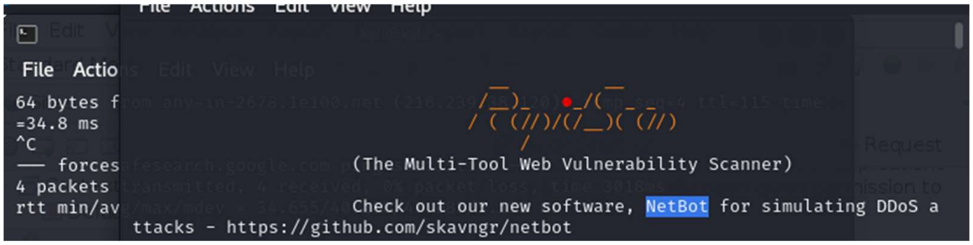
Lampiran

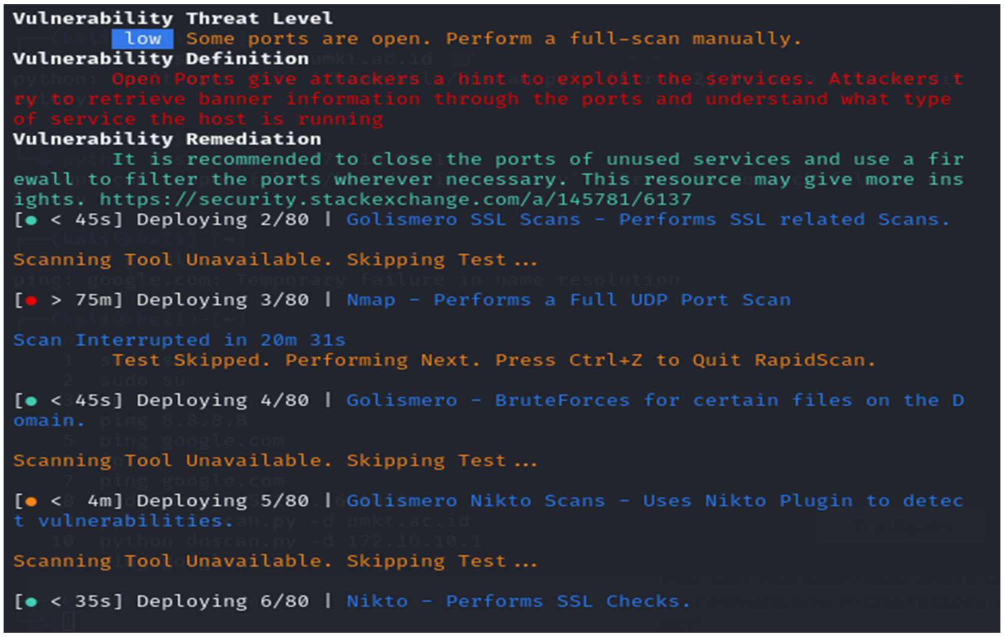
Lampiran1 : Riwayat Hidup

Fitria Nur Yaqin, lahir di Samarinda 13 Desember 2001. Penulis lahir dari Ibu Suparti dan Bapak Normani yang merupakan anak ketiga dari tiga bersaudara. Pada tahun 2007 penulis masuk Sekolah Dasar Negeri 012 Sungai Kunjang dan lulus pada tahun 2013. Pada tahun yang sama melanjutkan Pendidikan di SMPN 25 Samarinda dan lulus pada tahun 2016. Kemudian pada tahun 2016 melanjutkan pendidikan di SMK Negeri 2 Samarinda Jurusan Teknik Listrik dan lulus pada tahun 2019. Pada tahun 2019 Penulis melanjutkan pendidikan perguruan tinggi di Universitas Muhammadiyah Kalimantan Timur dengan melalui jalur mandiri dan di terima pada Program Studi S1 Teknik Informatika.

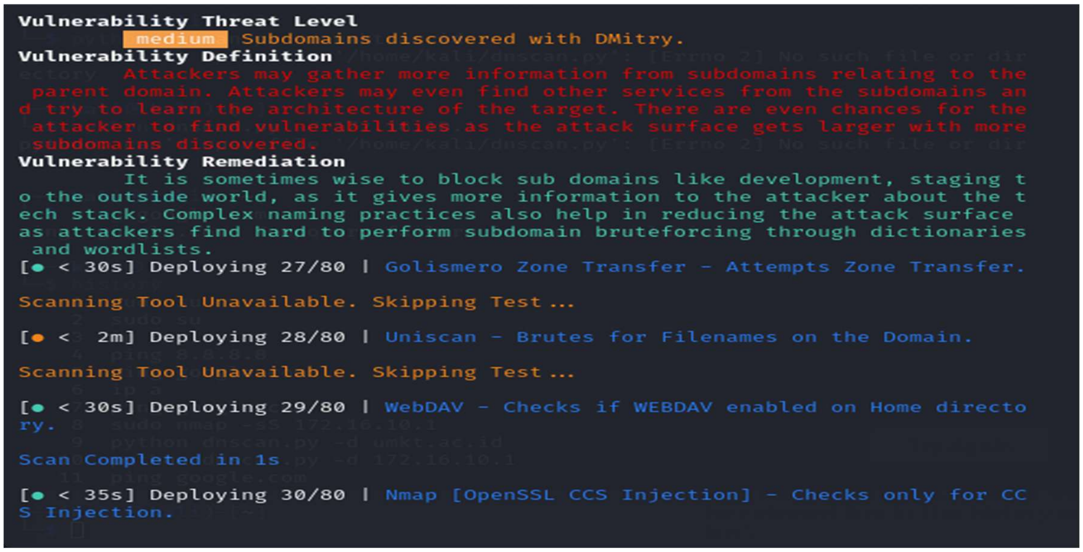
Lampiran 2 Hasil Scaning



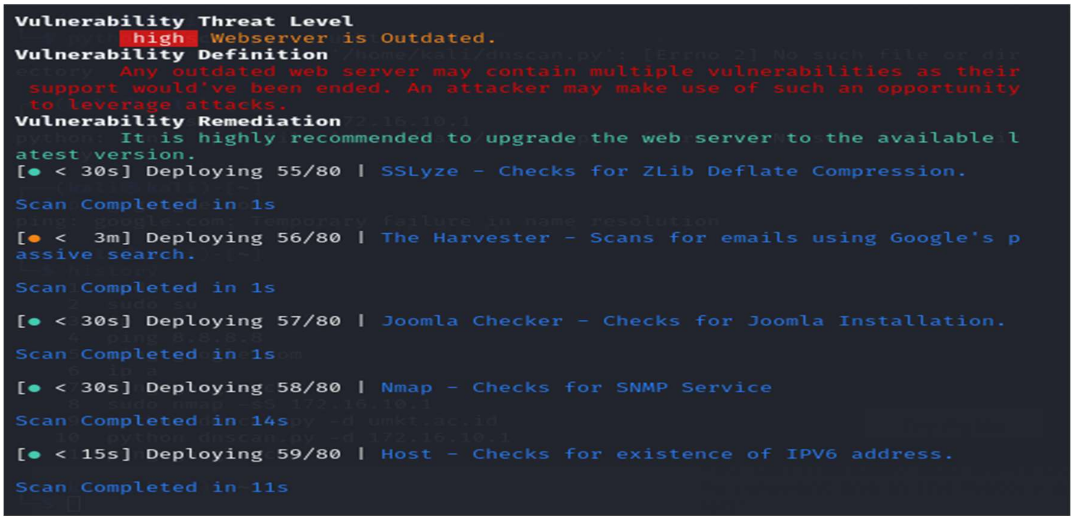
```
64 bytes f
=34.8 ms
^C
—— forces
4 packets
rtt min/av
                    (The Multi-Tool Web Vulnerability Scanner)

                    Check out our new software, NetBot for simulating DDoS a
ttacks - https://github.com/skavngr/netbot
```



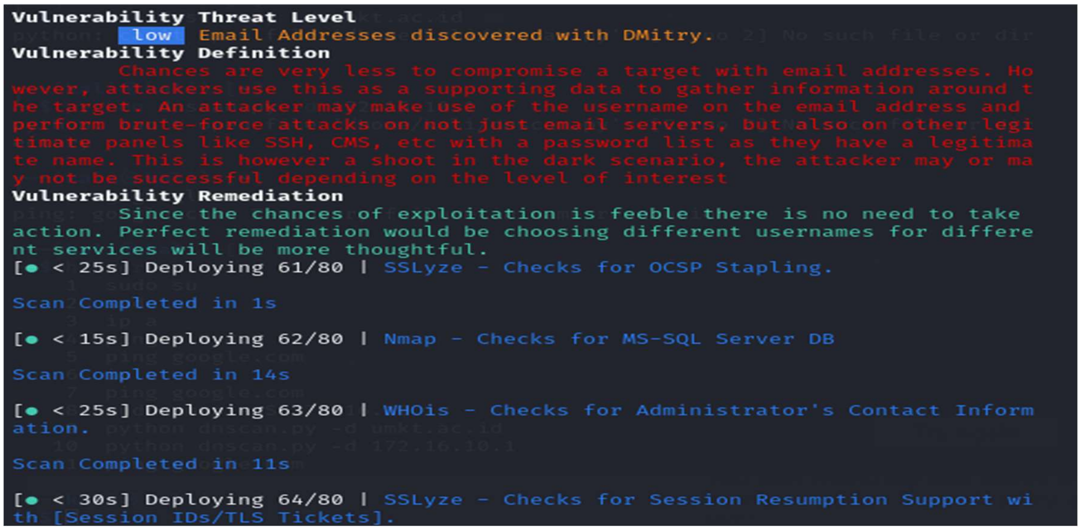
```
Vulnerability Threat Level
        low  Some ports are open. Perform a full-scan manually.
Vulnerability Definition
        Open Ports give attackers a hint to exploit the services. Attackers t
ry to retrieve banner information through the ports and understand what type
of service the host is running
Vulnerability Remediation
        It is recommended to close the ports of unused services and use a fir
ewall to filter the ports wherever necessary. This resource may give more ins
ights. https://security.stackexchange.com/a/145781/6137
[● < 45s] Deploying 2/80 | Golismero SSL Scans - Performs SSL related Scans.

Scanning Tool Unavailable. Skipping Test...

[● > 75m] Deploying 3/80 | Nmap - Performs a Full UDP Port Scan

Scan Interrupted in 20m 31s
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 45s] Deploying 4/80 | Golismero - BruteForces for certain files on the D
omain.

Scanning Tool Unavailable. Skipping Test...

[● <  4m] Deploying 5/80 | Golismero Nikto Scans - Uses Nikto Plugin to detec
t vulnerabilities.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 6/80 | Nikto - Performs SSL Checks.
```



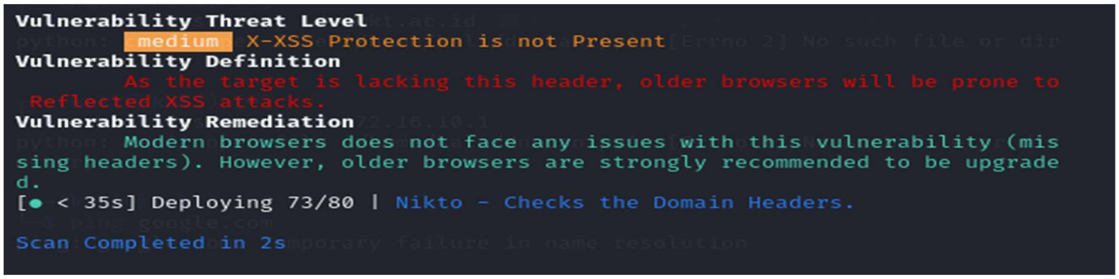
```
Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the
 parent domain. Attackers may even find other services from the subdomains an
d try to learn the architecture of the target. There are even chances for the
 attacker to find vulnerabilities as the attack surface gets larger with more
 subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging t
o the outside world, as it gives more information to the attacker about the t
ech stack. Complex naming practices also help in reducing the attack surface
as attackers find hard to perform subdomain bruteforcing through dictionaries
 and wordlists.
[● < 30s] Deploying 27/80 | Golismero Zone Transfer - Attempts Zone Transfer.

Scanning Tool Unavailable. Skipping Test ...

[● <  2m] Deploying 28/80 | Uniscan - Brutes for Filenames on the Domain.

Scanning Tool Unavailable. Skipping Test ...

[● < 30s] Deploying 29/80 | WebDAV - Checks if WEBDAV enabled on Home directo
ry.

Scan Completed in 1s

[● < 35s] Deploying 30/80 | Nmap [OpenSSL CCS Injection] - Checks only for CC
S Injection.
```



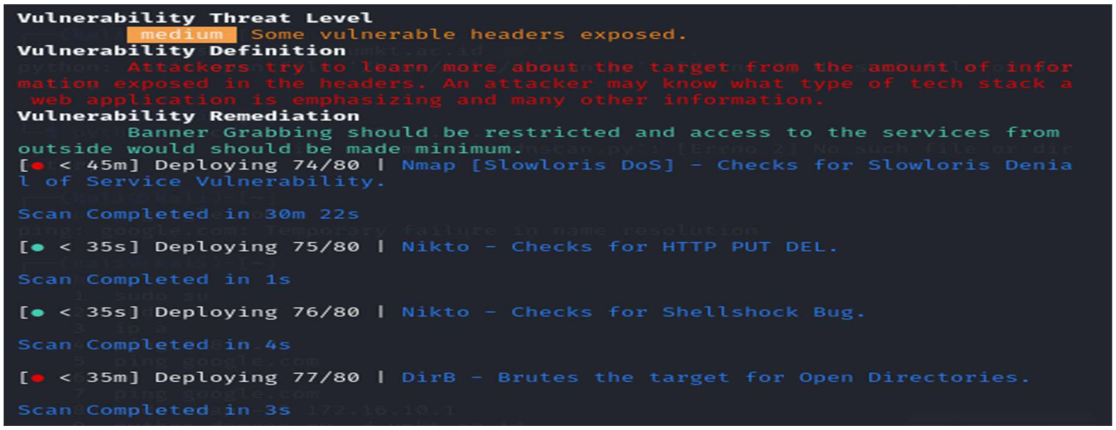
```
Vulnerability Threat Level
        high  Webserver is Outdated.
Vulnerability Definition
        Any outdated web server may contain multiple vulnerabilities as their
 support would've been ended. An attacker may make use of such an opportunity
 to leverage attacks.
Vulnerability Remediation
        It is highly recommended to upgrade the web server to the available l
atest version.
[● < 30s] Deploying 55/80 | SSLyze - Checks for ZLib Deflate Compression.

Scan Completed in 1s

[● <  3m] Deploying 56/80 | The Harvester - Scans for emails using Google's p
assive search.

Scan Completed in 1s

[● < 30s] Deploying 57/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 1s

[● < 30s] Deploying 58/80 | Nmap - Checks for SNMP Service

Scan Completed in 14s

[● < 15s] Deploying 59/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 11s
```



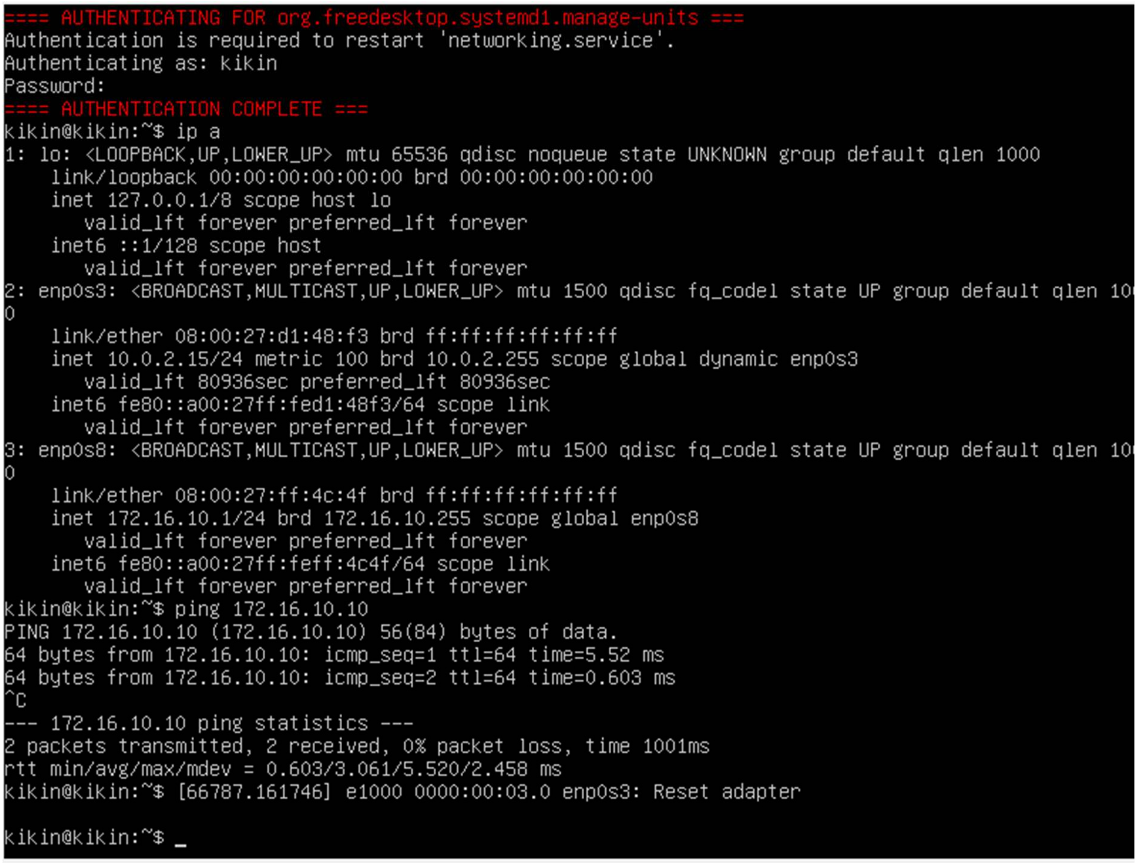
```
Vulnerability Threat Level
         low   Email Addresses discovered with DMitry.
Vulnerability Definition
        Chances are very less to compromise a target with email addresses. Ho
wever, attackers use this as a supporting data to gather information around t
he target. An attacker may make use of the username on the email address and
perform brute-force attacks on not just email servers, but also on other legi
timate panels like SSH, CMS, etc with a password list as they have a legitima
te name. This is however a shoot in the dark scenario, the attacker may or ma
y not be successful depending on the level of interest
Vulnerability Remediation
        Since the chances of exploitation is feeble there is no need to take
action. Perfect remediation would be choosing different usernames for differe
nt services will be more thoughtful.
[● < 25s] Deploying 61/80 | SSLyze - Checks for OCSP Stapling.

Scan Completed in 1s

[● < 15s] Deploying 62/80 | Nmap - Checks for MS-SQL Server DB

Scan Completed in 14s

[● < 25s] Deploying 63/80 | WHOis - Checks for Administrator's Contact Inform
ation.

Scan Completed in 11s

[● < 30s] Deploying 64/80 | SSLyze - Checks for Session Resumption Support wi
th [Session IDs/TLS Tickets].
```



```
Vulnerability Threat Level
         medium   X-XSS Protection is not Present
Vulnerability Definition
         As the target is lacking this header, older browsers will be prone to
 Reflected XSS attacks.
Vulnerability Remediation
         Modern browsers does not face any issues with this vulnerability (mis
sing headers). However, older browsers are strongly recommended to be upgrade
d.
[● < 35s] Deploying 73/80 | Nikto - Checks the Domain Headers.

Scan Completed in 2s
```

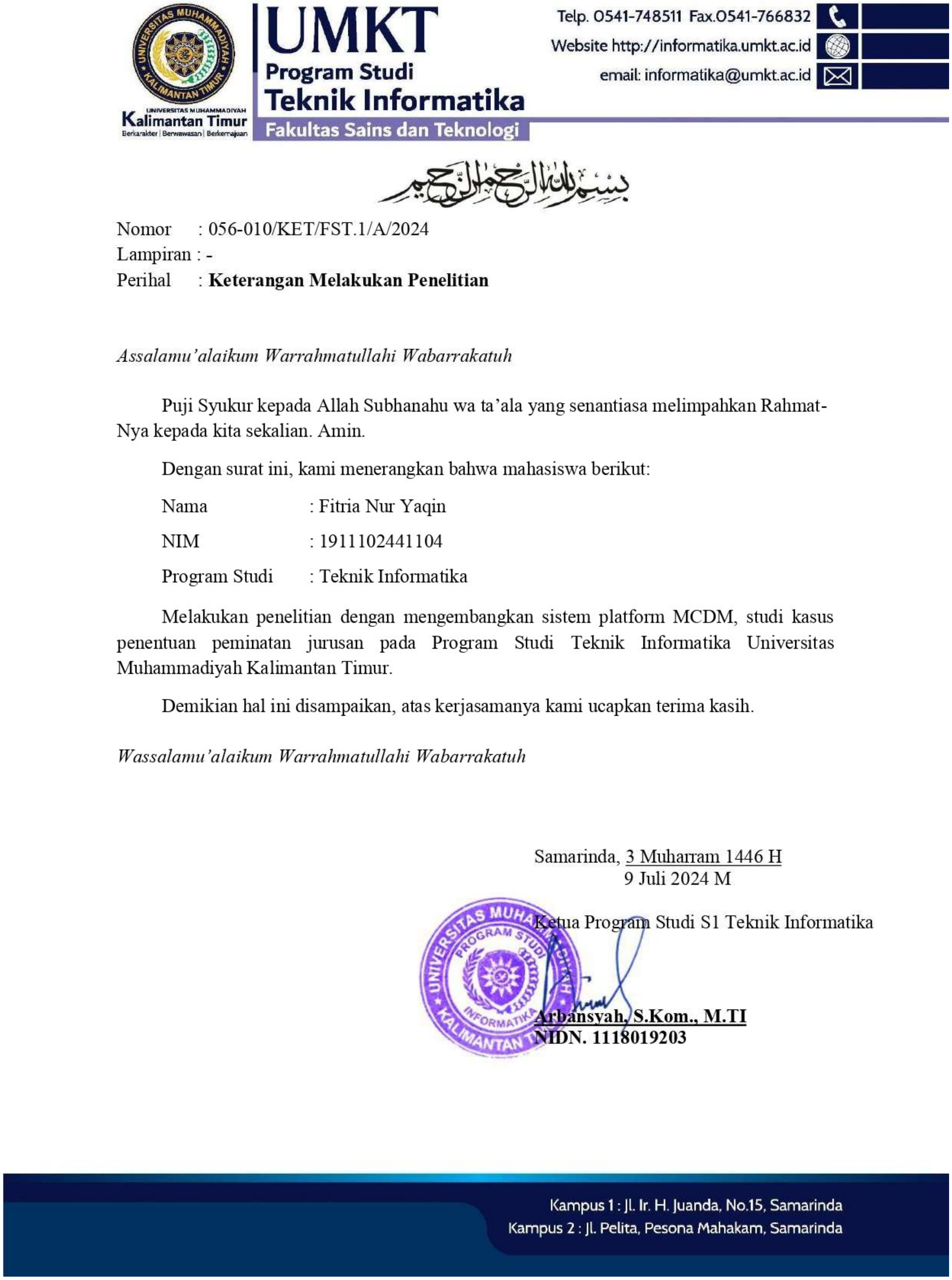


```
Vulnerability Threat Level
         medium   Some vulnerable headers exposed.
Vulnerability Definition
         Attackers try to learn more about the target from the amount of infor
mation exposed in the headers. An attacker may know what type of tech stack a
 web application is emphasizing and many other information.
Vulnerability Remediation
         Banner Grabbing should be restricted and access to the services from
outside would should be made minimum.
[● < 45m] Deploying 74/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denia
l of Service Vulnerability.

Scan Completed in 30m 22s

[● < 35s] Deploying 75/80 | Nikto - Checks for HTTP PUT DEL.

Scan Completed in 1s

[● < 35s] Deploying 76/80 | Nikto - Checks for Shellshock Bug.

Scan Completed in 4s

[● < 35m] Deploying 77/80 | DirB - Brutes the target for Open Directories.

Scan Completed in 3s
```



```
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'networking.service'.
Authenticating as: kikin
Password:
==== AUTHENTICATION COMPLETE ===
kikin@kikin:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:d1:48:f3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 80936sec preferred_lft 80936sec
    inet6 fe80::a00:27ff:fed1:48f3/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:ff:4c:4f brd ff:ff:ff:ff:ff:ff
    inet 172.16.10.1/24 brd 172.16.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feff:4c4f/64 scope link
       valid_lft forever preferred_lft forever
kikin@kikin:~$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_seq=1 ttl=64 time=5.52 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=64 time=0.603 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.603/3.061/5.520/2.458 ms
kikin@kikin:~$ [66787.161746] e1000 0000:00:03.0 enp0s3: Reset adapter

kikin@kikin:~$ _
```

Lampiran 3 Surat ijin Penelitian



UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
UNIVERSITAS MUHAMMADIYAH
Kalimantan Timur
Berkarakter | Berwawasan | Berkemajuan

UMKT
Program Studi
Teknik Informatika
Fakultas Sains dan Teknologi

Telp. 0541-748511 Fax.0541-766832 ☎
Website http://informatika.umkt.ac.id
email: informatika@umkt.ac.id ✉

بسم الله الرحمن الرحيم

Nomor : 056-010/KET/FST.1/A/2024
Lampiran : -
Perihal : **Keterangan Melakukan Penelitian**

Assalamu'alaikum Warrahmatullahi Wabarrakatuh

Puji Syukur kepada Allah Subhanahu wa ta'ala yang senantiasa melimpahkan Rahmat-Nya kepada kita sekalian. Amin.

Dengan surat ini, kami menerangkan bahwa mahasiswa berikut:

Nama : Fitria Nur Yaqin
NIM : 1911102441104
Program Studi : Teknik Informatika

Melakukan penelitian dengan mengembangkan sistem platform MCDM, studi kasus penentuan peminatan jurusan pada Program Studi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.

Demikian hal ini disampaikan, atas kerjasamanya kami ucapkan terima kasih.

Wassalamu'alaikum Warrahmatullahi Wabarrakatuh

Samarinda, 3 Muharram 1446 H
9 Juli 2024 M

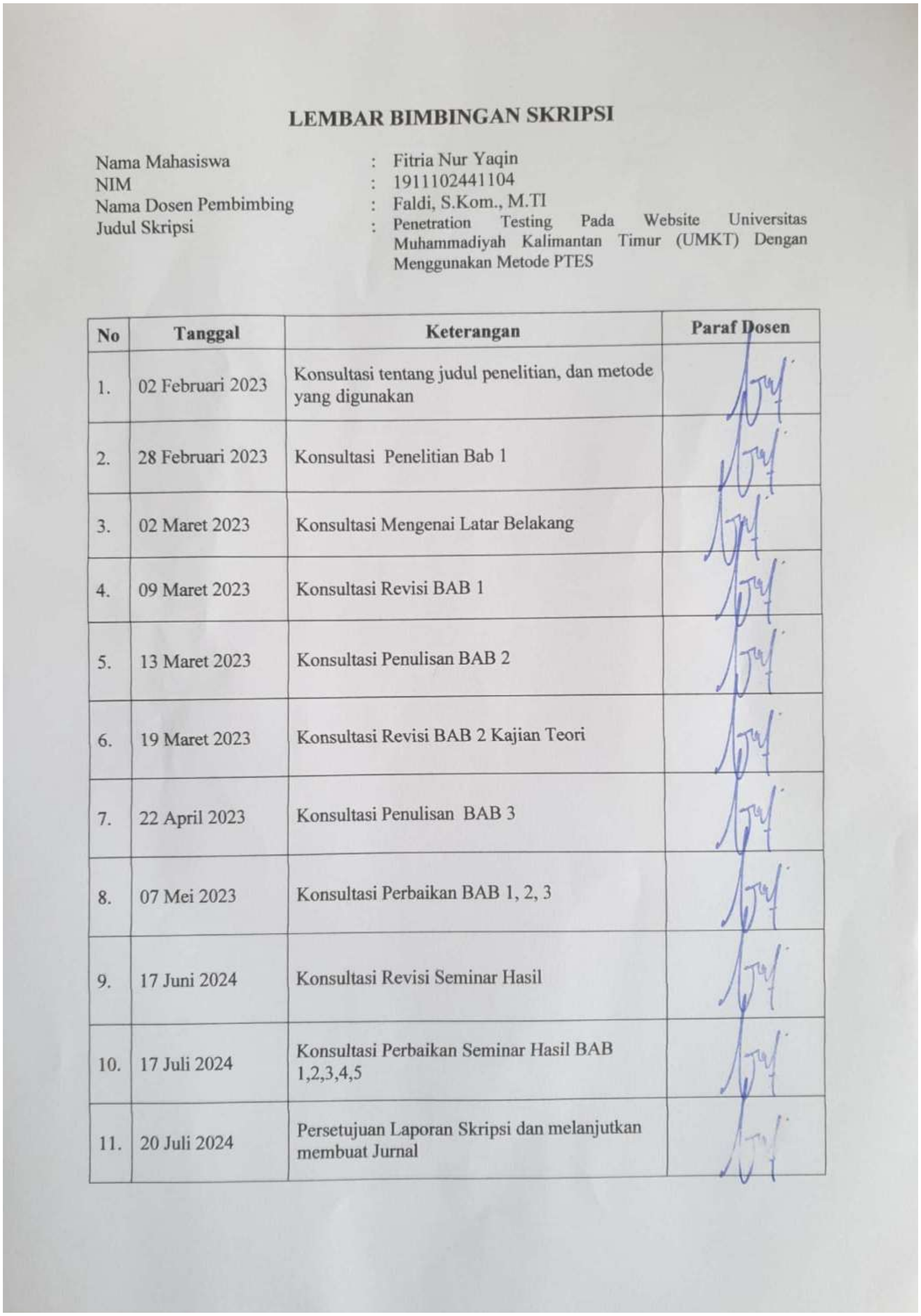
Ketua Program Studi S1 Teknik Informatika

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
PROGRAM STUDI INFORMATIKA

Arbansyah, S.Kom., M.TI
NIDN. 1118019203

Kampus 1 : Jl. Ir. H. Juanda, No.15, Samarinda
Kampus 2 : Jl. Pelita, Pesona Mahakam, Samarinda

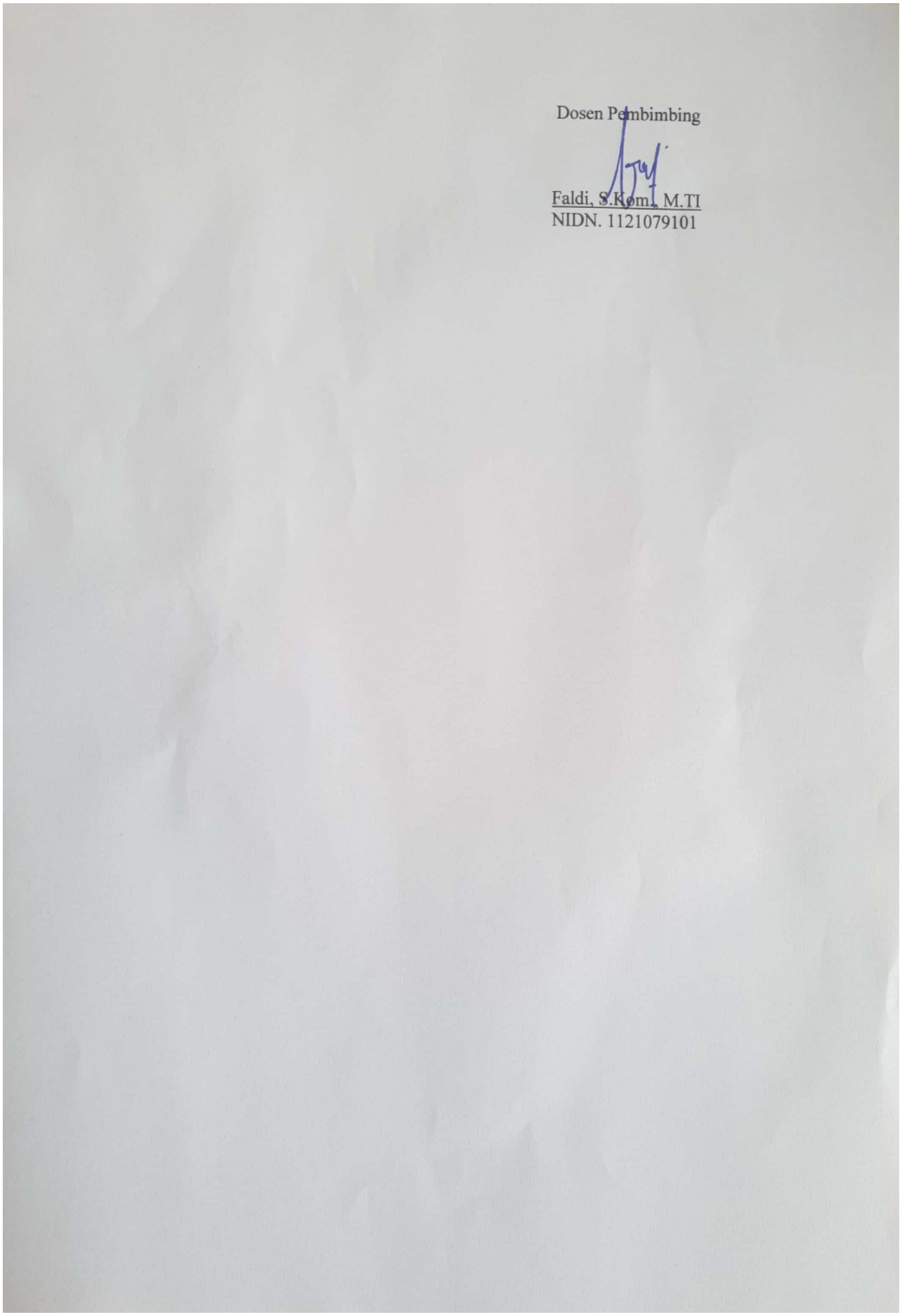
Lampiran 4 Bimbingan Skripsi



LEMBAR BIMBINGAN SKRIPSI

Nama Mahasiswa : Fitria Nur Yaqin
NIM : 1911102441104
Nama Dosen Pembimbing : Faldi, S.Kom., M.TI
Judul Skripsi : Penetration Testing Pada Website Universitas Muhammadiyah Kalimantan Timur (UMKT) Dengan Menggunakan Metode PTES

No	Tanggal	Keterangan	Paraf Dosen
1.	02 Februari 2023	Konsultasi tentang judul penelitian, dan metode yang digunakan	
2.	28 Februari 2023	Konsultasi Penelitian Bab 1	
3.	02 Maret 2023	Konsultasi Mengenai Latar Belakang	
4.	09 Maret 2023	Konsultasi Revisi BAB 1	
5.	13 Maret 2023	Konsultasi Penulisan BAB 2	
6.	19 Maret 2023	Konsultasi Revisi BAB 2 Kajian Teori	
7.	22 April 2023	Konsultasi Penulisan BAB 3	
8.	07 Mei 2023	Konsultasi Perbaikan BAB 1, 2, 3	
9.	17 Juni 2024	Konsultasi Revisi Seminar Hasil	
10.	17 Juli 2024	Konsultasi Perbaikan Seminar Hasil BAB 1,2,3,4,5	
11.	20 Juli 2024	Persetujuan Laporan Skripsi dan melanjutkan membuat Jurnal	



Dosen Pembimbing

Faldi, S.Kom., M.TI
NIDN. 1121079101