漏洞扫描

主机扫描

sudo nmap -T4 -sS -sV -A -Pn -O IP

sudo nmap -T5 -O -A -v -sC vuln IP　　利用脚本进行简单漏洞扫描

MS08067　: --script=smb-vuln-ms08-067

MS-17-010：--script=smb-vuln-ms17-010

主机服务扫描

1.Web **服务：**

nmap -sS -PS80 -p 80 –oG web.txt

use auxiliary/sanner/http/webdav_scanner(Webdav 服务器)

2.SSH **服务：**

use auxiliary/sanner/ssh/ssh_version

猜解：use auxiliary/sanner/ssh/ssh_login

3.Telnet **服务**

use auxiliary/sanner/telnet/telnet_version

4.FTP **服务**

use auxiliary/sanner/ftp/ftp_version

use auxiliary/sanner/ftp/anonymous　//探测是否允许匿名登录

5.SMB **服务：**

猜解：use auxiliary/smb/smb_login(易被记录)

use exploit/windows/smb psexec　#凭证攻击登录域控制器

use auxiliary/admin/smb/psexec_command #命令执行

6.Oracle **服务：**

nmap -sS -p 1521 IP

use auxiliary/sanner/oracle/tnslsnr_version

7.Mssql **服务：**

nmap -sS -p T:1433,U:1434 IP nmap –sU 192.168.33.130 -p1434

use auxiliary/sanner/mssql/mssql_ping

8.Mysql **服务**:

use auxiliary/sanner/mysq/mysql_version 发现 mysql 服务

use auxiliary/scanner/mysql/mysql

9.VNC **服务**

use auxiliary/sanner/vnc/vnc_none_auth //探测 VNC 空口令

10.SNMP **服务：**

use auxiliary/sanner/snmp/snmp_enum

猜解：use auxiliary/sanner/snmp_login

admsnmp IP –wordfile snmp.password [-outputfile <name>]

利用字符串获取系统信息：./snmpenum.pl IP 字符串 cisco.txt(linux.txt)

11.OpenX11 **空口令：**

use auxiliary/scanner/x11/open_x11

当扫描到此漏洞的主机后可以使用 xspy 工具来监视对方的键盘输入：

cd/pentest/sniffers/xspy/

xspy –display 192.168.1.125:0 –delay 100

路由设备

路由器探测：

nmap -p1-25,80,512-515,2001,4001,6001,9001 IP 段

nmap -sU -p69 -nvv IP 段　(大多数路由器支持 TFTP 服务)

nmap -O -F -n IP　#路由器系统扫描

破解 ssh 方式管理的路由 web: use auxiliary/scanner/ssh/ssh_login

路由登录口令破解： use auxiliary/scanner/http/http_login

Cisco **路由漏洞探测**

(1)cge.pl #查看漏洞类型(对应序号)

cge.pl　IP 漏洞序号　　#指定探测漏洞

(2)默认密码扫描： ciscos 目标 IP -t 4(超时时间) -C 10(线程)

(3)Cisco Auditing Tool

扫描默认密码，SNMP community 字符串和一些老的 IOS bug

cat -h IP -w list/community -a lists/passwords -i(查看是否有历史性 bug)

Web 扫描

nikto

nikto -h 目标 IP [-p port,port (port-port)] -F htm -o result.html

nikto.pl -h 10.100.100.10　扫描主机 10.100.100.10 的 80 口上的 WEB

nikto.pl -h 10.100.100.10 -p 443 -s -g　扫描主机 10.100.100.10 端口 443，强制使用 SSL 模式 -g

nikto.pl -h 10.100.100.10 -p 80-90　扫描主机 10.100.100.10 端口 80-90 ,Nikto 自动判定是 HTTP 还是 HTTPS

nikto.pl -h 10.100.100.10 -p 80,443,8000,8080　扫描主机 10.100.100.10 端口 80 443 8000 8080

nikto.pl -h 10.100.100.10 -p 80 -e 167　-e 167：使用 IDS 规避技术

golismero

golismero scan http://url -o report.html

Skipfish

一款 Web 应用安全侦查工具，Skipfish 会利用递归爬虫和基于字 典的探针生成一幅交互式网站地图，最终生成的地图会在通过安全检查后输出。

skipfish -m 5 -LY -S /usr/share/skipfish/dictionaries/complete.wl -o

skipfish2 -u URL

nmap

nmap -sS -sV --script=vulscan/vulscan.nse target

nmap -sS -sV --script=vulscan/vulscan.nse –script-args vulscandb=scipvuldb.csv target

nmap -sS -sV --script=vulscan/vulscan.nse –script-args vulscandb=scipvuldb.csv -p80 target

nmap -PN -sS -sV --script=vulscan –script-args vulscancorrelation=1 -p80 target

nmap -sV --script=vuln target

nmap -PN -sS -sV --script=all –script-args vulscancorrelation=1 target

扫描 WordPress：

wpscan –url http://IP/ –enumerate p 后台爆破 :类似工具 patator,dirbuster

dirb http://IP:PORT /usr/share/dirb/wordlists/common.txt

wpscan -u IP 使用 WPScan 攻击

WordPresswpscan -u IP -e u vp 列出用户名列表

wpscan -u IP -e u --wordlist /path/ wordlist.txt 暴力破解密码

网站目录扫描：

use /auxiliary/scanner/http/dir_scanner

搜索网站中的邮件地址：

use /auxiliary/gather/search_email_collector

检测 XSRF 和 XSS 的检测

ratproxy-v <outdir> -w <outfile> -d <domain> -lextifscgjm