

## **Analiza wybranych narzędzi do skanowania systemów informatycznych**

Dariusz Chaładyniak\*, Andrzej Czarnecki†

Warszawska Wyższa Szkoła Informatyki

---

### **Abstrakt**

Skanowanie jest procesem zdalnego wykrywania hostów, serwerów, urządzeń sieciowych oraz realizowanych usług. Polega to na próbkowaniu aktywności analizowanego urządzenia sieciowego, poprzez wysyłanie do niego odpowiednio spreparowanych pakietów. W rezultacie otrzymane odpowiedzi mają dostarczyć informacji na temat aktywności badanego urządzenia lub usługi. Skanowanie jest operacją, która udziela informacji o zdarzeniach i urządzeniach w sieci. Pozwala stwierdzić czy dany komputer jest aktywny oraz rozpoznać uruchomione na nim usługi oraz system operacyjny.

**Słowa kluczowe** – skanowanie, protokoły sieciowe, adresy IP, porty TCP i UDP, usługi sieciowe

### **1. Wprowadzenie**

Skanowanie jest metodą aktywną. Administratorzy testowanej firmy mogą zarejestrować adres IP atakującego oraz jego działalność i poinformować odpowiednie służby. Dlatego bardzo ważne jest posiadanie pełnej zgody na przeprowadzenie skanowania.

Przed przystąpieniem do wykonywania testów należy zmienić User Agenta, aby nie zdradzać z jakiego systemu operacyjnego wykonuje się skanowanie. Podczas odwiedzania stron internetowych przeglądarka wysyła dane identyfikujące użytkownika, które zawierają na przykład nazwę systemu operacyjnego.

---

\* E-mail: dchalad@wwsi.edu.pl

† E-mail: a\_czarnecki@poczta.wwsi.edu.pl

System Kali Linux jest mało popularny, dlatego jeśli nie chcemy wyróżnić się w Internecie warto zmienić informacje wysyłane przez przeglądarkę na takie, które są wysyłane przez programy uruchomione w systemie Windows.

Podczas testów User Agent w Kali Linux został zmieniony na **User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)**.

Skanowanie najlepiej przeprowadzić kilkoma narzędziami, ponieważ wyniki mogą się różnić (skanery różnie klasyfikują podatności).

W trakcie skanowania należy zwrócić szczególną uwagę na usługi zdalnego dostępu na przykład: SSH (*ang. Secure shell*), Telnet, FTP (*ang. File Transfer Protocol*), PC AnyWhere i VNC (*ang. Virtual Network Computing*), ponieważ uzyskanie do nich dostępu bardzo często skutkuje przejściem pełnej kontroli nad atakowanym systemem.

## 2. Analiza wybranych narzędzi do skanowania systemów informatycznych

W procesie skanowania systemów informatycznych zostały przeanalizowane poniższe narzędzia programistyczne.

### 2.1. Ping, Fping oraz Hping3

Narzędzie Ping [1] służy do wysyłania pakietów ICMP (*ang. Internet Control Message Protocol*), dzięki którym można określić czy interfejs w urządzeniu sieciowym jest włączony. Dodatkowo dostajemy informację o czasie trwania podróży pakietu oraz poziomie strat w trakcie komunikacji, co pozwala na określenie niezawodności połączenia (patrz rysunek 1).

```
root@kali:~/etc/apache2/sites-available# ping wws1.edu.pl
PING wws1.edu.pl (148.81.195.146) 56(84) bytes of data.
64 bytes from 148.81.195.146: icmp_req=1 ttl=128 time=12.2 ms
64 bytes from 148.81.195.146: icmp_req=2 ttl=128 time=11.5 ms
64 bytes from 148.81.195.146: icmp_req=3 ttl=128 time=11.8 ms
64 bytes from 148.81.195.146: icmp_req=4 ttl=128 time=11.0 ms
64 bytes from 148.81.195.146: icmp_req=5 ttl=128 time=10.7 ms
64 bytes from 148.81.195.146: icmp_req=6 ttl=128 time=11.0 ms
64 bytes from 148.81.195.146: icmp_req=7 ttl=128 time=11.9 ms
^C
--- wws1.edu.pl ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 10.778/11.486/12.204/0.489 ms
```

Rysunek 1. Wynik skanowania narzędziem Ping

Dużo ciekawsze opcje oferuje skrypt Fping [2] umożliwiający testowanie wielu urządzeń sieciowych wykorzystując plik, w którym są zapisane adresy IP lub nazwy do sprawdzenia. Uzyskane informacje można zapisać do pliku. Narzędzie w prostym zapytaniu udziela krótkiej informacji czy urządzenie jest dostępne (patrz rysunek 2).

```
root@kali:~/Desktop# fping wp.pl
wp.pl is alive
root@kali:~/Desktop# █
```

**Rysunek 2.** Zapytanie wykonane za pomocą narzędzia Fping

```
root@kali:~/Desktop# fping -A -d -e -c 2 < servers.txt > wynikfping.txt
wp.pl (212.77.98.9) : xmt/rcv/%loss = 2/2/0%, min/avg/max = 10.6/11.1/11.6
wwsi.edu.pl (148.81.195.146) : xmt/rcv/%loss = 2/2/0%, min/avg/max = 10.9/11.0/11.2
onet.pl (213.180.141.140) : xmt/rcv/%loss = 2/2/0%, min/avg/max = 14.7/15.2/15.8
interia.pl (217.74.65.23) : xmt/rcv/%loss = 2/2/0%, min/avg/max = 15.4/15.6/15.8
tv.pl (217.149.249.61) : xmt/rcv/%loss = 2/2/0%, min/avg/max = 10.9/11.3/11.7
root@kali:~/Desktop# cat wynikfping.txt
wp.pl (212.77.98.9) : [0], 84 bytes, 10.6 ms (10.6 avg, 0% loss)
wwsi.edu.pl (148.81.195.146) : [0], 84 bytes, 10.9 ms (10.9 avg, 0% loss)
onet.pl (213.180.141.140) : [0], 84 bytes, 14.7 ms (14.7 avg, 0% loss)
interia.pl (217.74.65.23) : [0], 84 bytes, 15.4 ms (15.4 avg, 0% loss)
tv.pl (217.149.249.61) : [0], 84 bytes, 10.9 ms (10.9 avg, 0% loss)
wp.pl (212.77.98.9) : [1], 84 bytes, 11.6 ms (11.1 avg, 0% loss)
wwsi.edu.pl (148.81.195.146) : [1], 84 bytes, 11.2 ms (11.0 avg, 0% loss)
onet.pl (213.180.141.140) : [1], 84 bytes, 15.8 ms (15.2 avg, 0% loss)
interia.pl (217.74.65.23) : [1], 84 bytes, 15.8 ms (15.6 avg, 0% loss)
tv.pl (217.149.249.61) : [1], 84 bytes, 11.7 ms (11.3 avg, 0% loss)
```

**Rysunek 3.** Wyniki działania narzędzia Fping

Jest to bardzo dobra alternatywa do popularnego narzędzia Ping i oferująca dużo większy potencjał, poprzez podanie nazw i adresów IP z dokładnym czasem wędrowki pakietów oraz możliwością zapisania wyników do pliku (patrz rys. 3).

Narzędzie Hping3 [3] wykonuje wszystkie powyższe czynności i dodatkowo może wysyłać pakiety z wykorzystaniem protokołów warstwy czwartej TCP (patrz rysunek 4) lub UDP (patrz rysunek 5). Aplikacja umożliwia generowanie pakietów, zmieniając pola, flagi i typy protokołów TCP/IP.

```
root@kali:~/Desktop# hping3 -A -p 23 wp.pl -c 1
HPING wp.pl (eth1 212.77.98.9): A set, 40 headers + 0 data bytes
len=46 ip=212.77.98.9 ttl=128 id=60919 sport=23 flags=R seq=0 win=32767 rtt=0.4 ms

--- wp.pl hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.4 ms
root@kali:~/Desktop#
```

Rysunek 4. Wynik skanowania z użyciem protokołu TCP

```
root@kali:~/Desktop# hping3 --udp -p 53 wp.pl -c 1
HPING wp.pl (eth1 212.77.98.9): udp mode set, 28 headers + 0 data bytes

--- wp.pl hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~/Desktop#
```

Rysunek 5. Wynik skanowania protokołu UDP

Hping3 pozwala na tworzenie skryptów, które umożliwiają sprawdzenie systemu wykrywającego włamania. Dodatkowo oferuje on śledzenie pakietów na każdym skoku trasy, weryfikację co przepuszcza lub blokuje zaporę oraz określenie jednostki MTU (*ang. Maximum Transmission Unit*), czyli wielkości datagramu dopuszczalnego do danej sieci.

### 2.3. Nmap

Narzędzie Nmap [4] dużo lepiej radzi sobie ze skanowaniem niż wcześniej przedstawione narzędzia. Dostarcza poprawne wyniki, ponieważ posiada zdefiniowane wzorce pakietów, które są wysyłane w zależności od użytych opcji. Do każdego przypadku należy dobrać odpowiedni sposób skanowania.

Oprogramowanie Nmap może spowodować uszkodzenie działających systemów, dlatego powinno się go bardzo ostrożnie używać. Skanowanie należy przeprowadzić na wszystkich portach, aby uzyskać informację o otwartych i używanych usługach w skanowanym systemie, co jednak spowoduje wydłużenie czasu realizacji. Celem skanowania jest wykrycie wszystkich otwartych portów i ustalenie usług udostępnianych przez dany system z zamiarem wyszukania luk w zabezpieczeniach pod kontem podatności na atak, dzięki którym można uzyskać dostęp do komputera ofiary.

### **2.3.1. Skanowanie TCP SYN**

Podczas skanowania TCP SYN nie jest nawiązywane pełne połączenie. Do testowanego hosta wysyła się sygnał SYN i na podstawie otrzymanej odpowiedzi SYN-ACK jest określane czy port jest otwarty lub zamknięty. Ponieważ nie jest odsyłany sygnał ACK, a jedynie pakiet RST (zerowanie), który nakazuje skanowanemu komputerowi zignorowanie poprzednich pakietów i zamknięcie połączenia, dlatego jest to skanowanie półotwarte. W takim skanowaniu używa się flagi -sS (patrz rysunek 6).

```
root@kali:/# nmap -sS 192.168.1.3-5 -oA skanowanieSYN
Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 08:41 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse
Nmap scan report for 192.168.1.3
Host is up (0.00034s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:19:E4:40 (VMware)

Nmap scan report for 192.168.1.4
Host is up (0.00029s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
MAC Address: 00:0C:29:02:BC:D1 (VMware)

Nmap scan report for 192.168.1.5
Host is up (0.00025s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
MAC Address: 00:0C:29:22:CB:95 (VMware)

Nmap done: 3 IP addresses (3 hosts up) scanned in 4.35 seconds
```

**Rysunek 6.** Skanowanie TCP SYN

Jest stosunkowo bezpieczne i minimalizuje niebezpieczeństwo doprowadzenia do awarii skanowanego komputera lub uznania skanowania za atak typu DoS (*ang. Denial of Service*).

Podczas skanowania Nmap-em podaje się pojedynczy adres hosta lub zakres adresów IP. Flaga `-oA` umożliwia zapisanie wyników skanowania do pliku we wszystkich dostępnych formatach. Umożliwia to później łatwą pracę z danymi zapisanymi w pliku poprzez odfiltrowywanie interesujących nas informacji za pomocą narzędzia Grep.

### 2.3.2. Skanowanie UDP

Skanowanie portów UDP jest inne od skanowania portów TCP, ponieważ są to porty bezpołączeniowe. Nmap nie jest w stanie poprawnie ustalić czy port UDP jest zamknięty czy filtrowany przez zaporę. Otrzymana odpowiedź oznacza, że port nie jest otwarty ale może być również zablokowany.

```
root@kali:/# nmap -sU -sV 192.168.1.3-5 -oA skanowanieUDP
Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 08:44 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system
Stats: 5:40:09 elapsed; 0 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 97.85% done; ETC: 14:30 (0:05:33 remaining)
Nmap scan report for 192.168.1.3
Host is up (0.00046s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE      VERSION
123/udp   open       ntp           Microsoft NTP
137/udp   open       netbios-ns?
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
MAC Address: 00:0C:29:19:E4:40 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.4
Host is up (0.00057s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
111/udp   open       rpcbind      2 (RPC #100000)
137/udp   open       netbios-ns   Samba nmbd (workgroup: WORKGROUP)
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs          2-4 (RPC #100003)
5353/udp  open       mdns         DNS-based service discovery
MAC Address: 00:0C:29:02:BC:D1 (VMware)
Service Info: Host: UBUNTU

Nmap scan report for 192.168.1.5
Host is up (0.00080s latency).
Not shown: 998 open|filtered ports
PORT      STATE      SERVICE      VERSION
137/udp   open       netbios-ns   Microsoft Windows NT netbios-ssn (workgroup: WORKGROUP)
1434/udp  open       ms-sql-m?
```

Rysunek 7. Skanowanie UDP

Natomiast w przypadku braku odpowiedzi, nmap klasyfikuje port jako otwarty. Skanowanie jest dużo wolniejsze i mniej precyzyjne, jednak powinno być przeprowadzane, żeby wykryć usługi, które korzystają z tego protokołu. Do wykonania skanowania UDP należy użyć flagi `-sU` (patrz rysunek 7).

Nmap domyślnie skanuje tylko porty najczęściej używane. Za pomocą flagi `-p` można wybrać skanowanie wszystkich portów lub zawęzić skanowanie do konkretnego portu. Żeby nie pominąć żadnego otwartego portu dobrze jest na samym początku używać tej usługi. Dodatkowo opcja `-T` pozwala na zmianę szybkości skanowania od 0 do 5, a opcja `-0` umożliwi ustalenie systemu operacyjnego w skanowanym komputerze. Narzędzie Nmap posiada bardzo dużo możliwości, dlatego jest niezbędne w wyposażeniu profesjonalnego pentestera. Zdarzają się jednak sytuacje, że podczas skanowania niektóre usługi sieciowe ulegają awarii.

### 2.3.3. Skanowanie Xmas

Skanowanie Xmas ma na celu wyszukanie potencjalnych słabości i dziur oraz ustalenie listy otwartych portów.

```
root@kali:/# nmap -sX -p- -PN 192.168.1.3-5
Starting Nmap 6.40 ( http://nmap.org ) at 2016-09-07 07:42 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.00048s latency).
All 65535 scanned ports on 192.168.1.3 are closed
MAC Address: 00:0C:29:6F:39:18 (VMware)

Nmap scan report for 192.168.1.4
Host is up (0.00026s latency).
Not shown: 65525 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
2049/tcp  open|filtered nfs
33725/tcp open|filtered unknown
35968/tcp open|filtered unknown
40715/tcp open|filtered unknown
MAC Address: 00:0C:29:F8:B9:86 (VMware)

Nmap scan report for 192.168.1.5
Host is up (0.00036s latency).
All 65535 scanned ports on 192.168.1.5 are closed
MAC Address: 00:0C:29:AA:EA:CA (VMware)

Nmap done: 3 IP addresses (3 hosts up) scanned in 22.72 seconds
```

Rysunek 8. Skanowanie Xmas

Podczas skanowania wysyłane są pakiety z włączonymi flagami FIN, PSH i URG, a z wyłączonymi flagi SYN i ACK. Zamknięty port otrzymujący pakiet nieposiadający włączonych flag SYN, ACK lub RST powinien udzielić odpowiedzi w postaci pakietu wraz z włączoną flagą RST, natomiast włączony port otrzymujący pakiet bez ustawionej flagi SYN, ACK lub RST – powinien zignorować taki pakiet. W celu wykonania skanowania Xmas powinna być użyta flaga – sX (patrz rysunek 8).

### 2.3.4. Skanowanie Null

Skanowanie Null wykorzystuje pakiety bez ustawionych jakichkolwiek flag, czyli nagłówek TCP zawiera 0 (stąd nazwa skanowania). Ten typ skanowania jest niezgodny ze specyfikacją zawartą w dokumentach RFC (*ang. Request for Comments*). Umożliwia ominięcie tak samo jak w Xmas prostych filtrów i list kontroli dostępu ACL oraz jest również nieskuteczny w stosunku do systemu Windows. Skanowanie używa flagi -sN (patrz rysunek 9).

```
root@kali:/# nmap -sN -p- -PN 192.168.1.3-5
Starting Nmap 6.40 ( http://nmap.org ) at 2016-09-07 08:17 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.00028s latency).
All 65535 scanned ports on 192.168.1.3 are closed
MAC Address: 00:0C:29:6F:39:18 (VMware)

Nmap scan report for 192.168.1.4
Host is up (0.00028s latency).
Not shown: 65525 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
2049/tcp  open|filtered nfs
33725/tcp open|filtered unknown
35968/tcp open|filtered unknown
40715/tcp open|filtered unknown
MAC Address: 00:0C:29:F8:B9:86 (VMware)

Nmap scan report for 192.168.1.5
Host is up (0.00038s latency).
All 65535 scanned ports on 192.168.1.5 are closed
MAC Address: 00:0C:29:AA:EA:CA (VMware)

Nmap done: 3 IP addresses (3 hosts up) scanned in 21.80 seconds
```

Rysunek 9. Skanowanie Null

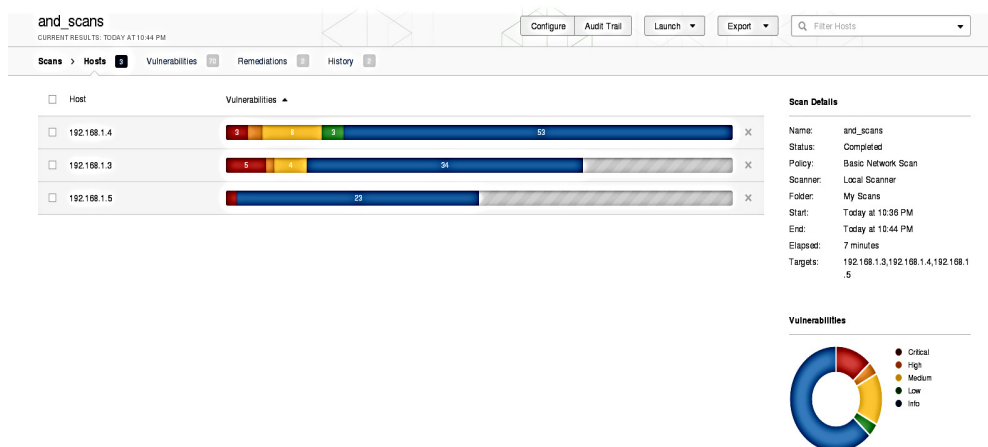


Uzyskany wynik jest taki sam jak w Xmas, chociaż nie są ustawiane żadne flagi. Główną zaletą tego typu skanowań jest to, że są one w stanie ominąć zapory bezstanowe i filtrowanie na routerach. Jednak nowe systemy IDS są konfigurowane do ich wykrywania. Ten rodzaj skanowania nie potrafi jednak odróżnić portów otwartych od filtrowanych.

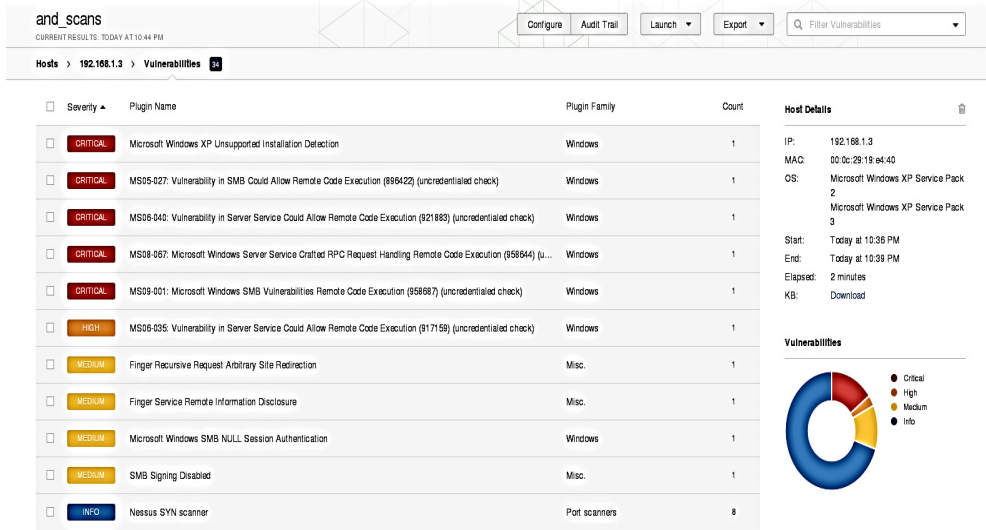
## 2.4. Nessus

Program Nessus [5] przeprowadza skanowanie systemu pod kątem jego podatności na atak poprzez wykrycie słabych punktów lub błędów w konfiguracji. Narzędzie posiada w swoich zasobach bardzo duże ilości danych o podatnościach i lukach w zabezpieczeniach systemów operacyjnych, co jest bardzo przydatne podczas przeprowadzania testów penetracyjnych. Bardzo efektywnie i szybko udziela informacji o testowanym środowisku wyświetlając, jakie oprogramowanie jest używane oraz jakich poprawek brakuje, co od razu wskazuje, na jakie podatności jest narażone. Działa na serwerze, a komunikacja z nim odbywa się za pomocą przeglądarki.

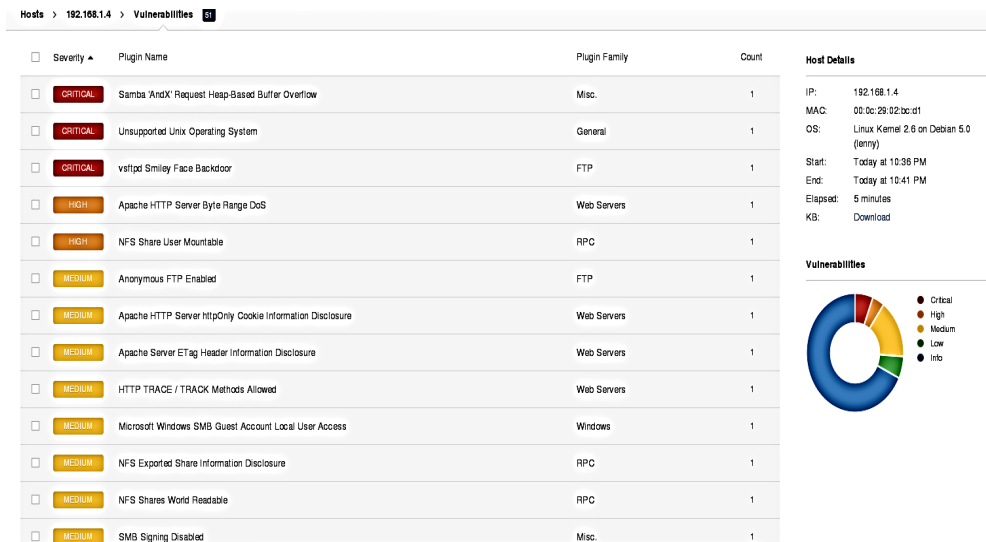
Po zainstalowaniu aplikacji i uruchomieniu, należy w przeglądarce wpisać adres <https://kali:8834>, co pozwoli wejść do strony internetowej narzędzia. Podczas konfiguracji można utworzyć dwa rodzaje polityk w jednej zaznaczając opcję *SafeChecks*. W polu *Scan Targets* wpisuje się adresy IP do przeskanowania lub można wczytać plik z adresami. Informacje o znalezionych lukach w skanowanych systemach skaner wyświetla w raporcie. Podatności z oznaczeniami Critical oznaczają największą wrażliwość systemu na atak (patrz rysunek 10).



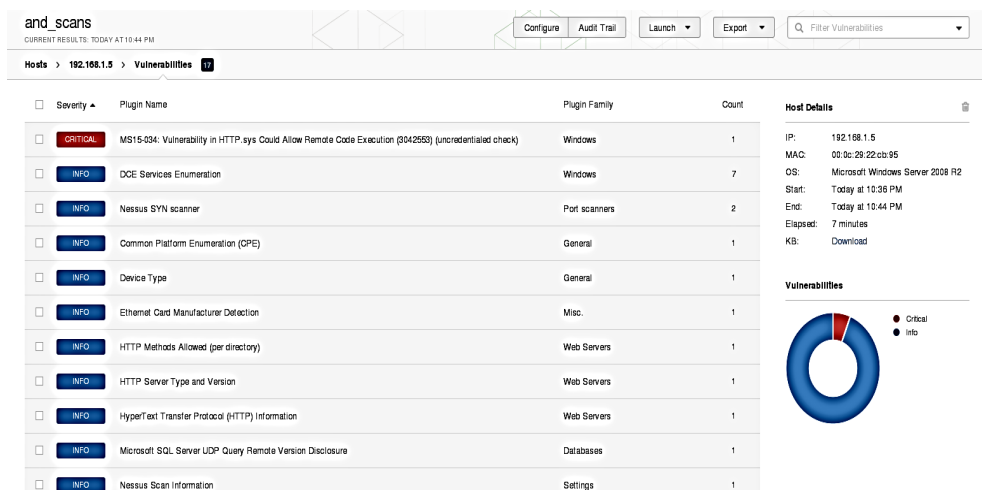
Rysunek 10. Wyniki działania skanera Nessus



Rysunek 11. Podatności w systemie MS Windows XP



Rysunek 12. Podatności w systemie Ubuntu



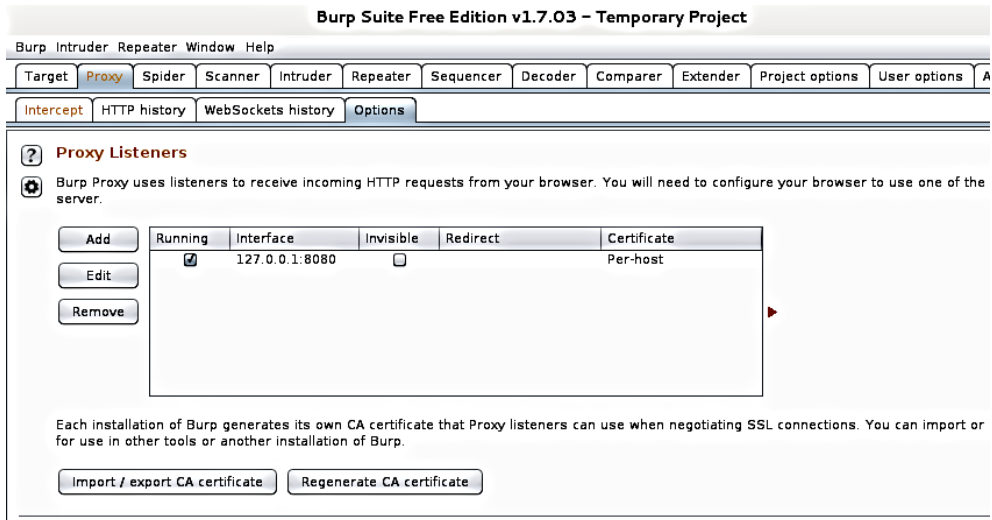
Rysunek 13. Podatności w systemie MS Windows 7

Testowane systemy zostały przeskanowane przez narzędzie Nessus, które wykryło bardzo dużo poważnych zagrożeń w systemie MS Windows XP (patrz rysunek 11), jak również w systemie Ubuntu (patrz rysunek 12).

Najmniej sklasyfikowano podatności w systemie operacyjnym MS Windows 7 (patrz rysunek 13). Wykryte luki przez system Nessus są ułożone według kryteriów CVSS (*ang. Common Vulnerability Scoring System*), opracowanych przez NIST (*ang. National Institute of Standards and Technology*), które określają, jaki wpływ na system mają wykryte dziury w zabezpieczeniach. Uzyskane wyniki są bardzo szczegółowe i dokładne, przedstawiając wszystkie możliwe podatności na testowanych systemach. Nessus przedstawia rezultaty skanowania w bardzo przejrzystej formie raportu z opisem każdej znalezionej luki.

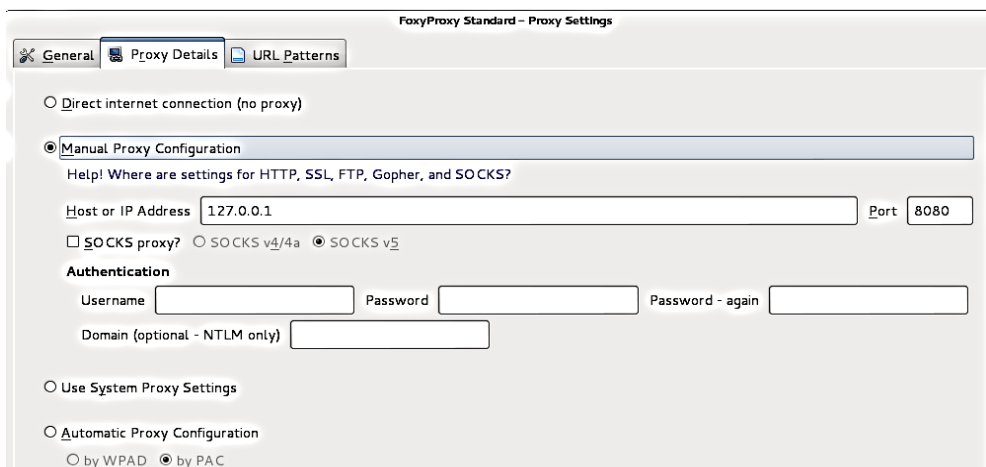
## 2.5. Burp Suite

Bardzo użytecznym narzędziem do analizy i skanowania aplikacji webowych jest Burp Suite [6]. Profesjonalne narzędzie jest płatne, natomiast do celów testowych została wykorzystana darmowa wersja z ograniczeniami. Narzędzie można pobrać ze strony <http://portswigger.net/burp/download.html> i uruchomić poleceniem `java -jar burpsuite_free_v1.7.03.jar`. Następnie należy ustawić proxy w zakładce *Proxy*, karta *Options* na port 8080 (patrz rysunek 14).



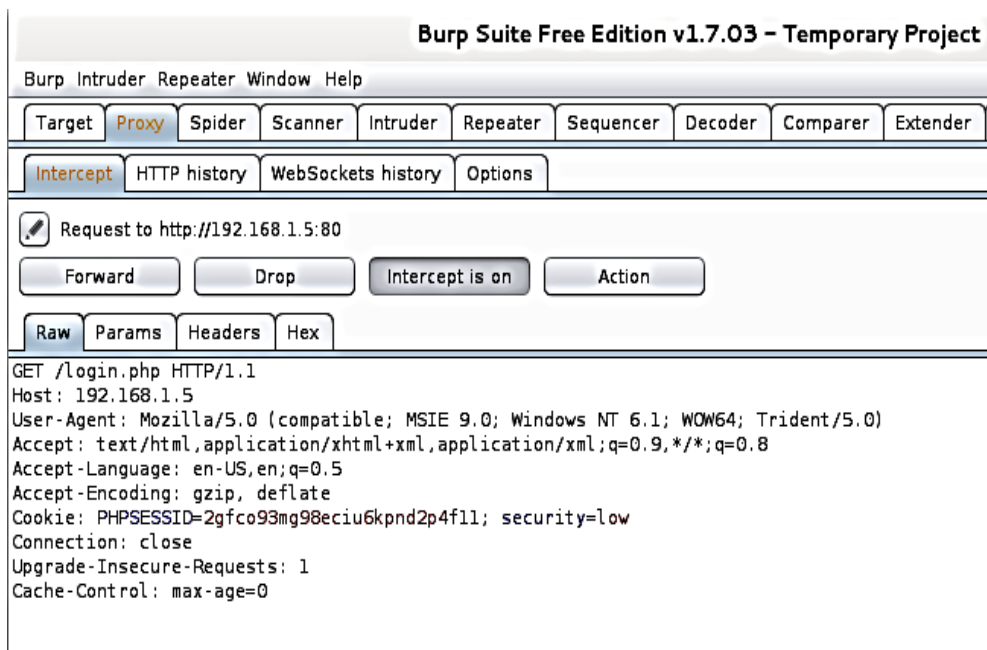
Rysunek 14. Ustawienie adresu serwera Proxy

Kolejny krok to instalacja rozszerzenia *FoxyProxy for Firefox*, które umożliwi automatyczne przełączanie połączenia internetowego pomiędzy serwerami proxy, zgodnie z regułami zdefiniowanymi przez użytkownika. W przeglądarce należy wybrać *Add New Proxy*, a następnie w karcie *Proxy Details* w części *Manual Proxy Configuration* wpisać w polu *Host or IP* adres 127.0.0.1, a tam gdzie jest port podać numer 8080 (patrz rysunek 15). Wszystkim ustawieniom lub zmianom nadać nazwę i zapisać.



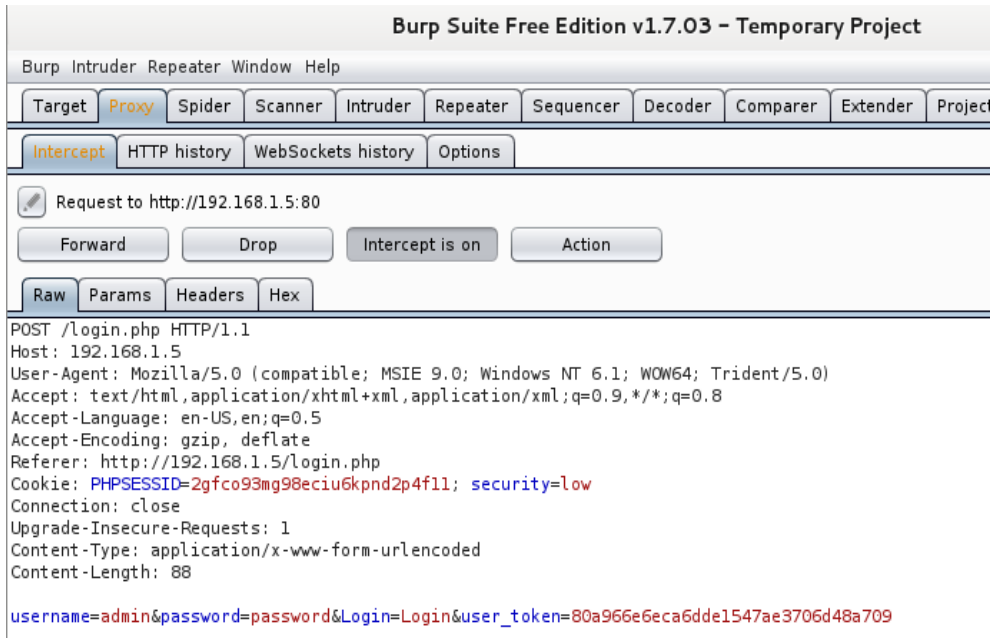
Rysunek 15. Ustawienia proxy w przeglądarce

Przeglądarka będzie przekazywała cały ruch na port 8080 do narzędzia Burp Suite, które dalej przekieruje do właściwego celu. Kiedy wszystko jest już poprawnie ustawione i przeglądarka używa Proxy można analizować witrynę testowanej aplikacji internetowej. W przeglądarce wpisujemy adres testowanej witryny, następnie przechodzimy do Burp Suite i otwieramy zakładkę *Proxy*, a w niej kartę *Intercept* (patrz rysunek 16).



Rysunek 16. Dane przechwycone przez Burp Suite

Informacje przechwycone przez narzędzie Burp Suite pomiędzy przeglądarką z Kali Linux a serwerem obsługującym stronę internetową można odczytać, zmienić, przesłać dalej lub odrzucić. Można ponadto podejrzeć opcje logowania i odczytać login oraz hasło, jeżeli jest przesyłane niezaszyfrowaną komunikacją (patrz rysunek 17).



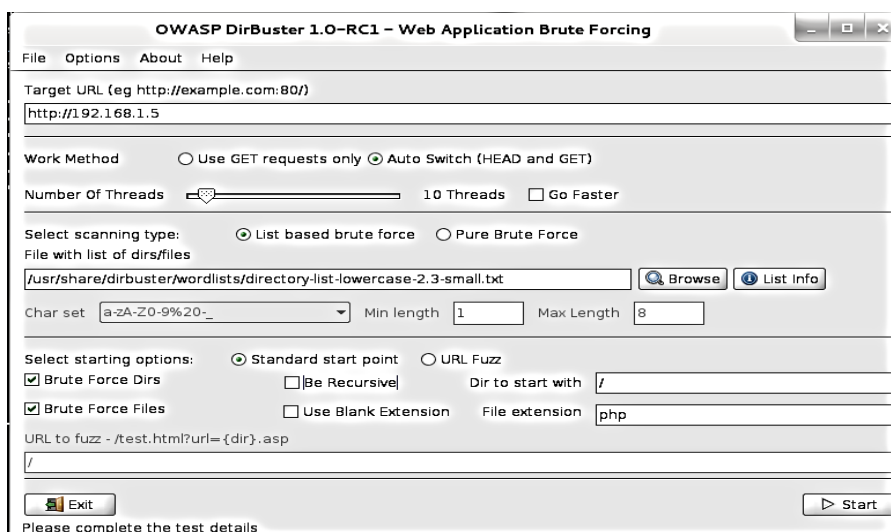
Rysunek 17. Uzyskane dane do logowania

## 2.6. DirBuster

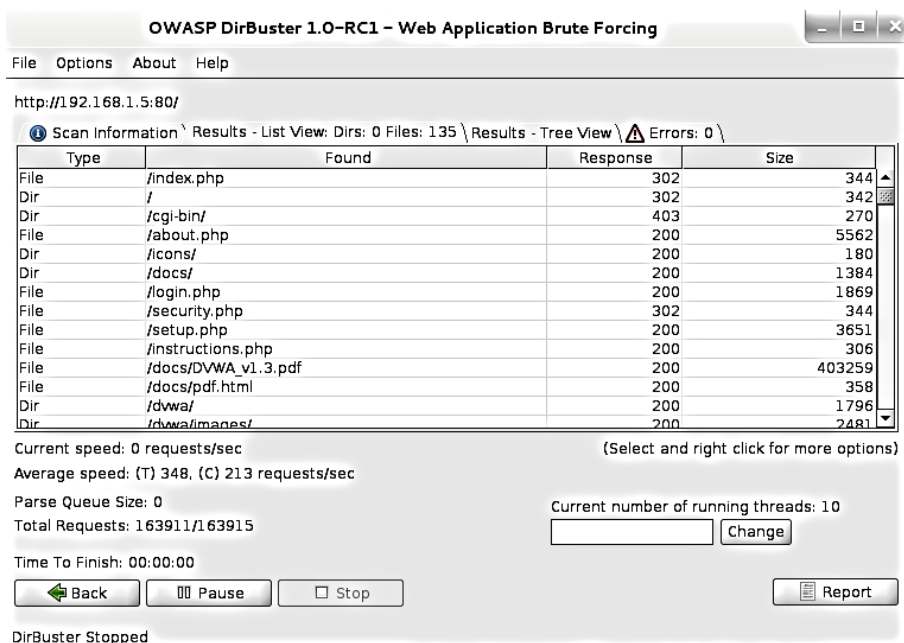
Aplikacja DirBuster [7] służy do poszukiwania plików lub katalogów w webaplikacjach. Wykorzystując własny słownik zapytań DirBuster sprawdza, jaki jest kod HTTP odpowiedzi z serwera. Dzięki nim można ustalić czy dany plik lub katalog istnieje, czy jest przekierowanie do innej strony. Po wpisaniu adresu URL, należy wybrać metodę, typ skanowania i zaznaczyć jakie zasoby mają być przeszukane (patrz rysunek 18).

Opis ustawień:

- adres strony na serwerze (http://192.168.1.5);
- ustawić opcje Auto Switch;
- wybrać czy metoda brute force (Pure Brute Force) i określić zakres znaków czy metoda słownikowa (List based brute force) i wybrać słownik;
- zaznaczyć, że szukane są pliki i foldery (Brute Force Dirs i Files).



Rysunek 18. Ustawienia OWASP DirBuster



Rysunek 19. Wyniki skanowania DirBuster

Po uruchomieniu można podejrzeć w *Results-List View* wyniki znalezionych plików i folderów, ich wielkość oraz sprawdzić je poprzez uruchomienie w przeglądarce (patrz rysunek 19). Program umożliwi znalezienie plików zostawionych przez programistę lub administratora, w których mogą się znajdować ważne dane. Można ustalić wersje oprogramowania, co może pomóc w znalezieniu podatności i dopasować exploit. Na koniec można wygenerować dokładny raport. Wszystkie powyższe czynności można wykonać również narzędziem Burp Suite.

## 2.7. Fimap

Fimap [8] jest to skaner wyszukujący podatności typu LFI (*ang. Local File Include*) i RFI (*ang. Remote File Include*). LFI jest to błąd w skrypcie PHP (*ang. PHP Hypertext Preprocessor*), dzięki któremu można odczytać dowolny plik na serwerze znając do niego ścieżkę (na przykład plik zawierający loginy użytkowników, informacje o katalogach). Dużo bardziej niebezpieczny błąd RFI może zdalnie dołączyć pliki, uruchomić skrypt ze swojego serwera na atakowanej stronie i uruchomić *shella php*.

```
http://hiderefer.com/?http://www.dvwa.co.uk/DVWA
http://192.168.1.5/hackable/users/?C=S;O=D
http://192.168.1.5/vulnerabilities/view_help.php?id=sqli_blind&security=low
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://192.168.1.5/icons/small/sound.gif
http://www.inkscape.org/namespace/inkscape
http://192.168.1.5/security.php
http://hiderefer.com/?https://blog.g0tmilk.com/
http://192.168.1.5/hackable/users/?C=S;O=A
http://192.168.1.5/vulnerabilities/fi/?page=file2.php
http://hiderefer.com/?http://www.dvwa.co.uk/
http://192.168.1.5/icons/folder.png
http://192.168.1.5/icons/small/compressed.gif
http://192.168.1.5/vulnerabilities/view_source.php?id=upload&security=low
http://hiderefer.com/?https://secure.php.net/manual/en/function.htmlspecialchars.php
http://192.168.1.5/fds_log.php
http://192.168.1.5/dvwa/?C=N;O=D
http://192.168.1.5/icons/ball.red.png
http://192.168.1.5/vulnerabilities/view_help.php?id=xss_r&security=low
http://192.168.1.5/dvwa/?C=N;O=A
http://192.168.1.5/icons/small/forward.gif
http://192.168.1.5/icons/uuencoded.gif
http://192.168.1.5/index.php
http://192.168.1.5/icons/screw2.png
http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html
http://192.168.1.5/icons/small/broken.png
http://192.168.1.5/vulnerabilities/view_source.php?id=xss_s&security=low
http://192.168.1.5/dvwa/js/?C=S;O=A
http://192.168.1.5/icons/small/generic3.png
http://tedi.heriyanto.net/
http://www.google.com/recaptcha/api/challenge?k=
http://192.168.1.5/icons/small/generic2.gif
http://192.168.1.5/icons/text.gif
http://192.168.1.5/icons/image3.gif
http://hiderefer.com/?http://www.ss64.com/bash/
http://192.168.1.5/icons/odf6odf.png
```

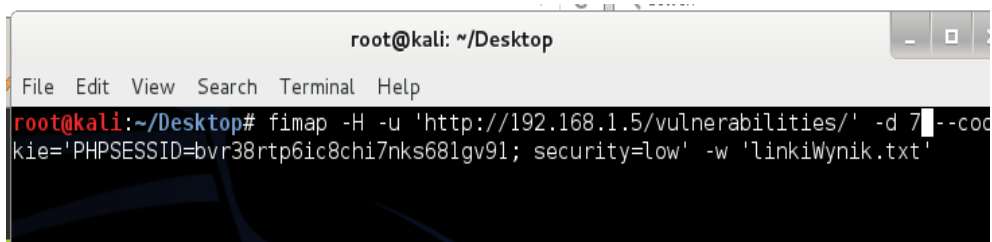
Rysunek 20. Zebrane linki z serwera za pomocą narzędzia Burp Suite



Skaner Fimap umożliwia skanowanie adresów URL przy wykorzystaniu wyszukiwarki Google. Znalezione podatności, po ustawieniu odpowiedniego parametru, mogą zostać automatycznie wykorzystane.

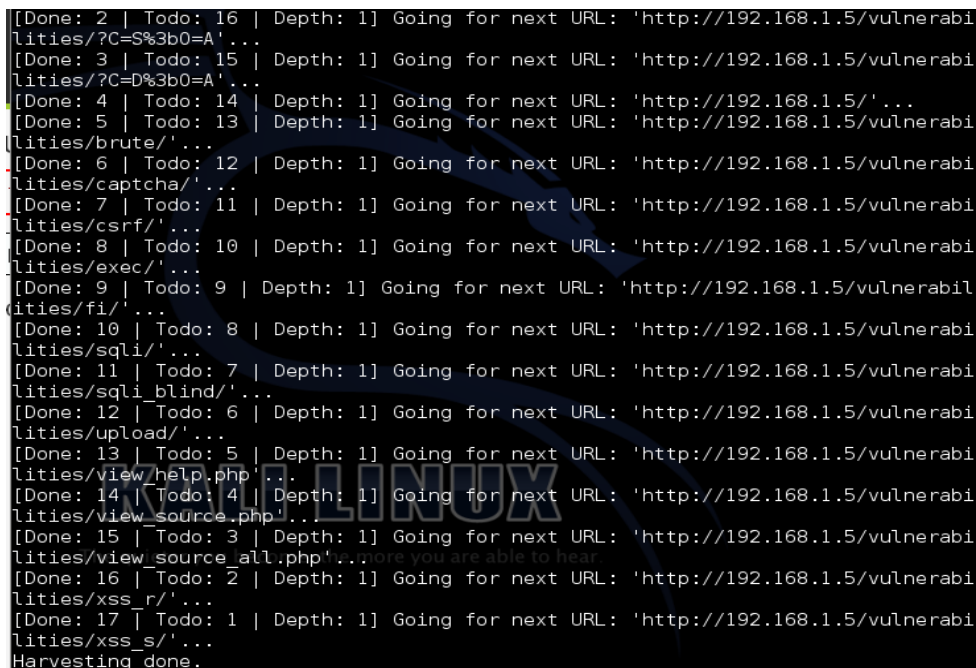
Wykorzystując funkcję *spider* w programie Burp Suite wyszukane zostały wszystkie adresy URL i linki znajdujące się na badanej stronie internetowej serwera i zapisane do pliku (patrz rysunek 20).

Fimap umożliwia również zebranie linków (patrz rysunek 21).



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# fimap -H -u 'http://192.168.1.5/vulnerabilities/' -d 7 --cookie='PHPSESSID=bvr38rtp6ic8chi7nks681gv91; security=low' -w 'linkiWynik.txt'
```

Rysunek 21. Polecenie wyszukiwania linków



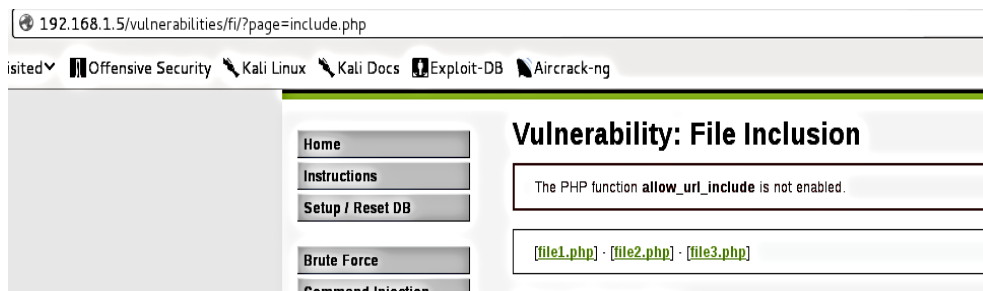
```
[Done: 2 | Todo: 16 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/?C=S%3b0=A'...
[Done: 3 | Todo: 15 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/?C=D%3b0=A'...
[Done: 4 | Todo: 14 | Depth: 1] Going for next URL: 'http://192.168.1.5/'...
[Done: 5 | Todo: 13 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/brute/'...
[Done: 6 | Todo: 12 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/captcha/'...
[Done: 7 | Todo: 11 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/csrf/'...
[Done: 8 | Todo: 10 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/exec/'...
[Done: 9 | Todo: 9 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/fi/'...
[Done: 10 | Todo: 8 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/sql/'...
[Done: 11 | Todo: 7 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/sql_bland/'...
[Done: 12 | Todo: 6 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/upload/'...
[Done: 13 | Todo: 5 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/view_help.php'...
[Done: 14 | Todo: 4 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/view_source.php'...
[Done: 15 | Todo: 3 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/view_source_all.php'... more you are able to hear
[Done: 16 | Todo: 2 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/xss_r/'...
[Done: 17 | Todo: 1 | Depth: 1] Going for next URL: 'http://192.168.1.5/vulnerabilities/xss_s/'...
Harvesting done.
```

Rysunek 22. Zebrane linki za pomocą narzędzia Fimap

```
[09:47:58] [INFO] Testing file 'c:\boot.ini'...
[09:47:58] [INFO] Testing file 'php://input'...
[09:47:58] [INFO] Testing file 'http://www.phpbb.de/index.php'...
#####
#[1] Possible PHP-File Inclusion #
#####
#::REQUEST #
# [URL] http://192.168.1.5/vulnerabilities/fi/?page=include.php #
# [HEAD SENT] Cookie #
#::VULN INFO #
# [GET_PARAM] page #
# [PATH] C:\xampp\htdocs\vulnerabilities\fi #
# [OS] Windows #
# [TYPE] Absolute Clean #
# [TRUNCATION] No Need. It's clean. #
# [READABLE FILES] #
# No Readable files found :( #
#####
[412][MASS_SCAN] Scanning: 'http://192.168.1.5/icons/folder.sec.gif'...
[09:47:58][OUT] Inspecting URL 'http://192.168.1.5/icons/folder.sec.gif'...
[09:47:58] [INFO] Fiddling around with URL...
[413][MASS_SCAN] Scanning: 'http://www.designnewcastle.co.uk/'...
[09:47:58][OUT] Inspecting URL 'http://www.designnewcastle.co.uk/'...
[09:47:58] [INFO] Fiddling around with URL...
```

Rysunek 23. Wyniki skanowania narzędziem Fimap

Fimap bardzo precyzyjnie ustalił podatny link do strony (patrz rysunek 23), który po wklejeniu w przeglądarce, potwierdził wrażliwość aplikacji na tego typu atak (patrz rysunek 24), co uwierzytelnia jego skuteczne wykrywanie luk.



Rysunek 24. Wykryta podatność

Fimap bardzo sprawnie poradził sobie z wykryciem wielu podatności w aplikacji webowej.

## 2.8. Nikto

Nikto [9] jest to skaner wykonujący kompleksowe testy w celu wyszukania luk w zabezpieczeniach serwera WWW. Sprawdzając konfigurację testowanego systemu narzędzie to nie tylko wykryje zagrożenia, ale również wskaże zalecenia, które poprawią działanie serwera. Uruchamiając program należy podać adres URL lub adres IP skanowanego serwera oraz zakres portów (patrz rysunek 25).

```
root@kali:~/usr/share/set/src/html# nikto -h 192.168.1.5 -p 1-1000
- Nikto v2.1.5
-----
+ No web server found on 192.168.1.5:1
-----
+ No web server found on 192.168.1.5:2
-----
+ No web server found on 192.168.1.5:3
-----
```

Rysunek 25. Polecenie uruchamiające narzędzie Nikto

```
+ Target Hostname: 192.168.1.5
+ Target Port: 80
+ Start Time: 2016-09-08 09:52:17 (GMT-4)
-----
+ Server: Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.5.37
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.37
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: login.php
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x1
a 0x52156c6a290c0
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302
)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appro
p
riate line in httpd.conf or restrict access to allowed hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Uncommon header 'x-webkit-csp' found, with contents: default-src 'self' ;scrip
t-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self'
'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'content-security-policy' found, with contents: default-src 's
elf' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;;style-src 'self' 'unsafe
-inline' ;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;
+ Uncommon header 'x-content-security-policy' found, with contents: default-src
'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' da
```

Rysunek 26. Wynik uzyskany ze skanowania serwera WWW

Narzędzie wykonało testy serwera WWW uruchomionego na maszynie z systemem MS Windows 7 skanując porty od 1 do 1000. Podczas skanowania zostało wykrytych dużo podatności oznaczonych w OSVDB (*ang. Open Source Vulnerability Database*), które można wykorzystać do przeprowadzenia ataku (patrz rysunek 26). OSVDB jest to internetowa baza danych zawierająca informacje o błędach w oprogramowaniu i lukach zbieranych z raportów bezpieczeństwa.

### 3. Podsumowanie

Skanowanie systemów jest bardzo ważnym przedsięwzięciem a uzyskane wyniki znacząco pomagają w dalszym działaniu w ramach wyszukiwania podatności i luk w testowanych sieciach. Dzięki skanowaniu uzyskujemy informacje takie jak: identyfikacja serwerów, lista otwartych portów, wykaz działających usług, listy kontroli dostępu ACL (*ang. Access Control List*). Aby przeprowadzić skanowanie wymagane jest posiadanie zgody na przeprowadzenie badania, dlatego wszystkie testy zostały wykonane w specjalnie przygotowanym laboratorium. W trakcie tego etapu można uzyskać szczegółowe dane o stosowanych zabezpieczeniach, rodzajach używanego oprogramowania wraz z ich numerem wersji oraz sprawdzić czy strony internetowe są podatne na ataki, co posłuży do dobrania odpowiednich złośliwych skryptów. Skanowanie może pomóc również w rozpoznaniu topologii sieci i konfiguracji urządzeń dostępowych (np.: list kontroli dostępu, tablic routowania). Jest ono wykorzystywane przez administratorów do rozwiązywania problemów z siecią, jak również przez intruzów w celach rozpoznawczych.

### Bibliografia

- [1] <https://hostovita.pl/blog/jak-sprawdzic-ping-traceroute/>
- [2] <https://fping.org/>
- [3] <https://www.hacking.pl/hping3/>
- [4] <https://nmap.org/>
- [5] <https://lifelhacker.com/how-to-use-nessus-to-scan-a-network-for-vulnerabilities-1788261156>
- [6] <https://portswigger.net/burp>
- [7] <https://tools.kali.org/web-applications/dirbuster>
- [8] <https://tools.kali.org/web-applications/fimap>
- [9] <https://cirt.net/nikto2-docs/>

## **Analysis of selected tools for scanning it systems**

### **Abstract**

Scanning is the process of remotely detecting hosts, servers, network devices, and services. This involves sampling the activity of the network device being analyzed by sending packaged packets to it. As a result, the answers received provide information about the activity of the device or service being tested. Scanning is an operation that provides information about events and devices on the network. Allows you to determine if your computer is active and recognize the services and operating system that are running on it.

**Keywords** – scanning, network protocols, IP addresses, TCP and UDP ports, network services