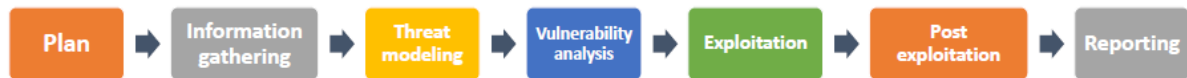


Penetration testing



Planning

Scope : Team project5 jackson nano

Goal : Penetration test with project artifacts to find vulnerabilities.

Information gathering

Environments

- IP addresses : 192.168.0.166
- Network protections : Nothing

OS Version

```
uname -a
```

```
Linux LgFaceRecProject 4.9.201-tegra #1 SMP PREEMPT Fri Feb 19 08:40:32 PST 2021  
aarch64 aarch64 aarch64 GNU/Linux
```

```
lsb_release -a
```

```
No LSB modules are available.
```

```
Distributor ID: Ubuntu
```

```
Description:   Ubuntu 18.04.5 LTS
```

```
Release:      18.04
```

```
Codename:     bionic
```

```
cat /proc/version
```

```
Linux version 4.9.201-tegra (buildbrain@mobile-u64-5294-d8000) (gcc version 7.3.1  
20180425 [linaro-7.3-2018.05 revision d29120a424ecfbc167ef90065c0eeb7f91977701]  
(Linaro GCC 7.3-2018.05) ) #1 SMP PREEMPT Fri Feb 19 08:40:32 PST 2021
```

Software Package Version

```
cryptmount-5.2.4
openssl - 1.1.1-1ubuntu2.1~18 arm64
```

nmap scanning result

```
Host is up (0.0005s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain       dnsmasq 2.79
111/tcp   open  rpcbind      2-4 (RPC #100000)
3389/tcp  open  ms-wbt-server xrdp
5000/tcp  open  upnp?
5001/tcp  open  tcpwrapped
6000/tcp  open  X11?
6001/tcp  open  X11:1?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- 5000 & 5001 tcp port for non-secure mode
- 6000 & 6001 tcp port for secure mode

Threat Modeling

It checks whether there is a way to penetrate Team5's end product through vulnerabilities contained by the Software or OS.

1. Exploits the TCP port used by the implemented SW, causing system malfunction.
2. Exploits the TCP port used by the implemented SW to obtain root through privilege escalation.
3. Exploits the TCP port used by implemented SW to cause crash/hang of services and reduce availability.
4. Find vulnerabilities in other ports running on the OS and penetrate to cause system malfunctions or acquire root.

Vulnerability analysis & exploitation

To analyze the vulnerabilities, we analyzed some of the tools mentioned in the class and confirmed that they are available in this phase2.

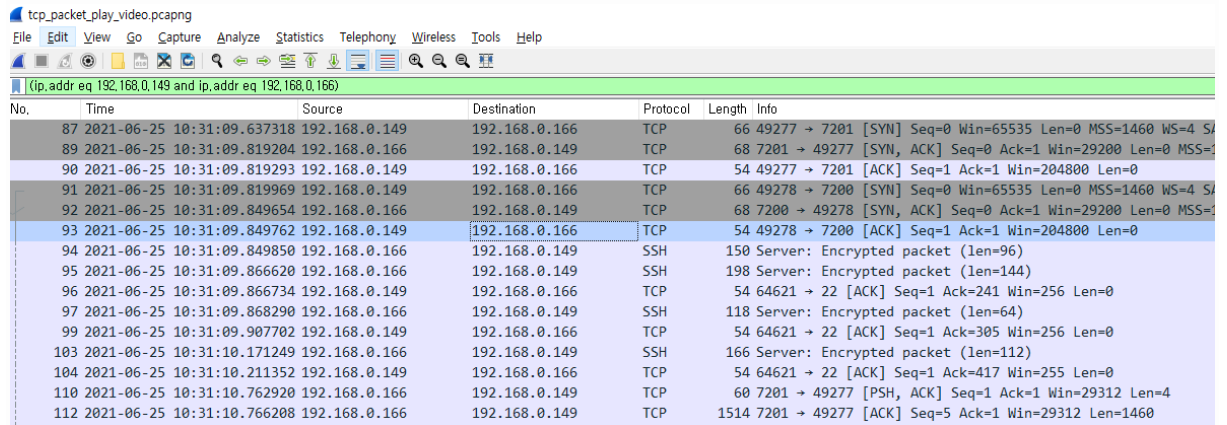
Test Domain	How to test	Tools
Network System	Check communication data between server and client	wireshark, Burp Suite, netcat
Server/Client System	Check the vulnerabilities in a program or OS system.	netcat, nmap, metasploit
Library used in Server/Client	Check the version of the library used and find there is a public CVE that has not	Searching internet

been improved.

Network System Analysis with wireshark

1. non-secure mode

Checked : There is no encryption and handshake. It is a normal operation.



tcp_packet_play_video.pcapng

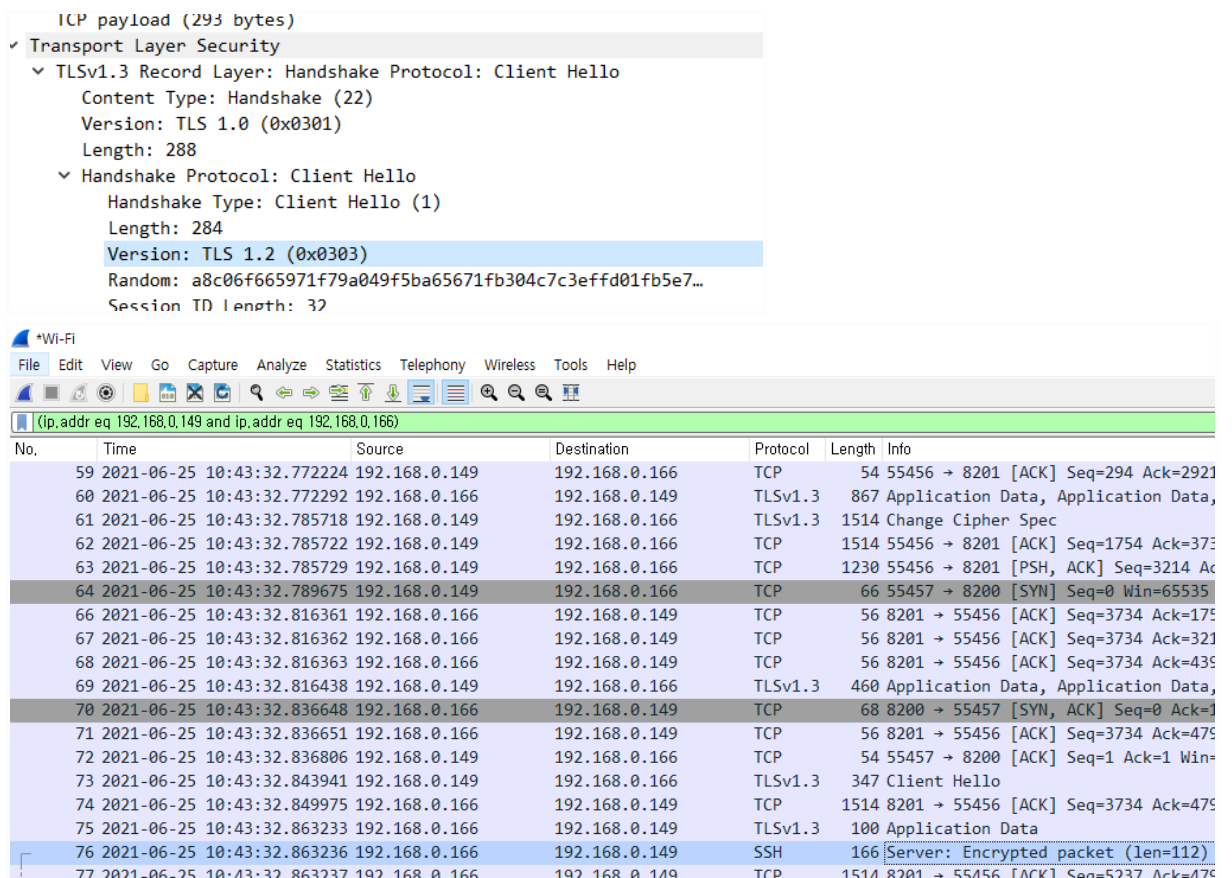
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 192.168.0.149 and ip.addr eq 192.168.0.166)

No.	Time	Source	Destination	Protocol	Length	Info
87	2021-06-25 10:31:09.637318	192.168.0.149	192.168.0.166	TCP	66	49277 → 7201 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 S
89	2021-06-25 10:31:09.819204	192.168.0.166	192.168.0.149	TCP	68	7201 → 49277 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
90	2021-06-25 10:31:09.819293	192.168.0.149	192.168.0.166	TCP	54	49277 → 7201 [ACK] Seq=1 Ack=1 Win=204800 Len=0
91	2021-06-25 10:31:09.819969	192.168.0.149	192.168.0.166	TCP	66	49278 → 7200 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 S
92	2021-06-25 10:31:09.849654	192.168.0.166	192.168.0.149	TCP	68	7200 → 49278 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
93	2021-06-25 10:31:09.849762	192.168.0.149	192.168.0.166	TCP	54	49278 → 7200 [ACK] Seq=1 Ack=1 Win=204800 Len=0
94	2021-06-25 10:31:09.849850	192.168.0.166	192.168.0.149	SSH	150	Server: Encrypted packet (len=96)
95	2021-06-25 10:31:09.866620	192.168.0.166	192.168.0.149	SSH	198	Server: Encrypted packet (len=144)
96	2021-06-25 10:31:09.866734	192.168.0.149	192.168.0.166	TCP	54	64621 → 22 [ACK] Seq=1 Ack=241 Win=256 Len=0
97	2021-06-25 10:31:09.868290	192.168.0.166	192.168.0.149	SSH	118	Server: Encrypted packet (len=64)
99	2021-06-25 10:31:09.907702	192.168.0.149	192.168.0.166	TCP	54	64621 → 22 [ACK] Seq=1 Ack=305 Win=256 Len=0
103	2021-06-25 10:31:10.171249	192.168.0.166	192.168.0.149	SSH	166	Server: Encrypted packet (len=112)
104	2021-06-25 10:31:10.211352	192.168.0.149	192.168.0.166	TCP	54	64621 → 22 [ACK] Seq=1 Ack=417 Win=255 Len=0
110	2021-06-25 10:31:10.762920	192.168.0.166	192.168.0.149	TCP	60	7201 → 49277 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=4
112	2021-06-25 10:31:10.766208	192.168.0.166	192.168.0.149	TCP	1514	7201 → 49277 [ACK] Seq=5 Ack=1 Win=29312 Len=1460

2. secure mode

Checked : handshake for tls communication and verified crypto communication.



ICP payload (293 bytes)

✓ Transport Layer Security

- TLsv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 288
- Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 284
 - Version: TLS 1.2 (0x0303)
 - Random: a8c06f665971f79a049f5ba65671fb304c7c3effd01fb5e7...
 - Session ID Length: 32

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 192.168.0.149 and ip.addr eq 192.168.0.166)

No.	Time	Source	Destination	Protocol	Length	Info
59	2021-06-25 10:43:32.772224	192.168.0.149	192.168.0.166	TCP	54	55456 → 8201 [ACK] Seq=294 Ack=2921
60	2021-06-25 10:43:32.772292	192.168.0.166	192.168.0.149	TLsv1.3	867	Application Data, Application Data,
61	2021-06-25 10:43:32.785718	192.168.0.149	192.168.0.166	TLsv1.3	1514	Change Cipher Spec
62	2021-06-25 10:43:32.785722	192.168.0.149	192.168.0.166	TCP	1514	55456 → 8201 [ACK] Seq=1754 Ack=373
63	2021-06-25 10:43:32.785729	192.168.0.166	192.168.0.166	TCP	1230	55456 → 8201 [PSH, ACK] Seq=3214 Ac
64	2021-06-25 10:43:32.789675	192.168.0.149	192.168.0.166	TCP	66	55457 → 8200 [SYN] Seq=0 Win=65535
66	2021-06-25 10:43:32.816361	192.168.0.166	192.168.0.149	TCP	56	8201 → 55456 [ACK] Seq=3734 Ack=175
67	2021-06-25 10:43:32.816362	192.168.0.166	192.168.0.149	TCP	56	8201 → 55456 [ACK] Seq=3734 Ack=321
68	2021-06-25 10:43:32.816363	192.168.0.166	192.168.0.149	TCP	56	8201 → 55456 [ACK] Seq=3734 Ack=435
69	2021-06-25 10:43:32.816438	192.168.0.149	192.168.0.166	TLsv1.3	460	Application Data, Application Data,
70	2021-06-25 10:43:32.836648	192.168.0.166	192.168.0.149	TCP	68	8200 → 55457 [SYN, ACK] Seq=0 Ack=1
71	2021-06-25 10:43:32.836651	192.168.0.166	192.168.0.149	TCP	56	8201 → 55456 [ACK] Seq=3734 Ack=475
72	2021-06-25 10:43:32.836806	192.168.0.149	192.168.0.166	TCP	54	55457 → 8200 [ACK] Seq=1 Ack=1 Win=
73	2021-06-25 10:43:32.843941	192.168.0.149	192.168.0.166	TLsv1.3	347	Client Hello
74	2021-06-25 10:43:32.849975	192.168.0.166	192.168.0.149	TCP	1514	8201 → 55456 [ACK] Seq=3734 Ack=475
75	2021-06-25 10:43:32.863233	192.168.0.166	192.168.0.149	TLsv1.3	100	Application Data
76	2021-06-25 10:43:32.863236	192.168.0.166	192.168.0.149	SSH	166	Server: Encrypted packet (len=112)
77	2021-06-25 10:43:32.863237	192.168.0.166	192.168.0.149	TCP	1514	8201 → 55456 [ACK] Seq=5237 Ack=475

Burp Suite : Supports the ability to run from browser in client, configure proxy in local, and check and forward packets one by one. In this project, it was difficult to do something using that tool, and we found another tool that could configure proxy on the local, but there was no significant difference from Wireshark.

netcat : This tool can network scan and other things. Especially, we can acquire a shell if netcat is run on the server side by reserving port.

System Analysis with Metasploit

1. We can't find exploit methods for port 500/5001/6000/6001 which are reserved for server(camera) service.
2. rpcbind using port 111 has below CVEs.
check rpcbind version : 0.2.3-0.6ubuntu0.18.04.1 arm64

```
hedaesik@LgFaceRecProject:~$ dpkg -l rpcbind
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
++-----+
|| Name          | Version              | Architecture | Description
++-----+
ii rpcbind       | 0.2.3-0.6ubuntu0.18.04.1 | arm64        | converts RPC program numbers into universal addresses
```

- CVE-2010-2061 (gain privilege to local users only)
- CVE-2010-2064 (gain privilege to local users only)
- CVE-2017-8779 (script : auxiliary/dos/rpc/rpcbomb)

The DOS attack was successful through the script corresponding to this CVE item, and the camera image was stopped in the Client due to the DOS attack.

3. xrdp using port 3389 has below CVEs. But xrdp's version is higher than the issued version including found CVE.

```
xrdp -v

xrdp: A Remote Desktop Protocol server.
Copyright (C) Jay Sorg 2004-2014
See http://www.xrdp.org for more information.
Version 0.9.5
```

- CVE-2008-5903 (xrdp <=0.4.1)
- CVE-2008-5902 (xrdp <=0.4.1)
- CVE-2008-5904 (xrdp <=0.4.1)

Library used in Server/Client

Team5 guide that we should install openssl by apt-get command. We install openssl to build and run a server program. Latest openssl version is 1.1.1k but openssl 1.1.1 is installed when installing the library with the "apt-get" command.

- openssl : 1.1.1-1

```
hedaesik@LgFaceRecProject:~/work$ openssl version
OpenSSL 1.1.1 11 Sep 2018
hedaesik@LgFaceRecProject:~/work$ dpkg -l | grep openssl
ii  openssl                    1.1.1-1ubuntu2.1~18.04.9
Secure Sockets Layer toolkit - cryptographic utility
```

arm64

openssl CVEs list : [Openssl CVE list](#)

We checked for vulnerabilities between 1.1.1 and 1.1.1k versions.
There are 14 vulnerabilities after version 1.1.1 and all are resolved in 1.1.1k.

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2018	2														
2019	6			1							1				
2020	1	1													
2021	5	2		2						1					
Total	14	3		2						1	1				

We can't find metasploit scripts but there are some vulnerabilities causing crashes and dos.

Team5 guide that we should install cryptmount and cryptsetup by apt-get command. We install cryptmount and it's dependency module. The Below package is installed to the system. To minimize vulnerabilities, investigation and improvements are also required for 3rd party libraries used in programs.

- **cryptmount : 5.2.4-1**

```
hedaesik@LgFaceRecProject:~/work$ dpkg -l | grep cryptmount
ii  cryptmount                    5.2.4-1build1
Management of encrypted file systems
```

arm64

CVE list : No CVE list.

- **cryptsetup : 2.0.2-1**

```
hedaesik@LgFaceRecProject:~/work$ dpkg -l | grep cryptsetup
ii  cryptsetup                    2:2.0.2-1ubuntu1.2
disk encryption support - startup scripts
```

arm64

CVE list : [CVE list for cryptsetup](#)

- **libdevmapper : 1.02.145-4.1**

```
hedaesik@LgFaceRecProject:~/work$ dpkg -l | grep libdevmapper
```

ii libdevmapper1.02.1:arm64 arm64 Linux Kernel Device Mapper userspace library	2:1.02.145-4.1ubuntu3.18.04.3
-----------------------------------------------------------------------------------	-------------------------------

CVE list : No CVE list.

- **libgcrypt20 : 1.8.1**

hedaesik@LgFaceRecProject:~/work\$ dpkg -l grep libgcrypt20 ii libgcrypt20:arm64 1.8.1-4ubuntu1.2 LGPL Crypto library - runtime library	arm64
----------------------------------------------------------------------------------------------------------------------------------------------------	-------

CVE list : [CVE list for libgcrypt](#)

Post exploitation & reporting

Executive summary of results

Team potential performed a penetration test on the final artifact of Team5. Team 5 artifacts provide a streaming and face recognition service using a camera.

The aim of this assessment was to discover the vulnerabilities present in the team 5 artifacts which could pose an information security risk.

This assessment was performed from 06/22/2021 to 06/28/2021.

The vulnerabilities have been marked according to the following table:

Severity	Description
Critical	Easy exploitation / High business impact
High	Indirect exploitation / Limited target scope / Required privilege
Medium	Difficult exploitation / Low business impact
Low	Low and information level issues

Executive summary of results

We checked the following items.

1. Server/Client System
2. Network System
3. DDos
4. Library used in Server/Client

Penetration Results

	Urgent	Critical	High	Medium	Low
Server/Client System					
Network System					
DDos			1		
Library used in Server/Client					
Total	0	0	1	0	0

One issue found is as follows.

Issue	Type	Impact	Total Score
Dos attack to opened port used for rpcbind.	Dos(Denial Of Service)	Camera streaming is stop and	high

When dos attack is successful, the camera is not operated and also the admin can't connect to the camera. Then the admin can't restart the camera program because there is no scenario to run programs automatically. So risk of dos attack is assessed to high.

Recommendations

Set up systemd for production products so that the rpc bind does not work, and prevent dos attacks through firewall in the network environment where the actual product works.

For libraries that your application uses, we recommend that you use the latest version that addresses security issues, etc.