计算机网络攻防实验课

第8周

陈健

chenj@nju.edu.cn

被动信息收集网站补充

- censys
  - search.censys.io
- fofa
  - fofa.so
- netcraft
  - sitereport.netcraft.com

UDP服务扫描

> db_nmap –Pn –sU –sV –sC –n –v --reason --open target_IP

发现用户

- SNMP探测
  - db_nmap -p 161 -sU -sV –Pn target_IP
- SNMP枚举
  - use auxiliary/scanner/snmp/snmp_enumusers
  - show options
  - set RHOSTS target_IP
  - run

暴力破解用户密码

- FTP用户密码破解
  - Hydra
  - MSF的ftp_login模块
- SSH用户密码破解
  - MSF的ssh_login模块

漏洞评估与利用

- TCP端口9200
  - 软件及其版本
  - 是否有漏洞
  - 如何利用

后渗透阶段

- 查询监听端口
  - netstat -naob
- 查询用户信息
  - net user
  - net localgroup Administrators
- 查询安装程序目录
  - 查找用户名和密码信息
    - C:\glassfish

后渗透阶段

- 如何访问被防火墙阻挡的服务
  - RDP服务
- 如何利用被防火墙阻挡的服务漏洞
  - SMB服务