ip1] [dst.ip]：欺骗源地址，同时会建议你加e参数指定网络接口

* g [port]：欺骗源端口

* --proxies [url1] [url2] [url3] ...:使用代理

* --data [hex string]：增加data字段（必须为16进制数）

* --data-string [string]：ASCII string

* --spoof-mac [mac address]：欺骗mac

* badsum：check sum差错校验，发送不完整包