
网络攻防实战

第5周-2

陈健

chenj@nju.edu.cn

靶机demo 1的渗透测试

<https://box.nju.edu.cn/f/15b768edb5904b1c8f24/?dl=1>

主机发现

- arp-scan -l
- arping
 - for octet in {1..254}; do arping -c 1 10.0.2.\$octet; done
- netdiscover
 - netdiscover -r 10.0.2.0/24

主机发现: ping

□ 扫描网段

- for octet in {1..254}; do ping -c 1 10.0.2.\$octet -W 1 >> pingsweep.txt & done
- cat pingsweep.txt | grep "bytes from"
- cat pingsweep.txt | grep "bytes from" | cut -d " " -f4 | cut -d ":" -f1 > targets.txt

主机发现: nmap

- `sudo nmap -sn -iL ranges.txt -oA pingsweep -PE`
 - `-sn`: Ping Scan - disable port scan
 - `-iL` : Input from list of hosts/networks
 - `-oA` : Output in the three major formats at once
 - `-PE/PP/PM`: ICMP echo, timestamp, and netmask request discovery probes
 - `grep "Up" pingsweep.gnmap`
 - `grep "Up" pingsweep.gnmap | cut -d " " -f2 > targets.txt`
-

主机发现： RMI端口发现

- Top five RMIs
 - Microsoft Remote Desktop (RDP): TCP 3389
 - Secure Shell (SSH): TCP 22
 - Secure Shell (SSH): TCP 2222
 - HTTP/HTTPS: TCP 80, 443
 - nmap -Pn -n -p 22,80,443,2222,3389 -iL ranges.txt -oA rmisweep
 - -Pn: Treat all hosts as online -- skip host discovery
 - -n/-R: Never do DNS resolution/Always resolve
 - -p : Only scan specified ports
 - nmap -Pn -n -p 22,80,443,2222,3389 -iL ranges.txt -oA rmisweep --min-hostgroup 256 --min-rate 1280
 - cat rmisweep.gnmap | grep open | cut -d " " -f2
-

主机发现：其他方法

- DNS brute-forcing
 - atk6-dnsdict6
 - <https://github.com/blark/aiodnsbrute>
- Packet capture and analysis
 - Wireshark
 - tcpdump
- Hunting for subnets
 - sudo nmap -sn 10.0-255.0-255.1 -PE --min-hostgroup 10000 --min-rate 10000

开放端口和服务发现

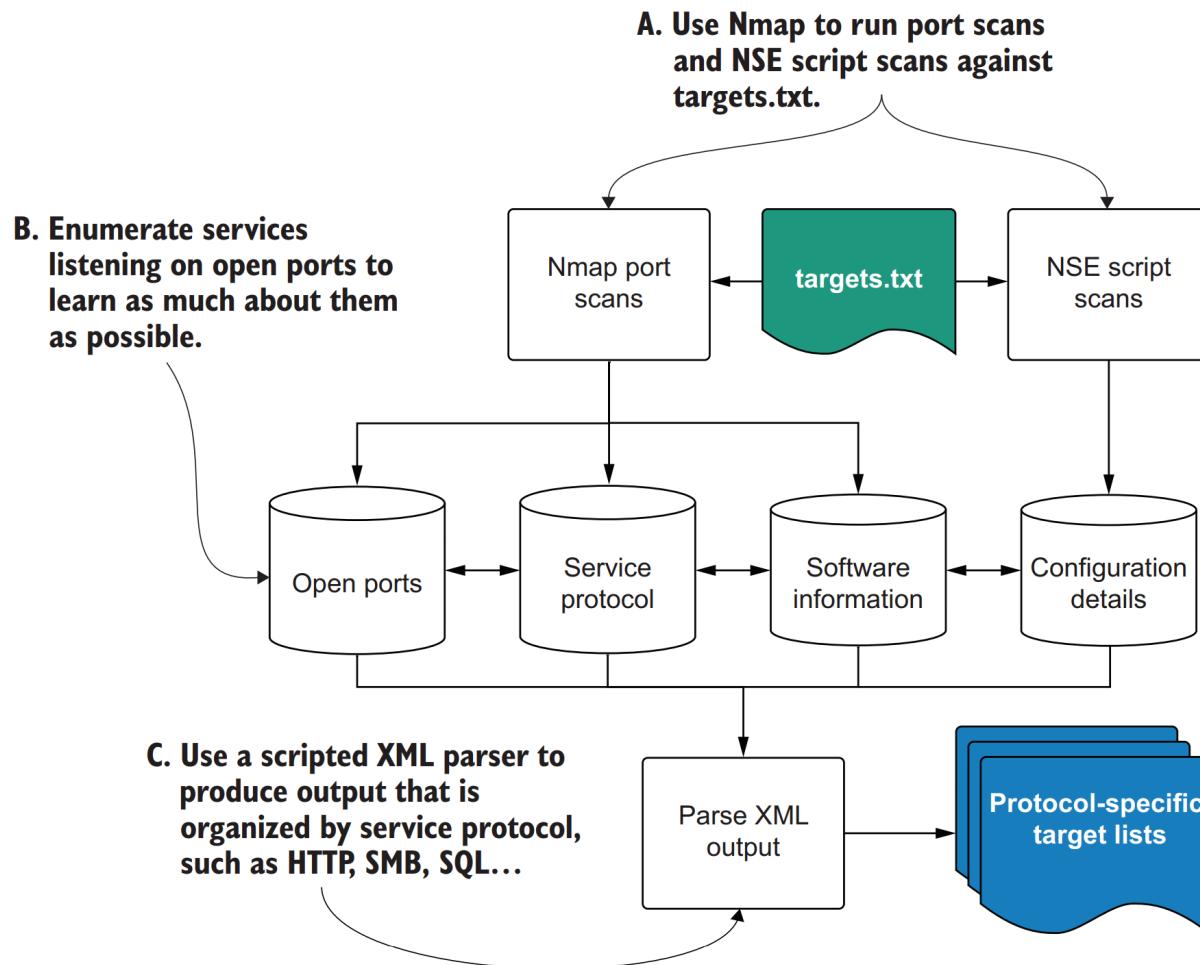
- 扫描靶机的开放端口
 - nmap -p- 靶机的IP地址
- 扫描靶机开放端口的服务版本信息
 - nmap -p开放端口号（以逗号分隔） -sV 靶机的IP地址

网络服务

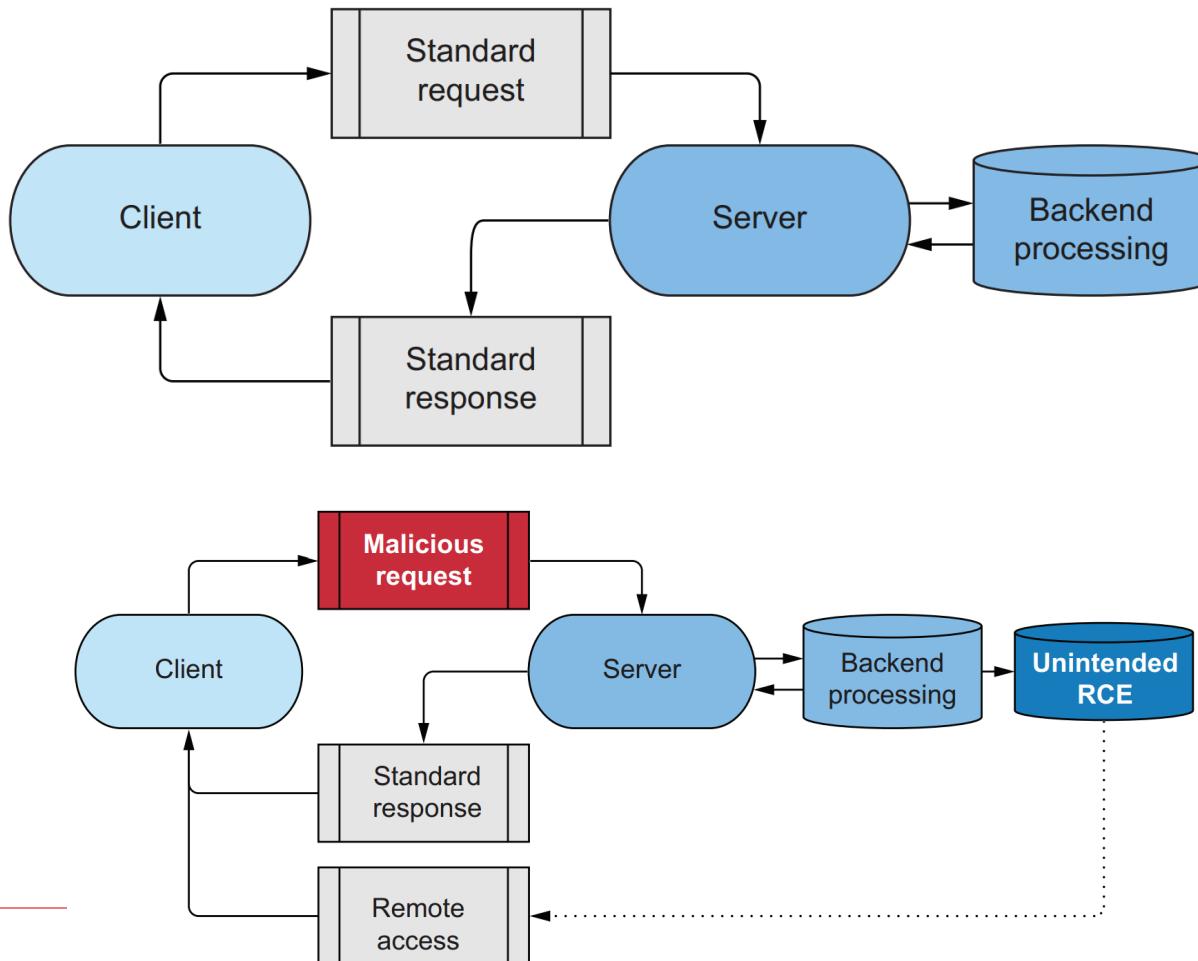
A **network service** can be defined as any application or software that is listening for requests on a network port from 0 to 65535

The **protocol** of a particular service dictates the proper format of a given request as well as what can be contained in the response

服务发现



网络服务的请求和响应



Network service banner

```
# curl --head 靶机IP地址
```

```
HTTP/1.1 200 OK
```

This service is using the
HTTP protocol

```
Date: Wed, 14 Sep 2025 14:59:27 GMT
```

```
Server: Apache/2.0.52 (CentOS)
```

```
X-Powered-By: PHP/4.3.9
```

```
Content-Type: text/html; charset=UTF-8
```

It's using PHP. This means
the server is likely talking to
a backend database server.

This is a Apache web server,
Version 2.0.52

快速端口扫描

```
# nmap -Pn -n -p  
22,25,53,80,443,445,1433,3306,3389,5800,5900,8080,844  
3 -iL targets.txt -oA quick-sweep
```

```
Nmap scan report for 10.0.2.5  
Host is up (0.0018s latency).  
  
PORT      STATE    SERVICE  
22/tcp    open     ssh  
25/tcp    closed   smtp  
53/tcp    closed   domain  
80/tcp    open     http  
443/tcp   open     https  
445/tcp   closed   microsoft-ds  
1433/tcp  closed   ms-sql-s  
3306/tcp  closed   mysql  
3389/tcp  closed   ms-wbt-server  
5800/tcp  closed   vnc-http  
5900/tcp  closed   vnc  
8080/tcp  closed   http-proxy  
8443/tcp  closed   https-alt  
MAC Address: 08:00:27:D6:03:FD (Oracle VirtualBox virtual NIC)
```

端口扫描

Port	Type
22	Secure Shell (SSH)
25	Simple Mail Transfer Protocol (SMTP)
53	Domain name service (DNS)
80	Unencrypted web server (HTTP)
443	SSL/TLS encrypted web server (HTTPS)
445	Microsoft CIFS/SMB
1433	Microsoft SQL server
3306	MySQL server
3389	Microsoft remote desktop
5800	Java VNC server
5900	VNC server
8080	Misc. web server port
8443	Misc. web server port

完整端口扫描

- `nmap -Pn -n -iL targets.txt -p 0-65535 -sV -A -oA full-sweep --min-rate 50000 --min-hostgroup 100`
 - `-sV`: Probe open ports to determine service/version info
 - `-A`: Enable OS detection, version detection, script scanning, and traceroute

靶机demo 1的渗透测试

- 可能会用到的渗透测试工具和命令
 - 本地搜索漏洞信息: searchsploit
 - 开源渗透测试框架: Metasploit framework
 - service postgresql start
 - msfdb init
 - msfconsole

作业2提交方法和截止期限

- 尝试通过攻击机Kali Linux对靶机demo 1进行渗透测试，并获得root权限
- 实验报告的文件名命名统一为：学号_lab02.pdf
- 提交截止期限：2025年10月14日零点
- 实验报告通过电子邮件发送给chenj@nju.edu.cn