Информзащита
Системный интегратор

Внешнее тестирование на проникновение

АО НИП «Информзащита»
Отдел анализа защищенности

Этапы

1. Разведка:
    - пассивная
    - активная
2. Эксплуатация

Разведка

Что она нам дает?

1. Domains/Subdomains
2. IP Address Scope
3. Emails
4. Staff Info
5. Files
6. Source Code
7. Credentials
8. Backend Technologies
9. DNS Records (MX, NS, SPF/DKIM/DMARC)
10. Open Ports/Services

Разведка

Tools

- **Domains/Subdomains** – bgp.he.net, riskiq, GDorks, crt.sh, whois, dnsdumpster.com, Sublist3r, dig ;)
- **Emails** – Hunter.io, theHarvester, Pastebin, HH, SimplyEmail, ismtp
- **IP Address Scope** – bgp.he.net, riskiq
- **Staff Info** – Social Networks, HH, theHarvester
- **Files** – GDorks, Pastebin, Target Site
- **Source Code** – Github, Pastebin, GDorks, Searchcode, Webarchive
- **Credentials** – Github, Pastebin, GDorks
- **Backend Technologies** – Wappalyzer, Webarchive, dnsdumpster.com
- **DNS Records (MX, NS, SPF/DKIM/DMARC)** – dig, nslookup
- **Open Ports/Services** – nmap, masscan, shodan, censys.io
- **Dirbust** – dirb, dirbuster, dirsearch, gobuster, turbo intruder

Сканирование

1. Сканирование портов
2. Определение сервисов
3. Поиск потенциальных уязвимостей

Сканирование

Tools

masscan -e eth0 -p1-65535,U:1-65535 **<target>** --rate=1000 – сканирование всех TCP- и UDP-портов со скорость 1000 пакетов в секунду

nmap –sS <target> – TCP SYN-сканирование, запускается по умолчанию без флагов

nmap –sU <target> – UDP-сканирование

nmap –sV –Pn -A <target> – пропускаем обнаружение хостов, сразу ищем информацию о сервисе/версии

nmap -sC -sV -Pn -p- --min-rate=400 --min-parallelism=512 -oA result -v –iL <target.txt>

*--min-rate – мин. кол-во пакетов в секунду

*--min-parallelism – распараллеливание запросов

Известные сетевые порты

- tcp/21 – FTP
- tcp/22 – SSH
- tcp/23 – Telnet
- tcp/25 – SMTP
- tcp/53 – DNS
- tcp/80 – HTTP
- tcp/445 – SMB
- udp/53 – DNS
- tcp/3306 – MySQL
- tcp/5432 – postgresql
- tcp/1433 – mssql
- tcp/6379 - redis

Well-known ports [hide]

Port	TCP	UDP	IANA status[1]	Descr
0	Reserved	Reserved	Official	
	N/A	N/A	Unofficial	In programming APIs (not in communication between hosts), requests a system-allocated
1	Yes	Assigned	Official	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigne
5	Assigned	Assigned	Official	Remote Job Entry[7] was historically using socket 5 in its old socket form, while MIB PIM h
7	Yes	Yes	Official	Echo Protocol[9][10]
9	Yes, and SCTP[11]	Yes	Official	Discard Protocol[12]
	No	Yes	Unofficial	Wake-on-LAN[13]
11	Yes	Yes	Official	Active Users (systat service)[14][15]
13	Yes	Yes	Official	Daytime Protocol[16]
15	Yes	No	Unofficial	Previously netstat service[1][14]
17	Yes	Yes	Official	Quote of the Day (QOTD)[17]
18	Yes	Yes	Official	Message Send Protocol[18][19]
19	Yes	Yes	Official	Character Generator Protocol (CHARGEN)[20]
20	Yes, and SCTP[11]	Assigned	Official	File Transfer Protocol (FTP) data transfer[10]
21	Yes, and SCTP[11]	Assigned	Official	File Transfer Protocol (FTP) control (command)[10][11][21][22]
22	Yes, and SCTP[11]	Assigned	Official	Secure Shell (SSH),[10] secure logins, file transfers (scp, sftp) and port forwarding
23	Yes	Assigned	Official	Telnet protocol—unencrypted text communications[10][23]
25	Yes	Assigned	Official	Simple Mail Transfer Protocol (SMTP),[10][24] used for email routing between mail servers
37	Yes	Yes	Official	Time Protocol[25]
42	Assigned	Yes	Official	Host Name Server Protocol[26]
43	Yes	Assigned	Official	WHOIS protocol[27][28][29]
47	Reserved	Reserved	Official	
49	Yes	Yes	Official	TACACS Login Host protocol.[30] TACACS+, still in draft which is an improved but dinstinct
51	Reserved	Reserved	Official	Historically used for Interface Message Processor logical address management,[32] entry h

SMTP TEST

- **EXPN** – запрашивает список псевдонимов. Используется для групп рассылки
- **VRFY** – проверяет имя пользователя системы
- **RCPT TO** – определяет получателей сообщения

```
root@kali:~# ismtp -h 192.168.1.107:25 -e /root/Desktop/email.txt

-------------------------------------------------------------------
 iSMTP v1.6 - SMTP Server Tester, Alton Johnson (alton.jx@gmail.com)
-------------------------------------------------------------------

Testing SMTP server [user enumeration]: 192.168.1.107:25
Emails provided for testing: 7

Performing SMTP VRFY test...

Error: 2.0.0 root.

Performing SMTP RCPT TO test...

[+] root@mail.ignite.lab --- [ valid ]
[-] toor@mail.ignite.lab --- [ invalid ]
[-] admin@mail.ignite.lab -- [ invalid ]
[+] raj@mail.ignite.lab ---- [ valid ]
[+] sr@mail.ignite.lab ----- [ valid ]
[+] aarti@mail.ignite.lab -- [ valid ]
[+] raaz@mail.ignite.lab --- [ valid ]

Completed SMTP user enumeration test.
```

AXFR

dig AXFR example.com @127.0.0.1

example.com – зона, которую мы хотим выгрузить

@127.0.0.1 – отвечающий за зону Name Server (NS)

AXFR – запрос на трансфер зоны

Разведка

Frameworks

- Spiderfoot
- Recon-ng
- Sn1per

Эксплуатация

На что обратить внимание?

- Старые версии ПО
- Необычные порты
- Анонимный доступ

Эксплуатация

Tools

- metasploit
- exsploit-db.com
- searchsploit
- https://sploitus.com/