

Politechnika Wrocławska, Informatyka Stosowana

OSINT

Cyberbezpieczeństwo, Laboratorium nr.10 - raport

Autor: Aleksander Stepaniuk
Nr. Indeksu: 272644

4. Pytania

Pytanie 1;

Tworzenie odcisków palców systemu operacyjnego polega na analizie charakterystycznych cech, takich jak odpowiedzi na pakiety TCP/IP, ustawienia TTL, znaczniki czasu, czy otwarte porty. Mogą one być tworzone przez użycie programów do skanowania systemu i zbierania informacji o wersji oprogramowania, zainstalowanych programach, analizie ruchu sieciowego oraz witryn internetowych otwieranych w systemie.

Pytanie 2;

Dzięki odciskom palców atakujący mogą dostosować swoje działania do konkretnego systemu, wykorzystując znane dla niego podatności, a także identyfikować użytkowników i urządzenia których używają. Z perspektywy ochrony, administratorzy mogą analizować takie informacje systemu i odpowiednio chronić przed różnego rodzaju atakami np. typu man in the middle.

Pytanie 3;

Aktywne techniki polegają na wysyłaniu zapytań do systemu i analizie odpowiedzi. Mogą wymagać one dodatkowej aktywności użytkownika poprzez zezwolenie na gromadzenie danych. Pasywne techniki, analizują ruch sieciowy bez ingerowania w komunikację oraz bez udziału użytkownika, co utrudnia ich wykrycie.

Pytanie 4;

Tak, można ograniczyć ujawniane informacje poprzez konfigurację firewalli, zmiany domyślnych ustawień protokołów, korzystanie z VPNa i korzystanie z przeglądarek chroniących prywatność.

Pytanie 5;

Tak, można użyć VPNa, który ukrywa niektóre dane użytkownika (między innymi jego lokalizację), albo odpowiednio skonfigurować firewalla, aby blokował lub zmieniał odpowiedzi na skanowania. Można też użyć honeypotów, które udają systemy lub serwery.

Pytanie 6;

Transfer stref DNS (AXFR) umożliwia pobranie pełnej zawartości strefy DNS. Atakujący mogą uzyskać listę subdomen i adresów IP, co ułatwia planowanie ataków. Ryzyko można ograniczyć, konfigurując serwery DNS tak, aby autoryzowały transfer tylko z zaufanych adresów.

Pytanie 7;

OSINT jest legalny, jeśli korzysta się z publicznie dostępnych informacji. Naruszenie prywatności lub zabezpieczeń może jednak prowadzić do łamania prawa. Należy więc zachowywać szczególną ostrożność w przypadku informacji, warto dowiadywać się czy nie są one poufne lub chronione jakiegoś rodzaju licencją.

Pytanie 8;

Największe zagrożenie to ujawnianie poufnych informacji w publicznie dostępnych źródłach, które mogą zostać wykorzystane przez atakujących do phishingu, inżynierii społecznej czy planowania ataków.

Pytanie 9;

Najlepiej ograniczyć ilość publicznie dostępnych danych, stosować polityki prywatności, przeszukiwać swoje informacje jak atakujący (audit OSINT), a także regularnie usuwać niepotrzebne treści i aktualizować zabezpieczenia.

5. Zadania

Zadania 1-3ab;

Wybrana przeze mnie domena to: wykop.pl

```
(stud@kali-vm)-[~]  
$ whois wykop.pl  
  
DOMAIN NAME:          wykop.pl  
registrant type:      organization  
nameservers:          cosmin.ns.cloudflare.com.  
                      elly.ns.cloudflare.com.  
created:              2005.12.28 10:55:36  
last modified:        2024.11.30 00:02:49  
renewal date:         2025.12.28 10:55:36  
  
option created:       2021.12.28 05:45:50  
option expiration date: 2024.12.28 05:45:50  
  
dnssec:               Unsigned  
  
REGISTRAR:  
Aftermarket.pl Limited  
Chytron, 3, Office 301, P.C.  
1075 Nicosia  
Cypr/Cyprus  
Tel: +357.22761649  
Fax: +357.22767543  
http://www.AfterMarket.pl/contact.php  
domains@dropped.pl
```

```
(stud@kali-vm)-[~]  
$ host wykop.pl  
wykop.pl has address 146.59.88.0  
wykop.pl has address 146.59.55.142  
wykop.pl has address 146.59.79.191  
wykop.pl mail is handled by 20 aspmx2.googlemail.com.  
wykop.pl mail is handled by 1 aspmx.l.google.com.  
wykop.pl mail is handled by 10 alt1.aspmx.l.google.com.  
wykop.pl mail is handled by 10 alt2.aspmx.l.google.com.
```

```
(stud@kali-vm)-[~]  
$ host -l wykop.pl cosmin.ns.cloudflare.com  
Using domain server:  
Name: cosmin.ns.cloudflare.com  
Address: 172.64.35.45#53  
Aliases:
```

```
Host wykop.pl not found: 1(FORMERR)  
; Transfer failed.
```

```
(stud@kali-vm)-[~]  
$ host -l wykop.pl elly.ns.cloudflare.com  
Using domain server:  
Name: elly.ns.cloudflare.com  
Address: 108.162.194.246#53  
Aliases:
```

```
Host wykop.pl not found: 1(FORMERR)  
; Transfer failed.
```

```
$ dig wykop.pl any  
  
; <<>> DiG 9.20.2-1-Debian <<>> wykop.pl any  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 42502  
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1220  
; COOKIE: d41597d04062589235e13921675f1523f9da885c63e1634f (good)  
;; QUESTION SECTION:  
;wykop.pl. IN ANY  
  
;; ANSWER SECTION:  
wykop.pl. 62518 IN NS cosmin.ns.cloudflare.com.  
wykop.pl. 62518 IN NS elly.ns.cloudflare.com.  
wykop.pl. 33 IN A 146.59.88.0  
wykop.pl. 33 IN A 146.59.55.142  
wykop.pl. 33 IN A 146.59.79.191  
  
;; Query time: 12 msec  
;; SERVER: 192.168.188.1#53(192.168.188.1) (TCP)  
;; WHEN: Sun Dec 15 18:42:59 CET 2024  
;; MSG SIZE rcvd: 170
```

```

(stud@kali-vm)-[~]
$ dig @8.8.8.8 wykop.pl

; <<>> DiG 9.20.2-1-Debian <<>> @8.8.8.8 wykop.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 38621
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;wykop.pl.                IN      A

;; ANSWER SECTION:
wykop.pl.                 60      IN      A      146.59.55.142
wykop.pl.                 60      IN      A      146.59.88.0
wykop.pl.                 60      IN      A      146.59.79.191

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Dec 15 18:44:23 CET 2024
;; MSG SIZE rcvd: 85

```

```

(stud@kali-vm)-[~]
$ dig @8.8.8.8 wykop.pl mx

; <<>> DiG 9.20.2-1-Debian <<>> @8.8.8.8 wykop.pl mx
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 12059
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;wykop.pl.                IN      MX

;; ANSWER SECTION:
wykop.pl.                 300     IN      MX      1 aspmx.l.google.com.
wykop.pl.                 300     IN      MX      10 alt2.aspmx.l.google.com.
wykop.pl.                 300     IN      MX      20 aspmx2.googlemail.com.
wykop.pl.                 300     IN      MX      10 alt1.aspmx.l.google.com.

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Dec 15 18:44:55 CET 2024
;; MSG SIZE rcvd: 147

```

```
(stud@kali-vm)-[~]
```

```
$ dig -x 8.8.8.8
```

```
; <<>> DiG 9.20.2-1-Debian <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 52483
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 1eb7850bc5c19b52c931ea9b675f15ba37e86d7e54ecb31d (good)
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.  42364   IN      PTR      dns.google.

;; Query time: 8 msec
;; SERVER: 192.168.188.1#53(192.168.188.1) (UDP)
;; WHEN: Sun Dec 15 18:45:31 CET 2024
;; MSG SIZE rcvd: 101
```

```
(stud@kali-vm)-[~]
```

```
$ dig wykop.pl +trace
```

```
; <<>> DiG 9.20.2-1-Debian <<>> wykop.pl +trace
;; global options: +cmd
.           42618   IN      NS      h.root-servers.net.
.           42618   IN      NS      c.root-servers.net.
.           42618   IN      NS      l.root-servers.net.
.           42618   IN      NS      d.root-servers.net.
.           42618   IN      NS      a.root-servers.net.
.           42618   IN      NS      k.root-servers.net.
.           42618   IN      NS      g.root-servers.net.
.           42618   IN      NS      j.root-servers.net.
.           42618   IN      NS      m.root-servers.net.
.           42618   IN      NS      f.root-servers.net.
.           42618   IN      NS      b.root-servers.net.
.           42618   IN      NS      i.root-servers.net.
.           42618   IN      NS      e.root-servers.net.
;; Received 267 bytes from 192.168.188.1#53(192.168.188.1) in 8 ms

pl.         172800  IN      NS      f-dns.pl.
pl.         172800  IN      NS      b-dns.pl.
pl.         172800  IN      NS      j-dns.pl.
pl.         172800  IN      NS      h-dns.pl.
pl.         172800  IN      NS      d-dns.pl.
pl.         172800  IN      NS      a-dns.pl.
pl.         86400   IN      DS      48559 8 2 6C7D94C6F25556EEB18
```

Zadanie 3c;

```
(stud@kali-vm)-[~]
$ dig wykop.pl SOA +noall +answer
wykop.pl. 1800 IN SOA cosmin.ns.cloudflare.com. dns
.cloudflare.com. 2356911600 10000 2400 604800 1800

(stud@kali-vm)-[~]
$ nslookup wykop.pl
Server: 192.168.188.1
Address: 192.168.188.1#53

Non-authoritative answer:
Name: wykop.pl
Address: 146.59.79.191
Name: wykop.pl
Address: 146.59.88.0
Name: wykop.pl
Address: 146.59.55.142

;; Query time: 8 msec
;; SERVER: 192.168.188.1#53(192.168.188.1) (UDP)
;; WHEN: Sun Dec 15 20:53:56 CET 2024
;; MSG SIZE rcvd: 113

;; Query time: 12 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Sun Dec 15 20:52:17 CET 2024
;; MSG SIZE rcvd: 85

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Dec 15 18:44:55 CET 2024
;; MSG SIZE rcvd: 147
```

Primary DNS: cosmin.ns.cloudflare.com

TTL: 1800s, domena zapisana w pamięci podręcznej DNS:

Czas żądania DNS: Query time = 16msec – bardzo szybka odpowiedź, rekord prawdopodobnie był w pamięci podręcznej Google DNS, 12msec dla Cloudflare DNS (1.1.1.1), 8msec dla lokalnego DNS.

Zadanie 4;

Użycie komendy dnsenum:

```
(stud@kali-vm)-[~]
$ dnsenum wykop.pl
dnsenum VERSION:1.3.1

———— wykop.pl ————

Host's addresses:
—————

wykop.pl. 14 IN A 146.59.79.19
1
wykop.pl. 14 IN A 146.59.55.14
2
wykop.pl. 14 IN A 146.59.88.0

Wildcard detection using: vcgjgnoubcbo
—————

vcgjgnoubcbo.wykop.pl. 300 IN CNAME wykop.pl.
wykop.pl. 14 IN A 146.59.55.14
2
wykop.pl. 14 IN A 146.59.88.0
wykop.pl. 14 IN A 146.59.79.19
```

Zadanie 5;

Użycie komendy `fierce`: (argument `dns` nie działał, więc użyłem `-domain`)

```
(stud@kali-vm)-[~]
$ fierce --domain wykop.pl
NS: cosmin.ns.cloudflare.com. elly.ns.cloudflare.com.
SOA: cosmin.ns.cloudflare.com. (172.64.35.45)
Zone: failure
Wildcard: 146.59.88.0, 146.59.79.191, 146.59.55.142
Found: email.wykop.pl. (34.111.99.212)
Nearby:
{'34.111.99.207': '207.99.111.34.bc.googleusercontent.com.',
 '34.111.99.208': '208.99.111.34.bc.googleusercontent.com.',
 '34.111.99.209': '209.99.111.34.bc.googleusercontent.com.',
 '34.111.99.210': '210.99.111.34.bc.googleusercontent.com.',
 '34.111.99.211': '211.99.111.34.bc.googleusercontent.com.',
 '34.111.99.212': '212.99.111.34.bc.googleusercontent.com.',
 '34.111.99.213': '213.99.111.34.bc.googleusercontent.com.',
 '34.111.99.214': '214.99.111.34.bc.googleusercontent.com.',
 '34.111.99.215': '215.99.111.34.bc.googleusercontent.com.',
 '34.111.99.216': '216.99.111.34.bc.googleusercontent.com.',
 '34.111.99.217': '217.99.111.34.bc.googleusercontent.com.'}
```

Zadanie 6;

Użycie komendy `tcptraceroute`:

```
(stud@kali-vm)-[~]
$ traceroute wykop.pl
traceroute to wykop.pl (146.59.79.191), 30 hops max, 60 byte packets
 1 fritz.box (192.168.188.1) 2.969 ms 2.766 ms 2.501 ms
 2 * * *
 3 host-87-99-33-89.internetia.net.pl (87.99.33.89) 6.267 ms 6.095 ms 5.8
74 ms
 4 POZNH002RT09.inetia.pl (83.238.248.22) 16.856 ms 11.901 ms 16.557 ms
 5 WARSC001RT91.inetia.pl (83.238.248.76) 30.776 ms 30.781 ms 12.506 ms
 6 be102.waw-wa1-pb1-nc5.pl.eu (178.33.100.202) 12.307 ms 8.741 ms 8.814
ms
 7 * * *
 8 * * *
 9 * * *
10 be101.waw1-oza1-g1-nc5.pl.eu (91.121.131.151) 47.000 ms 46.685 ms *
11 * * *
12 * * *
13 * * *
14 * * *
```



```

(stud@kali-vm)-[~]
$ sudo tcptraceroute wykop.pl
[sudo] password for stud:
Running:
      traceroute -T -O info wykop.pl
traceroute to wykop.pl (146.59.55.142), 30 hops max, 60 byte packets
 1 fritz.box (192.168.188.1)  0.436 ms  0.647 ms *
 2 * * *
 3 host-87-99-33-89.internetia.net.pl (87.99.33.89)  36.721 ms  4.849 ms  4.
683 ms
 4 POZNH002RT09.inetia.pl (83.238.248.22)  11.452 ms  13.226 ms  11.117 ms
 5 WARSC001RT91.inetia.pl (83.238.248.76)  12.897 ms  12.720 ms  12.749 ms
 6 be102.waw-wa1-pb1-nc5.pl.eu (178.33.100.202)  10.652 ms  8.493 ms  10.189
ms
 7 * * *
 8 * * *
 9 * * *
10 be101.waw1-oza1-g2-nc5.pl.eu (213.186.32.203)  12.611 ms *  9.988 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 ns31482055.ip-146-59-55.eu (146.59.55.142) <syn,ack,mss=1460,sack,timesta
mps>window_scaling>  12.305 ms  11.873 ms  13.053 ms

(stud@kali-vm)-[~]
$ sudo tctrace -i eth2 -d wykop.pl
1(1)    [192.168.188.1]
2(all)  Timeout
3(1)    [87.99.33.89]
4(1)    [83.238.248.22]
5(1)    [83.238.248.76]
6(1)    [178.33.100.202]
7(all)  Timeout
8(all)  Timeout
9(all)  Timeout
10(1)   [213.186.32.203]
11(all) Timeout
12(all) Timeout
13(all) Timeout
14(all) Timeout
15(1)   [146.59.55.142] (reached; open)

```

Zadanie 7;

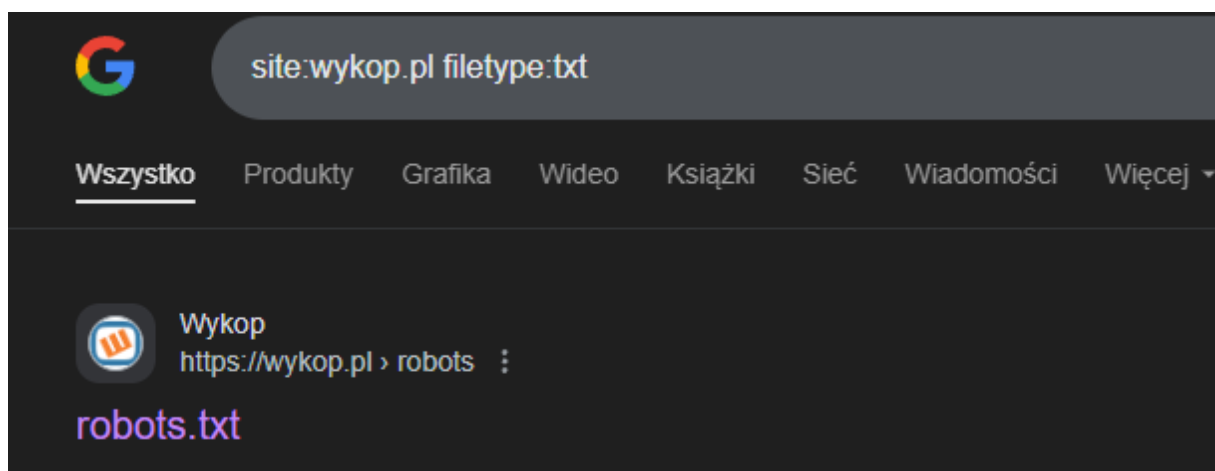
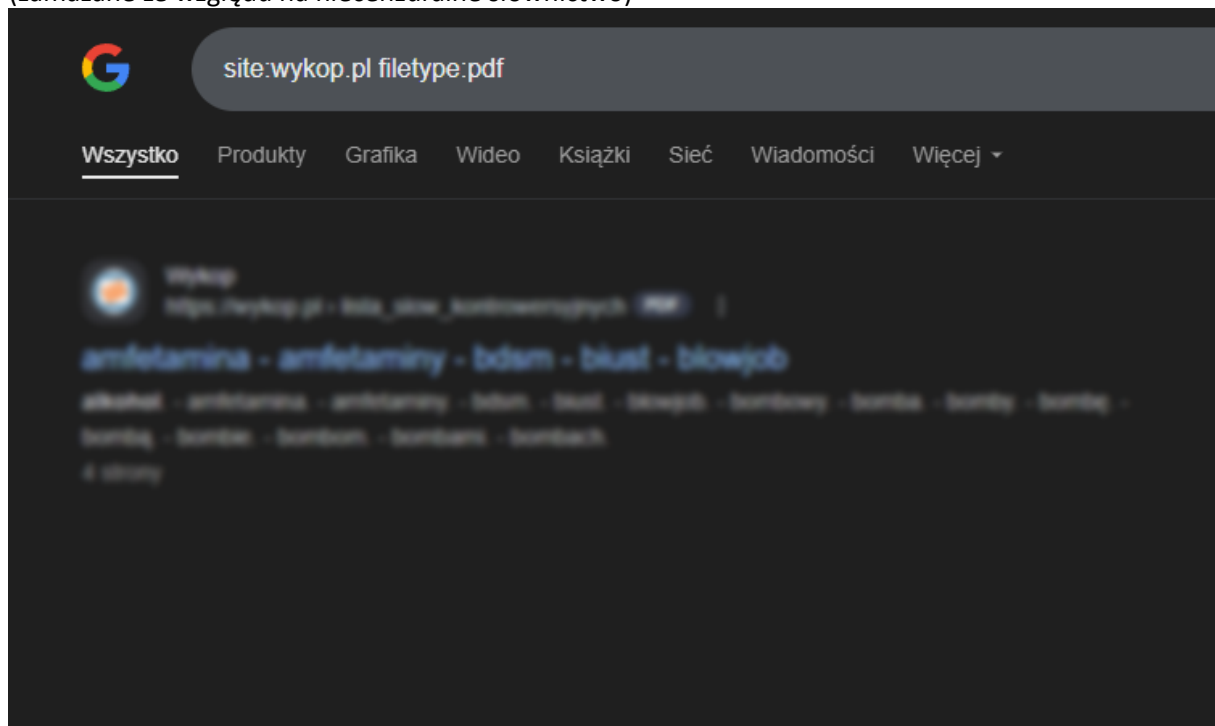
Narzędzia takie jak dig, traceroute, dnsenum, host i whois dostarczają informacji o domenach i infrastrukturze sieciowej. Dig i host są przydatne do analizowania rekordów typu DNS (A, MX, TXT), dnsenum automatyzuje wyszukiwanie subdomen oraz serwerów DNS, whois ujawnia informacje rejestrowe, takie jak dane właściciela domeny. Traceroute pokazuje trasę pakietów do celu, co pozwala na identyfikację węzłów sieciowych.

Złośliwy użytkownik może wykorzystać te dane do mapowania infrastruktury sieciowej, znajdowania potencjalnych punktów ataku, takich jak niechronione subdomeny czy słabe konfiguracje serwerów.

Najbardziej wszechstronnym narzędziem jest tutaj dnsenum, ponieważ automatyzuje on proces analizy DNS i odkrywa subdomeny i serwery, co daje dobry obraz infrastruktury docelowej domeny.

Zadanie 8;

(zamazane ze względu na niecenzuralne słownictwo)





site:pwr.edu.pl "adres" filetype:pdf

Wszystko

Grafika

Wiadomości

Wideo

Sieć

Książki

Finanse



Politechnika Wrocławska

<http://marek.piasecki.staff.iiar.pwr.edu.pl> > dydaktyka PDF

WSKAŹNIKI / ADRESY Wskaźnik → jest zmienną, która ...

Ogólna postać definicji wskaźnika: $\text{typ_danych} * \text{identyfikator wskaźnika}$;. Najczęściej używane są wskaźniki „zdefiniowane” zawierające **adres** innej zmiennej.

4 strony



pwr.edu.pl

<http://marek.piasecki.staff.iiar.pwr.edu.pl> > dydaktyka PDF

wskaźniki / adresy

może być to **adres** obszaru danych lub **adres** kodu programu). Ogólna postać ... Najczęściej używane są wskaźniki „zdefiniowane” zawierające **adres** innej zmiennej.



Politechnika Wrocławska

<https://wm.pwr.edu.pl> > public > dok_do_obrony PDF

Imię i nazwisko Adres e-mail (prywatny/

Adres e-mail (prywatny/ niestudencki!) Ja, niżej podpisany oświadczam, że zostałem poinformowany o tym, że: 1. Administratorem moich danych osobowych po ...



Wydział Informatyki i Telekomunikacji

<https://wit.pwr.edu.pl> > public > pdfy > kn_solvro PDF

Ogólny adres e-mail uczelnianej organizacji studenckiej

Ogólny **adres** e-mail uczelnianej organizacji studenckiej: sknsolvro@gmail.com ... Dane kontaktowe: **adres** e-mail, strona internetowa, media społecznościowe.

8 stron



site:pwr.edu.pl "adres" filetype:pdf



WYSZUKAJ


COPILOT

SZKOŁA

OBRA

Okolo 298 wynikow (0,17 s)

Liczba wyników – okolo 19 100



site:pwr.edu.pl intitle:"index of"

Wszystko

Grafika


Wideo

Wiadomości

Sieć

Książki

Finanse




Politechnika Wrocławska

https://kcir.pwr.edu.pl > ~witold

Index of /~witold/ip

Index of /~witold/ip ; [PARENTDIR], Parent Directory, -.



site:pwr.edu.pl "password" filetype:txt

Wszystko

Grafika


Wideo

Wiadomości

Sieć

Książki

Finanse




Politechnika Wrocławska

https://cs.pwr.edu.pl > articles > C... · Tłumaczenie strony

CHARI-eck.txt

RI can be understood as an universal solution for replacing login and **password** mechanisms. It has to secure against adversaries that gather personal data by ...



site:pwr.edu.pl filetype:doc

Wszystko

Produkty

Grafika


Wideo

Książki

Sieć

Wiadomości

Więcej



Politechnika Wrocławska

https://doktoranci.pwr.edu.pl > pliki > 5_w7_studi... **DOC**

I II III IV V VI VII VIII

Aby pokazać najbardziej trafne wyniki, pominęliśmy kilka pozycji bardzo podobnych do 1 już wyświetlonych.

Jeśli chcesz, możesz [powtórzyć wyszukiwanie z uwzględnieniem pominiętych wyników.](#)

Statystyki dla domeny pwr.edu.pl (wykop.pl posiadał jedynie pojedyncze archaiczne rekordy)

Pdf: 50700

Doc: 1

Docx: 1

Txt: 1370

Xls: 1

Ppt: 1

Zadanie 9;

Narzędzie the Harvester dla bing:

```
[*] Target: pwr.edu.pl

Created default api-keys.yaml at /home/stud/.theHarvester/api-keys.yaml
Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 2
-----
sekretariat.w3@pwr.edu.pl
wydz.bud@pwr.edu.pl

[*] Hosts found: 6
-----
archiwum-eportal.pwr.edu.pl
eportal.pwr.edu.pl
rekrutacja.pwr.edu.pl
wbliw.pwr.edu.pl
wch.pwr.edu.pl
wme.pwr.edu.pl

(stud@kali-vm)-[~]
$
```

Yahoo:

```
File Actions Edit View Help
* | _ | | | | _ / / _ / ( _ | | | | \ v / _
* \ _ | | | _ \ _ | v / / \ _ , _ | | \ / \ _
*
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: pwr.edu.pl

[*] Searching Yahoo.

[*] No IPs found.

[*] Emails found: 8
-----
biurokarier@pwr.edu.pl
eunika.zielony@pwr.edu.pl
klaudia.rzewnicka@pwr.edu.pl
malgorzata.skoczylas@pwr.edu.pl
nazwisko@pwr.edu.pl
rekrutacja@pwr.edu.pl
sugestiezdalne@pwr.edu.pl
wydz.bud@pwr.edu.pl
```

```
[*] Hosts found: 19
-----
biurokarier.pwr.edu.pl
ddo.pwr.edu.pl
dona.pwr.edu.pl
e.pwr.edu.pl
ePortal.pwr.edu.pl
eportal.pwr.edu.pl
iccci.pwr.edu.pl
iwe.pwr.edu.pl
kcir.pwr.edu.pl
kgig.pwr.edu.pl
kotwa.pwr.edu.pl
lpf.wppt.pwr.edu.pl
poczta.pwr.edu.pl
registration.pwr.edu.pl
rekrutacja.pwr.edu.pl
ulopolis.pwr.edu.pl
wbliw.pwr.edu.pl
zdalne.pwr.edu.pl
zielony.wppt.pwr.edu.pl
```

Baidu:

```
[*] Target: pwr.edu.pl
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 18
_____
anna.musial@pwr.edu.pl
bartosz.uniejewski@pwr.edu.pl
jedrzej.kozal@pwr.edu.pl
kamil.z...@pwr.edu.pl
katarzyna.maciejowska@pwr.edu.pl
lukasz.sterczewski@pwr.edu.pl
maciej.sobotka@pwr.edu.pl
michal.jasinski@pwr.edu.pl
michal.nikodem@pwr.edu.pl
ngoc-thanh.nguyen@pwr.edu.pl
palmowski@pwr.edu.pl
pawel.kaczynski@pwr.edu.pl
sahnawaz.alam@pwr.edu.pl
t.serafin@pwr.edu.pl
teddy.ferdinan@pwr.edu.pl
veronica.lott@pwr.edu.pl
witold.nawrot@pwr.edu.pl
zbigniew.palmowski@pwr.edu.pl
```

Linkedin: (niestety nie zadziałał)

```
(stud@kali-vm)-[~]
$ theHarvester -d pwr.edu.pl -l 100 -b linkedin
Read proxies.yaml from /home/stud/.theHarvester/proxies.yaml
*****
*                                                                 *
* | _ | _ | _ \ / _ \ ^ ^ _ \ _ \ _ \ / _ \ v _ | _ | _ | _ | _ | _ |   *
* | | | | _ | _ \ / _ \ ( | _ \ _ \ v _ \ _ \ || _ | _ | _ | _ | _ |   *
* | | | | | _ \ / _ \ , _ | _ \ _ \ || _ | _ | _ | _ | _ | _ |   *
* _ | _ | _ | _ \ / _ \ , _ | _ \ _ \ || _ | _ | _ | _ | _ | _ |   *
* _ | _ | _ | _ \ / _ \ , _ | _ \ _ \ || _ | _ | _ | _ | _ | _ |   *
* theHarvester 4.6.0                                           *
* Coded by Christian Martorella                               *
* Edge-Security Research                                       *
* cmartorella@edge-security.com                                *
* _ | _ | _ | _ \ / _ \ , _ | _ \ _ \ || _ | _ | _ | _ | _ | _ |   *
*****
[!] Invalid source.

(stud@kali-vm)-[~]
```

Zadanie 10-11;

Luki w zabezpieczeniach:
FTP:

CVE-2024-52309 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

SFTPGo is a full-featured and highly configurable SFTP, HTTP/S, FTP/S and WebDAV server - S3, Google Cloud Storage, Azure Blob. One powerful feature of SFTPGo is the ability to have the EventManager execute scripts or run applications in response to certain events. This feature is very common in all software similar to SFTPGo and is generally unrestricted. However, any SFTPGo administrator with permission to run a script has access to the underlying OS/container with the same permissions as the user running SFTPGo. This is unexpected for some SFTPGo administrators who think that there is a clear distinction between accessing the system shell and accessing the SFTPGo WebAdmin UI. To avoid this confusion, running system commands is disabled by default in 2.6.3, and an allow list has been added so that system administrators configuring SFTPGo must explicitly define which commands are allowed to be configured from the WebAdmin UI.

QUICK INFO

CVE Dictionary Entry:
CVE-2024-52309
NVD Published Date:
11/21/2024
NVD Last Modified:
11/21/2024
Source:
GitHub, Inc.

Tp-link router:

CVE-2024-54126 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

This vulnerability exists in the TP-Link Archer C50 due to improper signature verification mechanism in the firmware upgrade process at its web interface. An attacker with administrative privileges within the router's Wi-Fi range could exploit this vulnerability by uploading and executing malicious firmware which could lead to complete compromise of the targeted device.

Przykład luki

CVE-2021-41617 - OpenSSH w wersji 6.2-8.7 oraz wcześniejszych zawierał błąd w mechanizmie uwierzytelniania publiczkey. Atakujący mógł zdalnie zalogować się bez uwierzytelnienia w określonych warunkach. Przykładowo shodan.io pokazuje, że dla wersji 7.7 mamy 54 systemy z tą podatnością z tego większość (23) z Włoch. <https://nvd.nist.gov/vuln/detail/CVE-2021-41617>

SHODAN

Explore

Pricing

OpenSSH 7.7


Q

Login

TOTAL RESULTS

54

TOP COUNTRIES



Italy	23
Germany	5
France	5
United States	5
Hungary	3
More...	

View Report

View on Map

Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

195.254.241.117

static-241117.xdsl.raiffe
isen.net
KONVERTO SPA
Italy, Milan

SSH-2.0-OpenSSH_7.7 FreeBSD-openssh-portable-7.7.p1_6,1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQGA8wDhheCT9nutneK1xe1KXNvF0lVrasyZqYsyATLgd
4LZZMteuZn7IjILWQKwfmQ5Gwqz+G0lltbaOVlKcm4qGymv174IH9kHPw79j77lpt9sa5Vovevk
So2cg6LX9136xPRZaHvRQAP3BLnAmPvc8C0X9ZncZxBahvbaXNYAXZ6kvgZkb...

2024-12-15T13:32:25.133814

192.96.24.93

storage-web.posix.co.za
a
Posix Systems (Pty)
Ltd
South
Africa, Johannesburg

SSH-2.0-OpenSSH_7.7 FreeBSD-openssh-portable-7.7.p1_6,1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQGC/v+qybEukn8SKJ5cvpJ95GhjsCjUwY80d0zbs9ZnRfAB
P2mKT3yoabhF65Lb1IQefE66KngMotouyFoCI1/V44g1f7+20kg9PLnXsvkkfDIKCE3QLKXLM0
3yftbCXT/YC0qdfRHTetaotL1Zf7GL4B37EP/Ae1lwQtea0Q1ws2LEHfrozmo...

2024-12-15T12:52:14.221529

185.230.82.37

37.82.230.185.ip.dolom

SSH-2.0-OpenSSH_7.7 FreeBSD-openssh-portable-7.7.p1_6,1

2024-12-15T12:06:24.800404