ANALISIS PENILAIAN KEAMANAN SERVER TERHADAP SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN METODE NIST SP 800-115 PADA UNIVERSITAS ISLAM NEGERI AR-RANIRY

TUGAS AKHIR

Diajukan Oleh:

Irfan Murti Raazi
NIM. 190705021
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI AR-RANIRY
BANDA ACEH
2023 M/1444 H

ANALISIS PENILAIAN KEAMANAN SERVER TERHADAP SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN METODE NIST SP 800-115 PADA UNIVERSITAS ISLAM NEGERI AR-RANIRY

TUGAS AKHIR

Diajukan Kepada Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana (S1)
dalam Prodi Teknologi Informasi

Oleh:
Irfan Murti Raazi
NIM. 190705021
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

Disetujui untuk Dimunaqasyahkan Oleh:

Pembimbing I,	**Pembimbing II,**
Malahayati, M.T	**Mulkan Fadhli, S.T., M.T**
NIP. 198301272015032003	**NIP. 198811282020121006**

Mengetahui,
Ketua Program Studi Teknologi Informasi

Ima Dwitawati, M.B.A
NIP. 198210132014032002

ANALISIS PENILAIAN KEAMANAN SERVER TERHADAP SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN METODE NIST SP 800-115 PADA UNIVERSITAS ISLAM NEGERI AR-RANIRY

TUGAS AKHIR

Telah Diuji Oleh Panitia Ujian Munaqasah Tugas Akhir
Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus
Serta Diterima Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
Dalam Prodi Teknologi Informasi

Pada Hari/Tanggal: Senin, 20 Maret 2023
27 Sya'ban 1444 H
di Darussalam, Banda Aceh

Panitia Ujian Munaqasah Tugas Akhir

Ketua,	**Sekretaris,**
Malahayati, M.T	**Mulkan Fadhli, S.T., M.T**
NIP. 198301272015032003	**NIP. 198811282020121006**
Penguji I,	**Penguji II,**
Ghufran Ibnu Yasa, M.T	**Hendri Ahmadian, S.Si., M.I.M**
NIP. 198409262014031005	**NIP. 198301042014031002**

Mengetahui:
Dekan Fakultas Sains dan Teknologi
UIN Ar-Raniry Banda Aceh,

Dr. Ir. Muhammad Dirhamsyah, M.T., IPU
NIP. 196210021988111001

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	: Irfan Murti Raazi
NIM	: 190705021
Program Studi	: Teknologi Informasi
Fakultas	: Sains dan Teknologi
Judul	: Analisis Penilaian Keamanan Server terhadap Sistem Informasi Manajemen Kepegawaian dengan Metode NIST SP 800-115 pada Universitas Islam Negeri Ar-Raniry

Dengan ini menyatakan bahwa dalam penulisan tugas akhir, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;
4. Tidak memanipulasi dan memalsukan data;
5. Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh.

Demikian pernyataan ini saya buat dengan sesungguhnya dan tanpa paksaan dari pihak manapun.

Banda Aceh, 30 Januari 2023

Yang Menyatakan,

Irfan Murti Raazi

ABSTRAK

Nama	: Irfan Murti Raazi
NIM	: 190705021
Program Studi	: Teknologi Informasi
Judul	: Analisis Penilaian Keamanan Server terhadap Sistem Informasi Manajemen Kepegawaian dengan Metode NIST SP 800-115 pada Universitas Islam Negeri Ar-Raniry
Tanggal Sidang	: 20 Maret 2023
Jumlah Halaman	: 86 Halaman
Pembimbing I	: Malahayati, M.T
Pembimbing II	: Mulkan Fadhli, S.T., M.T
Kata Kunci	: *Cybercrime*, *Penetration Testing*, NIST SP 800-115, Keamanan Server

Tindak kejahatan dunia maya terus berkembang seiring dengan meningkatnya kemampuan manusia dalam menggunakan teknologi digital, hal ini dapat memicu terjadi penyalahgunaan teknologi digital sebagai alat utama tindak kejahatan. Oleh karena itu, keamanan sistem menjadi prioritas utama dalam suatu instansi agar terhindari dari berbagai teknik ancaman dalam pencurian data dan informasi pada sebuah komputer server oleh pihak yang tidak memiliki otoritas. Universitas Islam Negeri Ar-Raniry merupakan suatu instansi yang telah memanfaatkan teknologi informasi dalam tata kelola universitas, salah satunya yaitu server yang memuat Sistem Informasi Manajemen Kepegawaian. Dalam hal ini, dengan terpublikasi sistem informasi tersebut ke dunia internet sehingga membuat rawan terjadinya serangan yang disebabkan oleh kerentanan (*vulnerability*). Penelitian ini dapat menjadi tolak ukur sejauh mana instansi yang dievaluasi untuk dapat melakukan perbaikan terhadap kerentanan yang telah ditemukan guna meminimalisir tindak kejahatan dalam memperoleh akses kewenangan sistem tersebut. Sehingga perlu dilakukan *penetration testing* untuk menilai kelayakan server berdasarkan aspek keamanan informasi yaitu: *confidentiality*, *integrity*, dan *availability*. Salah satu

cara mengatasi terjadinya serangan yaitu dengan menutup kerentanan yang terdapat pada suatu sistem. Namun, sebelum menutup suatu kerentanan tersebut, diperlukan penilaian keamanan untuk menanggulangi terjadinya tindak kejahatan dengan prosedur yang telah disepakati. Penilaian keamanan server dilakukan dengan menggunakan metode NIST SP 800-115 yang terdiri dari 4 tahapan pengujian, yaitu: *planning*, *discovery*, *attack*, dan *reporting*. Hasil dari penelitian ini adalah dapat diketahui bahwa Sistem informasi Manajemen Kepegawaian memiliki 9 kerentanan yang dapat dieksploitasi dengan rincian 2 kerentanan yang berada dalam *threat level high* yaitu: DNS Server *Spoofed Request Amplification* DDoS, dan *Interception Attack*, dan 7 kerentanan yang berada dalam *threat level medium* yaitu: TLS *Version* 1.0 *Protocol Detection*, TLS *Version* 1.1 *Protocol Detection*, SSL *Certificate Cannot Be Trusted*, SSL *Certificate Expiry*, SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure*, Nginx < 1.17.7 *Information Disclosure,* DNS Server *Recursive Query Cache Poisoning Weakness*. Dengan demikian, tingkat keparahan kerentanan server yang memuat sistem informasi tersebut berada pada skor 6.4 yang tergolong ke dalam *threat level medium*.

Kata kunci: *Cybercrime*, *Penetration Testing*, NIST SP 800-115, Keamanan Server

ABSTRACT

Name	: Irfan Murti Raazi
Student Number	: 190705021
Department	: Information Technology
Title	: Analysis Server Security Assessment of Staffing Management Information Systems Using the NIST SP 800-115 Method at Ar-Raniry State Islamic University
Date	: 20 March 2023
Thesis Pages	: 86 Pages
Supervisor I	: Malahayati, M.T
Supervisor II	: Mulkan Fadhli, S.T., M.T
Keywords	: *Cybercrime*, *Penetration Testing*, NIST SP 800-115, Server Security

Cyber crime continues to develop along with the increasing human ability to use digital technology, this can trigger the misuse of digital technology as the main tool for crime. Therefore, system security is a top priority in an institution to avoid various threat techniques in stealing data and information on a server computer by unauthorized parties. Ar-Raniry State Islamic University is an institution that has utilized information technology in university governance, one of which is a server that contains a Staffing Management Information System. In this case, the publication of information system to the internet makes it prone to attacks caused by vulnerabilities. This research can be a benchmark to what extent the institution being evaluated is able to make improvements to the vulnerabilities that have been found in order to minimize crime in gaining access to the authority of the system. So it is necessary to do penetration testing to assess the feasibility of the server based on aspects of information security, namely: confidentiality, integrity, and availability. One way to deal with an attack is to close the vulnerability in a system. However, before closing a vulnerability, a security assessment is needed to overcome the occurrence of crimes with agreed procedures. Server security assessment is carried out using the NIST SP 800-115 method which consists of 4

testing stages, namely: planning, discovery, attack, and reporting. The results of this study show that the Staffing Management Information System has 9 vulnerabilities that can be exploited with details of 2 vulnerabilities that are at a higt level threat, namely: DNS Server Spoofed Request Amplification DDoS, and Interception Attack, and 7 vulnerabilities that are at a medium level threat. namely: TLS Version 1.0 Protocol Detection, TLS Version 1.1 Protocol Detection, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSL/TLS Protocol Initialization Vector Implementation Information Disclosure, Nginx < 1.17.7 Information Disclosure, DNS Server Recursive Query Cache Poisoning Weakness. Thus, the vulnerability level of the server that contains system information is at a score of 6.4 which is classified as a medium threat level.

Keywords: Cyber Crime; Penetration Testing; NIST SP 800-115; Server Security

KATA PENGANTAR

Bismillahirrahmanirrahim.

Puji dan syukur kehadiran Allah SWT yang telah memberikan rahmat serta hidayah-Nya, Sang Maha kehendak sehingga peneliti dapat menyelesaikan tugas akhir ini. Shalawat serta salam semoga selalu tercurahkan kepada suri tauladan kita, Rasulullah Muhammad SAW yang telah membawa kita dari zaman jahiliyah menuju ke zaman terang benderang.

Peneliti sangat menyadari tugas akhir ini masih jauh dari kata sempurna. Namun demikian, peneliti berharap tugas akhir ini dapat memenuhi persyaratan guna memperoleh gelar Strata Satu (S1) dalam prodi Teknologi Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry Banda Aceh.

Tugas akhir yang berjudul "**Analisis Penilaian Keamanan Server terhadap Sistem Informasi Manajemen Kepegawaian dengan Metode NIST SP 800-115 pada Universitas Islam Negeri Ar-Raniry**", akhirnya dapat diselesaikan sesuai dengan harapan peneliti. Selama penyusunan tugas akhir ini tentunya ada banyak kesulitan dan hambatan yang peneliti hadapi, baik dalam pengumpulan data dan lain sebagainya. Namun berkat kesungguhan hati dan bantuan dari berbagai pihak, sehingga kesulitan tersebut dapat diatasi.

Pada kesempatan ini peneliti juga hendak mengucapkan terima kasih kepada pihak-pihak yang telah membantu memberikan dukungan, bimbingan, bantuan kepada saya selama melakukan penelitian tugas akhir dan proses penyelesaian tugas akhir ini. Secara khusus saya ucapkan terima kasih kepada:

1. Orang tua tersayang, Ayahanda Alm. Murthada AB dan Ibunda Puji Yanti yang telah mendidik, menyayangi, memberikan dukungan, semangat dan doa restu.
2. Ibu Ima Dwitawati, M.B.A selaku Ketua Program Studi Teknologi Informasi untuk segala dukungan dan motivasinya selama proses mengerjakan tugas akhir.
3. Bapak Khairan AR, M.Kom selaku Sekretaris Program Studi Teknologi Informasi untuk dukungannya selama proses mengerjakan tugas akhir.

4. Ibu Malahayati, M.T selaku Dosen Pembimbing I yang secara disiplin serta kooperatif telah memberikan ilmu dan membimbing peneliti dengan sabar serta membantu secara teknis dan non teknis dalam penyusunan tugas akhir ini.
5. Bapak Mulkan Fadhli, S.T., M.T selaku Dosen Pembimbing II yang banyak membantu serta memberikan dukungan ilmu dan secara teknis dan non teknis dalam penyusunan tugas akhir ini.
6. Bapak Lutfi selaku staff ICT Universitas Islam Negeri Ar-Raniry Banda Aceh yang telah memberikan dukungan kepada peneliti melaksanakan penelitian.
7. Ibu Sri Wahyuni, M.T selaku Pembimbing Akademik yang selalu memberikan bimbingan dan motivasi selama berada dibangku perkuliahan.
8. Bapak Bustami, M.Sc selaku Ketua Laboratorium Program Studi Teknologi Informasi untuk segala dukungan dan motivasinya.
9. Seluruh dosen Program Studi Teknologi yang telah memberikan ilmu selama peneliti duduk di bangku perkuliahan.
10. Ibu Cut Ida Rahmadiana, S.Si selaku staff Program Studi Teknologi Informasi yang telah membantu administrasi perkuliahan serta masukan dan motivasi kepada peneliti.
11. Terima kasih kepada Putri Nabila, Novi Ayu Irhami, Said Mahaqil Muhammad selaku sahabat peneliti yang selalu mendukung peneliti sehingga dapat menyelesaikan tugas akhir ini.
12. Terima kasih kepada kakak dan adik-adik tingkat serta teman-teman seperjuangan Program Studi Teknologi Informasi yang selalu mendukung dan menyemangati peneliti selama berkuliah dan dalam penyusunan tugas akhir.

Terima kasih atas segala bantuan dari semua pihak, peneliti mendoakan semoga Allah SWT membalas semua kebaikan yang telah diberikan oleh semua pihak dan semoga tugas akhir ini dapat bermanfaat bagi para pembaca serta berguna perkembangan penelitian lainnya di masa mendatang.

Banda Aceh, 30 Januari 2023
Peneliti,

Irfan Murti Raazi

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

I.1 Latar Belakang

Di era teknologi yang kian maju dan berkembang luas seperti sekarang ini, intensitas penggunaan teknologi komputer menjadi bagian yang tidak terpisahkan dari kehidupan manusia (Astriani dkk., 2021). Oleh karenanya kemampuan dan rasa keingintahuan manusia dalam menggunakan teknologi digital pun semakin meningkat. Namun, sejalan dengan perkembangan teknologi informasi juga munculnya beragam jenis kejahatan dunia maya (*cybercrime*), yang berkaitan dengan permasalahan sistem keamanan jaringan, dan informasi sebagai aset dalam penerapan kehandalan keamanan jaringan.

Informasi merupakan bagian terpenting pada sistem informasi sebuah instansi/organisasi. Hal ini berawal dari keandalan keamanan jaringan untuk menjaga validitas dan integritas data serta menjamin ketersedian layanan bagi pengguna (Sanjaya dkk., 2020). Sehingga dapat mencegah keandalan dari pihak yang tidak bertanggung jawab dalam mengimplementasikan teknik-teknik ancaman dan serangan untuk mencapai tujuan tertentu.

Dalam keamanan informasi mempunyai beberapa aspek yang harus dipahami dan dilindungi. Aspek keamanan informasi antara lain *confidentiality*, *integrity*, dan *availability* (Rochmadi & Pasa, 2021). Sehingga keamanan sistem menjadi prioritas utama dalam suatu instansi/organisasi agar terhindar dari berbagai macam teknik serangan dan pencurian informasi, seperti peretasan pada sistem server.

Berdasarkan informasi dari portal berita *British Broadcasting Corporation* (BBC) menyatakan bahwa tindak *cybercrime* pada tahun 2020 telah terjadi serangan siber yang menyerang *University of* California, San Francisco pada tanggal 1 Juni 2020. Para peretas anonim yang melakukan serangan siber *ransomware* pada server universitas dan menemukan data penting dari Fakultas Kedokteran tentang penelitian Covid-19. Peretas meminta tebusan sebesar US$ 3 Juta untuk memberikan kunci dekripsi, karena peretas berhasil enkripsi tujuh server

milik universitas sehingga pihak universitas melakukan negosiasi tembusan menjadi sebesar US$1,14 juta (Tidy J, 2020).

Kasus tersebut membuktikan bahwa kumpulan data penting terhimpun dalam sebuah server instansi/organisasi yang dapat diserang dan diakses oleh pihak yang tidak memiliki *authority*. Oleh karena itu, diperlukan perlindungan informasi dengan menerapkan pendekatan secara terstruktur guna menghindari terjadinya resiko yang mungkin timbul.

Pemilihan analisa keamanan sistem dilakukan karena *cybercrime* dapat terjadi kapanpun dan dimanapun khususnya pada universitas yang mengabaikan sistem keamanan serta menganggap tingkat keamanan sistem telah aman. Dalam hal ini, untuk mengatasi terjadinya peretasan pada sistem server yaitu dengan menutup kerentanan yang terdapat pada sistem tersebut. Namun, sebelum menutup suatu kerentanan maka diperlukan penilaian terhadap keamanan server yang ada.

Berdasarkan uraian di atas, peneliti berinisiatif untuk melakukan penelitian penilaian keamanan server terhadap Sistem Informasi Manajemen Kepegawaian yang berada di server Universitas Islam Negeri Ar-Raniry guna mengetahui tingkat kerentanan terhadap keamanan server universitas serta membantu meminimalisir dari tindak kejahatan. Adapun salah satu kegiatan yang dilakukan dengan *vulnerability scanning* pada target dan melakukan *penetration testing* menggunakan metode *National Institute of Standards and Technology* (NIST SP 800-115) dengan studi kasus pada Universitas Islam Negeri Ar-Raniry sebagai target dalam melakukan analisis penilaian keamanan server. Pengujian ini dilakukan melalui *open port*s dan *service* yang berjalan pada *port* tersebut.

Pemilihan metode NIST SP 800-115 sebagai tahapan dalam melakukan penilaian keamanan terhadap server dikarenakan memiliki tahapan, *tools* serta teknik yang jelas dan mudah untuk diimplementasikan dalam proses pengujian keamanan dan memberikan rekomendasi perbaikan kerentanan. Penilaian dalam metode ini menggunakan *Common Vulnerability Scoring System* (CVSS) yang mudah dimengerti oleh pengguna meskipun tidak berpengalaman di bidang *penetration testing*.

I.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka peneliti merumuskan permasalahan yang sudah dijelaskan terdapat beberapa rumusan masalah, antara lain:

1. Bagaimana cara menguji penilaian keamanan server terhadap Sistem Informasi Manajemen Kepegawaian pada studi kasus Universitas Islam Negeri Ar-Raniry?
2. Apa saja jenis kerentanan server yang mengakibatkan kegagalan keamanan sistem informasi menggunakan metode NIST SP 800-115?
3. Bagaimana cara rekomendasi perbaikan kerentanan yang didapatkan pada server Universitas Islam Negeri Ar-Raniry?

I.3 Batasan Masalah

Dalam peneliti ini agar menjadi lebih terarah serta mengurangi adanya penyimpangan dari yang telah peneliti uraikan berdasarkan pada latar belakang, maka peneliti membatasi masalah terhadap masalah penelitian yang dilakukan, yaitu:

1. Pengujian pada server *running* terhadap Sistem Informasi Manajemen Kepegawaian Universitas Islam Negeri Ar-Raniry.
2. Pengujian pada penelitian dilakukan di luar jam kerja guna meminimalisir *traffic* jaringan.
3. Penelitian ini dilakukan dengan menggunakan Sistem Operasi Linux, distro Kali Linux untuk pengujian serta beberapa *tools* ping, whois, sslscan, nmap, nessus, metasploit, dan wireshark.
4. Penilaian keamanan di dalam penelitian ini mengacu pada *penetration testing* dalam metode NIST SP 800-115 lalu kerentanan tersebut dianalisis melalui kalkulator berbasis web CVSS v3.0.
5. Pengujian server tidak mengganggu kinerja dari Universitas Islam Negeri Ar-Raniry.
6. *Internet Protocol* (*IP*) *Address* yang digunakan dalam penelitian tidak dipublikasi untuk menjaga keamanan sistem universitas.
7. Pengujian tidak menerapkan *Social Engineering*.

I.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas, maka tujuan dari penelitian ini, yaitu:

1. Pengujian yang dilakukan untuk mengetahui kondisi dari tingkat kerentanan terhadap server Universitas Islam Negeri Ar-Raniry.
2. Dengan diketahui kerentanan dapat mengurangi kemungkinan *cybercrime* yang mungkin terjadi akibat penyalahgunaan informasi yang ada di Universitas Islam Negeri Ar-Raniry.
3. Memperoleh kerentanan server Universitas Islam Negeri Ar-Raniry agar mendapat penanganan lebih lanjut untuk dioptimalkan sistem keamanan server tersebut.

I.5 Manfaat Penelitian

Manfaat dari hasil penelitian ini diharapkan dapat memberikan memberikan kontribusi kepada beberapa pihak, antara lain:

1. Bagi universitas, Penelitian ini diharapkan dapat membantu Universitas Islam Negeri Ar-Raniry untuk mengetahui kerentanan server sistem informasi yang ada. Kemudian mencegah terjadinya tindak *cybercrime* yang dapat merusak sistem server. Dan sebagai bahan evaluasi dalam meningkatkan keamanan sistem informasi yang ada baik berupa web maupun server, serta dapat menjadi bahan rujukan untuk penelitian keamanan sistem di masa mendatang.
2. Bagi peneliti, memenuhi salah satu syarat kelulusan Sarjana Strata Satu (S1) Teknologi Informasi Fakultas Sains dan Teknologi UIN Ar-Raniry, dan menambah pengetahuan dan pemahaman mengenai ilmu *cyber security* dalam bidang analisis penilaian keamanan server.
3. Bagi pembaca, penelitian ini diharapkan dapat memberikan informasi yang bermanfaat mengenai keilmuan di bidang Teknologi Informasi dan wawasan tentang penilaian keamanan server, serta dapat menjadi bahan rujukan untuk penelitian lebih lanjut di masa mendatang.

BAB II
TINJAUAN PUSTAKA

II.1 Penelitian Terdahulu

Penelitian terdahulu adalah mendeskripsikan tentang hasil penelitian yang sudah dilakukan sebelumnya seputar dengan masalah yang diteliti. Selain itu, penelitian terdahulu dapat menjelaskan penelitian dengan cara mendeskripsikan persamaan atau perbedaan yang telah dilakukan sebelumnya dengan memberikan hasil suatu penemuan baru atau diperbarui dengan berbagai metode. Berikut ini beberapa hasil penelitian terdahulu yang relevan untuk menjadi bahan telaah bagi peneliti, diantaranya:

Pertama, penelitian yang dilakukan Fahmi Fachri dkk, yang berjudul "Analisis Keamanan Web Server Menggunakan *Penetration Test*". Tujuan penelitian ini adalah untuk menguji kelemahan dan kerentanan pada web server sistem informasi akademik di perguruan tinggi. Studi kasus ini dilakukan akibat terjadi permasalahan *hacking system*, mengubah file index dengan meng-*inject file backdoor* ke dalam sistem yang menyebabkan web Sistem Informasi Akademik (SIA) tidak dapat berjalan sebagaimana mestinya. Dengan melakukan *penetration testing* pada web server terbukti ditemukan kerentanan. Hasil pengujian ditemukan beberapa *port* serta penyerangan sistem dilakukan pada *port* 22 (SSH) yang menyebabkan berhasil mendapatkan *username* dan *password* sehingga peretas dengan mudah masuk untuk mengeksploitasi informasi pada target uji (Fachri dkk., 2021).

Kedua, penelitian yang dilakukan oleh Muhammad Subagja Sastra Wardaya, yang berjudul "*Penetration Testing* terhadap Website Asosiasi Pekerja Profesional Informasi Sekolah Indonesia (APISI)". Pada penelitian ini dilakukan untuk mencari celah keamanan serta tingkat kerentanannya diukur menggunakan *Common Vulnerability Scoring System* (CVSS). Dalam hal keamanannya pernah terjadinya serangan siber yang menyebabkan kegagalan aspek keamanan informasi. Hasil pengujian kerentanan dan analisis ditemukan 41 kerentanan yang secara keseluruhan berada di angka 6.6 dengan kategori *medium* (Wardaya, 2019).

Ketiga, penelitian yang dilakukan oleh Wasis Wardana dkk, yang berjudul "*Vulnerability Assessment and Penetration Testing on the* XYZ *Website Using* NIST 800-115 *Standard*". *Tools* pengujian yang digunakan Nmap, OWASP ZAP, dan Burp Suite dalam menganalisis celah keamanan situs XYZ serta melakukan pengujian penetrasi sehingga memperoleh 7 kerentanan. Hasil pengujian ditemukan kerentanan 1 kategori *high* Sql *Injection*, 2 kategori *medium Cross-Domain Misconfiguration*, dan *Vulnerable JS Library*, dan kategori 4 *low Absence of Anti-CSRF Tokens, Incomplete or No Cache-control and Pragma HTTP Header Set, Server Leaks Information via "X-Powered-By" HTTP Response Header* Field, dan *X-Content-Type-Options Header Missing.* Dengan demikian, penemuan hasil kerentanan menunjukkan bahwa metode yang digunakan dapat melakukan *penetration testing* dengan beberapa tahapan serta memberikan rekomendasi, sehingga metode ini dapat dijadikan acuan untuk meningkatkan keamanan website agar terhindar dari serangan (Wardana dkk., 2022). Adapun ringkasan dari penelitian terdahulu yang dimuat dalam Tabel II.1.

Tabel II.1 Penelitian Terdahulu

No	Peneliti	Judul Penelitian	Hasil Penelitian	Persamaan Perbedaan
1	Fahmi Fachri dkk (2021)	Analisis Keamanan Web Server Menggunakan *Penetration Test*	Dengan ditemukan beberapa *open port* menyebabkan terjadinya penyerangan sistem pada *port* SSH yang berhasil mendapatkan *username* dan *password* sehingga dengan mudah masuk untuk mengeksploitasi Sistem Informasi Akademik (SIA). Hal ini pentingnya menjaga keamanan web server yang mana didalamnya terdapat data pribadi serta	**Persamaan** Persamaan penelitian ini terkait dengan sama halnya melakukan *penetration testing* pada server di perguruan tinggi. **Perbedaan** Perbedaan penelitian ini yaitu terdapat pada metode penelitian yang digunakan sehingga perolehan hasil penelitian berdasarkan teknik *black box testing* sebagai pendekatan dalam melakukan *penetration testing*

No	Peneliti	Judul Penelitian	Hasil Penelitian	Persamaan Perbedaan
			layanan informasi akademik.	dengan metode NIST 800-115; Objek penelitian dilakukan pada server yang memuat sistem informasi manajemen kepegawaian di perguruan tinggi; Penggunaan *tools* pengujian penetrasi; Dan terdapat pengukuran kerentanan menggunakan CVSS.
2	Muhammad Subagja Sastra Wardaya (2019)	*Penetration Testing* terhadap Website Asosiasi Pekerja Profesional Informasi Sekolah Indonesia (APISI)	Dengan ditemukan 41 kerentanan dari penelitian ini yang diukur tingkat kerentanannya menggunakan CVSS dapat dikategorikan *none*, *low*, *medium*, *high* dan *critical*. Kemudian juga menunjukkan vektor string dari temuan kerentanan serta dapat diketahui kerentanan berdasarkan aspek keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*.	**Persamaan** Persamaan penelitian ini terkait dengan sama halnya melakukan *penetration testing* dengan teknik *black box testing* pada sistem informasi; Dan pengukuran kerentanan menggunakan CVSS. **Perbedaan** Perbedaan penelitian ini yaitu terdapat pada metode penelitian dengan menggunakan NIST 800-115; Objek penelitian dilakukan pada server yang memuat sistem informasi di universitas; Dan penggunaan *tools* pengujian penetrasi.
3	Wasis Wardana, dkk (2022)	*Vulnerability Assessment and Penetration Testing on the*	Penggunaan metode NIST 800-115 sangat efektif yang mana di dalam metode	**Persamaan** Persamaan penelitian ini terkait dengan sama halnya melakukan

No	Peneliti	Judul Penelitian	Hasil Penelitian	Persamaan Perbedaan
		XYZ *Website Using* NIST 800-115 *Standard*	tersebut dapat melakukan *penetration testing* sehingga terbukti ditemukan 7 kerentanan dengan 1 kategori *high level*, 2 kategori *medium level*, dan 4 kategori *low level* serta mempunyai tahapan khusus dalam pemberian rekomendasi.	*penetration testing* berdasarkan acuan NIST 800-115 pada sistem informasi berbasis web. **Perbedaan** Perbedaan penelitian ini yaitu dengan menerapkan teknik *black box testing* sebagai pendekatan dalam melakukan *penetration testing* dalam metode NIST 800-115; objek penelitian dilakukan pada server yang memuat sistem informasi di universitas; Penggunaan *tools* pengujian penetrasi dalam menemukan kerentanan; Dan terdapat pengukuran kerentanan menggunakan CVSS.

Berdasarkan dari ketiga penelitian terdahulu tersebut, peneliti menyimpulkan bahwasanya kesamaan dan perbedaan penelitian terkait dengan penelitian ini yaitu; pertama berada pada objek dan tempat penelitian, dimana peneliti melakukan penilaian keamanan pada server yang memuat Sistem Informasi Manajemen Kepegawaian di Universitas Islam Negeri Ar-Raniry. Kedua, dari penelitian terdahulu pertama dan ketiga, hanya dibataskan pada perolehan tingkat kerentanan yang diketahui dari *tools* pengujian. Sehingga temuan kerentanan yang diperoleh belum dipastikan mengetahui apa saja kegagalan dari aspek keamanan informasi. Ketiga, penelitian terdahulu yang pertama dan kedua, hanya dibataskan pada tahap awal untuk menentukan *tools* pengujian. Sehingga tahapan yang digunakan sebatas *tools* yang telah direncanakan di awal untuk menyelesaikan *penetration testing*.

II.2 Kajian Teoritis

II.2.1 Sistem Informasi

Sistem informasi adalah suatu sistem yang mengintegrasikan kebutuhan pemrosesan tentang peristiwa penting baik internal maupun eksternal. Sistem informasi mempunyai komponen yang saling berhubungan dalam hal mengumpulkan, memproses, menyimpan dan mendistribusikan informasi guna mendukung kebutuhan organisasi. Salah satu komponen yang terdapat pada sistem informasi ialah *databases* yang kini sangat penting dalam hal penentuan kualitas informasi dan penyedian informasinya (Prasetio, 2017). Dengan demikian, sistem informasi akan digunakan sebagai penyimpanan data, perolehan informasi, memformat data serta layanan informasi *client/server*.

II.2.2 Sistem Informasi Manajemen Kepegawaian

Sistem Informasi Manajemen (SIM) adalah sistem terpadu yang menyediakan informasi dalam mendukung aktivitas operasional, manajemen, dan pengambilan keputusan dari suatu organisasi (Rusdiana, 2014). Sedangkan Sistem Informasi Manajemen Kepegawaian (SIMPEG) adalah suatu sistem yang bergerak dibidang kepegawaian pada suatu instansi/organisasi di dalamnya terhimpun pendataan pegawai, pengolahan data, prosedur, tata kerja, dan teknologi informasi untuk penyampaian informasi yang cepat dan akurat guna mendukung administrasi kepegawaian. SIMPEG diterapkan karena pemerintah perlu adanya penyelenggaraan dan pemeliharaan informasi kepegawaian dalam mendukung kebijakan manajemen Pegawai Negeri Sipil (PNS) terutama dalam hal mendukung kebijakan pembinaan PNS. Dengan adanya SIMPEG akan meliputi seluruh hierarki kepengurusan dalam suatu instansi/organisasi, dimulai dari hierarki manajemen tertinggi kepengurusan dengan tugas bertanggungjawab atas keberhasilan atau tidaknya organisasi hingga hierarki manajemen terendah dengan tugas menyelesaikan pekerjaan sehari-hari sesuai ruang lingkup departemen (Utami, 2017).

II.2.3 Keamanan Informasi

Informasi kini sangat mudah didapatkan dengan menggunakan berbagai macam jenis teknologi dari hasil perkembangan zaman sampai saat ini. Selain digunakan sebagai layanan untuk mendukung keakuratan informasi, teknologi juga harus memiliki keamanan yang baik. Hal ini diperlukan untuk melindungi informasi dari pihak yang tidak berwenang. Sedangkan keamanan informasi merupakan suatu kegiatan dalam mengamankan aset informasi suatu organisasi dari ancaman-ancaman yang mungkin dapat timbul. Dalam hal ini, dengan banyaknya informasi organisasi yang tersimpan pada suatu server dan dikelola maka semakin tinggi resiko terjadinya kerusakan, kehilangan ataupun terpublikasi informasi kepada pihak yang tidak bertanggung jawab (Ramadhani, 2018).

Keamanan informasi memiliki tiga prinsip utama dikenal sebagai CIA Triad yaitu *confidentiality*, *integrity*, dan *availability*. Ketiga prinsip tersebut merupakan landasan dari setiap program keamanan informasi yang dirancang dengan baik untuk menghindari berbagai serangan atau ancaman yang dapat terjadi pada sistem elektronik dapat dilihat pada Gambar II.1.

Gambar II.1 Prinsip Keamanan Informasi (Rochmadi & Pasa, 2021)

Confidentiality merupakan prinsip dalam memberikan jaminan terhadap kerahasian data atau informasi dengan menjaga kerahasiaan suatu informasi dari pihak yang tidak berwenang. Pada prinsip ini keamanan yang dilakukan berupa pengelolaan dari pembatasan hak terhadap informasi. Dimana *confidentily* mempunyai keterkaitan yang erat dengan *integrity*, karena jika integritas data dari objek terkontaminasi maka aspek kerahasiaan telah hilang (Ramadhani, 2018).

Integrity merupakan prinsip yang berhubungan dengan integritas suatu data dalam menjaga keaslian data dari aktivitas modifikasi tanpa adanya otorisasi. Dalam hal ini, penerapan *integrity* harus menangani segala aktivitas yang dapat menyebabkan terjadinya penambahan data, perubahan data, maupun penghapusan data *integrity* dalam waktu yang sama.

Availability merupakan prinsip yang dapat menyakinkan otorisasi dengan menyediakan informasi ber reliabilitas tinggi dari penggunaan sistem dengan tepat waktu dan akses tidak terinterupsi. Hal ini jika keamanan berhasil menjalankan *availability* suatu informasi yang tersedia harus memiliki izin dapat mengakses informasi dari berbagai sumber dengan menggunakan jalur yang aman. Dengan demikian, keamanan yang dapat dinilai dengan baik dilihat dari tiga penerapan prinsip yang digunakan untuk mencapai visi organisasi dalam mengamankan informasi yang berharga (Cardwell, 2016).

Dalam hal ini, terdapat masalah utama pada keamanan informasi yaitu (Guntoro dkk., 2020):

1. Ancaman (*Threats*)

   Ancaman adalah suatu tindakan yang dapat mengganggu keseimbangan sistem informasi dari segi dalam maupun luar sistem (Hanifah dkk., 2021). Oleh sebab itu, faktor yang mungkin dapat terjadi dari pengolahan informasi dapat berupa dari alam, manusia dan lingkungan. Namun, ancaman terhadap keamanan informasi berasal dari individu, organisasi, ataupun mekanisme yang menyebabkan kerusakan pada sumber informasi. Dimana ancaman tersebut dapat bersumber dari internal maupun eksternal yang semata-mata terjadi baik disengaja ataupun tidak disengaja.

2. Kerentanan (*Vulnerability*)

   Kerentanan adalah suatu celah keamanan yang muncul dalam suatu sistem pada saat mengimplementasikan kelemahan dari sistem kontrol yang dapat melanggar hak akses untuk mencoba menyusup ke dalam sistem tersebut (Baloch, 2017). Oleh karena itu, kerentanan dapat timbul yang diakibatkan oleh *cybercrime*. *Cybercrime* adalah suatu istilah yang memanfaatkan jaringan komputer dengan penyalahgunaan teknologi digital sebagai alat utama kejahatan (Wahyuni dkk., 2022).

Adapun tipe ancaman terhadap keamanan sistem komputer sebagai penyedia informasi dapat dikategorikan sebagai berikut (Kasau dkk., 2021):

1. Interupsi (*Interruption*)

   Interupsi adalah suatu ancaman yang berupaya untuk menghancurkan sumber daya dengan cara dirusak ataupun dihapus sehingga jika diperlukan suatu sumber informasi maka sudah tidak ada lagi. Ancaman ini terhadap syarat ketersedian. Misalkan kerusakan pada *hardware*, seperti hardisk yang tidak berfungsi, memutuskan kabel telekomunikasi.

2. Intersepsi (*Interception*)

   Intersepsi adalah suatu ancaman yang memiliki keterkaitan dengan kerahasiaan. Dimana pihak yang tidak berwenang dapat mengakses sumber daya baik berupa perorangan atau program komputer. Ancaman ini terhadap syarat kerahasian. Misalkan penyadapan, mengcopy file data tanpa izin.

3. Modifikasi (*Modification*)

   Modifikasi adalah suatu ancaman terhadap integritas yang dilakukan oleh pihak tak terotorisasi bukan hanya mengakses tetapi juga merusak sumber daya. Ancaman ini terhadap syarat integritas. Misalkan perubahan *value* pada data, perubahan pada program sehingga tidak sesuai dengan tujuan.

4. Fabrikasi (*Fabrication*)

   Fabrikasi adalah suatu ancaman yang dapat melakukan penyisipan atau memasukkan objek palsu ke dalam sistem hal ini berhubungan dengan integritas data yang dilakukan oleh pihak tak terotorisasi. Sehingga berhasil meniru atau memalsukan suatu informasi dari pihak pertama.

II.2.4 Keamanan Server

Server adalah komputer yang memberikan layanan kepada klien sehingga dibutuhkan spesifikasi yang lebih tinggi dan media penyimpanan yang besar. Namun, seiring berkembanganya penggunaan server ada faktor keamanan bagian yang perlu diperhitungkan secara serius untuk menghindari serangan dari berbagai pihak yang tidak berwenang. Adapun keamanan server ialah suatu kegiatan yang perlu diperhatikan secara mendetail pada saat melakukan konfigurasi server bertujuan untuk menghindari serangan dari pihak internal maupun eksternal yang

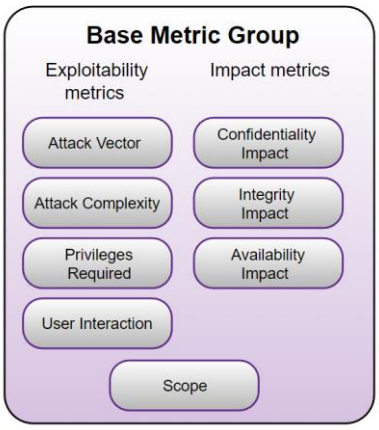
dapat membuat kerusakan fatal pada layanan server apabila terjadi serangan. Dengan demikian, dibutuhkan pengujian terhadap sistem keamanan server untuk dapat menemukan kerentanan-kerentanan yang ada didalamnya (Marta dkk., 2020).

II.2.5 *Vulnerability Assessment*

Vulnerability Assessment adalah suatu rangkaian proses yang dilakukan untuk mengidentifikasi, mengklasifikasi dan memprioritaskan kerentanan secara menyeluruh terkait keamanan informasi, *scanning*, konfigurasi pada sistem, cara mengelola serta akan kesadaran keamanan kepada pihak yang terlibat didalamnya dan mengetahui semua potensi kelemahan sistem yang ada. Dengan demikian, kegiatan *Vulnerability Assessment* harus dilakukan secara berkala atau terjadwal hal ini dikarena trend ancaman tindak kejahatan dunia maya akan terus berkembang sehingga diharuskan untuk mulai mengatasi kerentanan sedini mungkin untuk menjaga keamanan sistem informasi (Aziz, 2021). Jadi dapat disimpulkan bahwa kegiatan ini akan menemukan kerentanan terhadap sistem dan didokumentasikan sesuai dengan rangkaian penelitian ini dilakukan pencarian kerentanan pada Sistem Informasi Manajemen Kepegawaian yang berpotensi memiliki celah untuk dilakukan pelaporan kepada pihak terkait apabila terdapat celah.

II.2.6 *Common Vulnerability Scoring System*

Common Vulnerability Scoring System (CVSS) adalah suatu kegiatan untuk mendeskripsikan karakteristik dan tingkat keparahan kerentanan suatu sistem dalam mencakup teknis utama karakteristik *software, hardware,* dan *firmware*. Karakteristik kerentanan didapatkan dengan skor numerik yang mencerminkan tingkat keparahan kerentanan. CVSS berada di bawah *Forum of Incident Response and Security Teams* (*FIRST*) dengan tujuan untuk menanggapi insiden keamanan secara lebih efektif. Adapun *Base Matric Group* dapat dilihat pada Gambar II.2.



Gambar II.2 *Base Metrics Group* (FIRST, 2019)

Base metrics mempunyai karakteristik nilai kerentanan yang tetap di seluruh lingkungan pengguna. *Matrics* ini terdiri dua set yaitu (FIRST, 2019):

A. *Exploitability Metrics*

Metrics yang mencerminkan teknis kerentanan dapat dieksploitasi sehingga disebut sebagai komponen yang rentan.

1. *Attack Vector* (AV)

   AV adalah kerentanan yang dapat membuat eksploitasi terjadi. *Metrics* ini akan membuat *base score* lebih besar karena penyerang dapat mengeksploitasi kompen rentan. Dengan demikian, kemampuan yang dimiliki penyerang di seluruh jaringan lebih besar daripada mengeksploitasi kerentanan yang memerlukan akses fisik ke perangkat sehingga AV menjamin skor lebih besar. Adapun pada *Attack Vector* (AV) mempunyai *metrics value* yaitu:

   a. *Network* (N)

      Komponen yang berada di jaringan dan mengatur kemungkinan penyerang melakukan berbagai aktivitas. Hal ini dianggap sebagai serangan yang dapat dieksploitasi lebih dari satu protokol seperti melintasi satu router. Contohnya penyerang yang membuat penolakan layanan *Denial of Service* (DoS) dengan mengirim paket *Transmission Control Protocol* (TCP).

   b. *Adjacent* (A)

      Komponen yang berada di jaringan, nanun serangan terbatas pada tingkat protokol ke topologi. Hal ini harus meluncurkan serangan dari jaringan fisik.

Contohnya serangan yang berdekatan *Address Resolution Protocol* (ARP) *Flooding* (IPv4).

c. *Local* (L)

Komponen yang tidak bergantung langsung ke jaringan namun yang digunakan dalam menyerang adalah kemampuan *read/write/execute*. Contohnya dapat mengontrol sistem target secara local seperti keyboard, konsol atau jarak jauh *Secure Shell* (SSH) atau juga penggunaan *social engineering* dengan mengelabui target untuk memperoleh akses.

d. *Physical* (P)

Komponen serangan yang membutuhkan menyentuh secara fisik atau memanipulasi komponen yang rentan. Interaksi fisik dimungkinkan singkat misalkan menggunakan *Universal Serial Bus* (USB) yang telah dimodifikasi untuk membaca sistem target.

2. *Attack Complexity* (AC)

AC adalah kondisi yang membuat penyerang harus mengeksploitasi kerentanan untuk pengumpulan informasi tentang target. Adapun pada *Attack Complexity* (AC) mempunyai *metrics value* yaitu:

a. *Low* (L)

Tidak mempunyai kondisi akses khusus dalam melakukan eksploitasi berulang terhadap komponen yang rentan ini. Misalkan langsung menemukan kerentanan sql *injection*.

b. *High* (H)

Kondisi yang dimungkinkan berhasil dengan cara harus menjalankan segala upaya yang terukur dalam melakukan serangan terhadap komponen yang rentan. Misalkan *Man in the Middle Attack*.

3. *Privileges Required* (PR)

PR adalah tingkat hak istimewa yang dimiliki penyerang sebelum berhasil mengeksploitasi kerentanan sehingga membuat *base score* menjadi lebih besar jika tidak ada *privileges* yang dibutuhkan. Adapun pada *Privileges Required* (PR) mempunyai *metrics value* yaitu:

a. *None* (N)

Penyerang tidak mempunyai otorisasi sebelum terjadi serangan sehingga tidak membutuhkan akses ke sistem yang rentan untuk melakukan serangan. Misalkan kerentanan *Cross Site Scripting* (XSS) yang bisa dieksekusi tanpa harus login.

b. *Low* (L)

Penyerang memerlukan privileges rendah untuk informasi dasar yang tidak sensitif dimiliki pengguna ketika eksploitasi berhasil. Misalkan kerentanan XSS dengan ditemukan fitur edit profile user.

c. *High* (H)

Penyerang memerlukan privileges tinggi untuk memberikan kontrol yang dimiliki signifikan terhadap komponen rentan sehingga berhasil mendapatkan seluruh akses. Misalkan terdapat fitur upload yang seharusnya diakses dengan user level admin bukan user level dibawahnya.

4. *User Interaction* (UI)

UI adalah komponen pengguna selain penyerang yang memerlukan interaksi atau tidak untuk mengeksploitasi kerentanan. Sehingga *base score* akan lebih besar ketika tidak ada interaksi pengguna. Adapun pada *User Interaction* (*UI*) mempunyai *metrics value* yaitu:

a. *None* (N)

Dapat dieksploitasi tanpa adanya interaksi dari pengguna lain. Misalkan kesalahan konfigurasi pada sistem firewall.

b. *Required* (R)

Dapat dieksploitasi ketika adanya interaksi dari pengguna lain. Misalkan dengan menerapkan teknik *social engineering*.

5. *Scope* (S)

S adalah mengetahui kerentanan yang berdampak apakah ada terjadi perubahan di dalam cakupan keamanan. Misalkan pada aplikasi seperti *database* yang memiliki otoritas dalam mengontrol basis data. Adapun pada *Scope* (*S*) mempunyai *metrics value* yaitu:

a. *Unchanged* (U)

Kerentanan yang terdampak tidak berubah ketika eksploitasi berhasil sehingga tetap dikelola oleh otoritas keamanan yang sama. Misalkan *Distributed Denial of Service* (DDoS) pada sebuah aplikasi sehingga dampak yang terjadi pada aplikasi target.

b. *Changed* (C)

Kerentanan yang terdampak ikut berubah ketika eksploitasi berhasil. Misalkan serangan XSS berubah sehingga dampaknya juga terjadi di browser pengguna.

B. *Impact Metrics*

Metrics yang menjelaskan dampak dari eksploitasi yang sudah dilakukan pada komponen yang rentan.

1. *Confidentiality* (C)

   C adalah menyangkut pada akses informasi dan pengungkapan khusus kepada pihak yang terotorisasi (kerahasiaan suatu informasi). Adapun pada *Confidentiality* (*C*) mempunyai *metrics value* yaitu:

   a. *None* (N)

   Tidak ada data yang diketahui oleh pihak tak terotorisasi dari dampak kerentanan. Misalkan penemuan *Directory Listing* hanya berisi file static seperti gambar dan javascript.

   b. *Low* (L)

   Terdapat beberapa data yang terekspos namun tidak memiliki akses kontrol data yang terdampak. Misalkan celah *Insecure Direct Object Reference* (IDOR) yang terjadi pada *browser*.

   c. *High* (H)

   Banyaknya kehilangan kerahasian data yang serius atau akan sangat berdampak langsung sehingga membuat penyerang dapat akses kontrol. Misalkan *password administrator* server web.

2. *Integrity* (I)

   I adalah menyangkut pada integritas data yang berhasil dieksploitasi sehingga *base score* akan lebih besar ketika komponennya terdampak. Adapun pada *Integrity* (I) mempunyai *metrics value* yaitu:

   a. *None* (N)

      Penyerang tidak dapat melakukan modifikasi data dari hasil eksploitasi. Misalkan serangan DDoS.

   b. *Low* (L)

      Dapat melakukan modifikasi sebagian data yang terdampak. Namun, data yang terdampak tidak begitu serius. Misalkan celah pada XSS yang dapat dimodifikasi pada bagian *filed* kerentanan sehingga pengguna akan mengakses atau melakukan aktivitas sesuai dengan website bawaannya.

   c. *High* (H)

      Penyerang berhasil melakukan modifikasi data tanpa batas sesuai keinginan sehingga data yang terdampak akan sangat berbahaya, misalkan celah pada *database* suatu aplikasi.

3. *Availability* (A)

   A adalah menyangkut pada ketersediaan komponen yang terkena dampak dari kerentanan yang berhasil dieksploitasi. Namun, dengan kehilangan ketersedian komponen seperti layanan jaringan yang terdampak mengakibatkan ketersediaan aksesibilitas sumber daya informasi disebab oleh serangan yang menghabiskan *bandwidth* jaringan hal ini akan ketersedian komponen akan terganggu. Dengan begitu, *base score* juga lebih besar ketika terdampak. Adapun pada *Availability* (A) mempunyai *metrics value* yaitu:

   a. *None* (N)

      Ketersediaan data tidak terkena dampak dari komponen yang dieksploitasi. Misalkan temuan pada celah *directory listing* yang berisi data penting dari pengguna.

   b. *Low* (L)

      Terjadinya gangguan atau ketersediaan sumber daya berkurang yang jika dieksploitasi lebih lanjut tidak memiliki kemampuan sepenuhnya untuk meloak layanan kepada pengguna yang sah. Hal ini komponen yang terkena

dampak hanya sebagian tidak sepenuhnya tersedia sehingga tidak ada konsekuensi serius bagi komponen yang terkena dampak. Misalkan celah pada *Hypertext Markup Language* (HTML) *injection* dengan membuat kode berbahaya lalu dikirimkan ke email.

c. *High* (H)

Penyerang berhasil membuat ketersedian layanan terganggu sehingga sepenuhnya akses ke sumber daya komponen terkena dampak. Misalkan celah *Remote Code Execution* (RCE) yang dapat meng-*inject command shell* pada web server. Berdasarkan peringkat kerentanan skor CVSS dapat dilihat pada Tabel II.2.

Tabel II.2 CVSS *Score*

No	*Threat Level*	CVSS *Score*
1	*None*	0.0
2	*Low*	0.1 – 3.9
3	*Medium*	4.0 – 6.9
4	*High*	7.0 - 8.9
5	*Critical*	9.0 – 10.0

Dalam persamaan skor CVSS didefinisikan akan pembulatan (*roundup*) angka terkecil (*minimum*) dengan ke 1 tempat desimal yang sama dengan atau lebih tinggi dari inputnya. Misalkan pembulatan (4.02) akan menjadi (4.1); dan pembulatan (4.00) menjadi 4.0 hal ini untuk memastikan hal yang konsisten terhadap *CVSS score* (FIRST, 2019). Dengan demikian, rumus *base score* bagian dari *Impact* dan *Exploitability* sesuai *Impact Sub-Score* (ISC). Didefinisikan sebagai berikut (FIRST, 2019):

Definisi *Base score*: (1)

If (*Impact sub score* <=0 *else*, 0)

Scope Unchange *Roundup* (*Minimum* [(*Impact* + *Exploitability*),10])

Scope Change *Roundup* (*Minimum* [1.08 × (*Impact* + *Exploitability*),10])

Definisi *Impact sub score* (ISC): (2)

Scope Unchange $6.42 \times ISC_{Base}$

Scope Change $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Perhitungan *Impact sub score*: (3)

$ISC_{Base} = 1 - [(1 - ImpactConf) \times (1 - ImpactInteg) \times (1 - ImpactAvail)]$

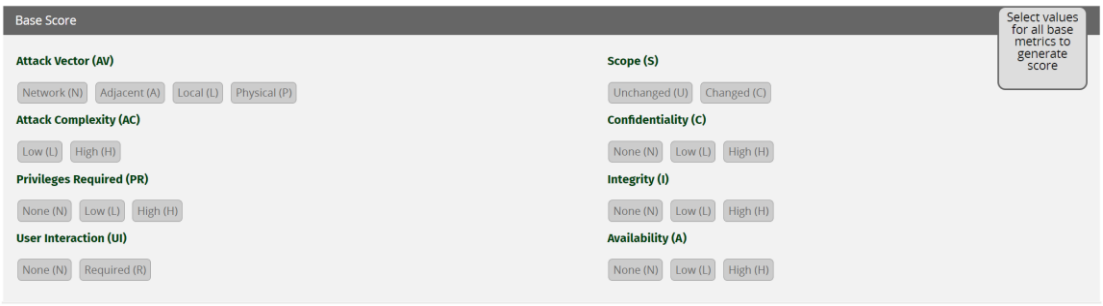
Perhitungan *Exploitability sub score*: (4)

$8.22 \times AttackVector \times AttackComplexity \times PrivilegesRequired \times UserInteraction$

Tabel II.3 Nilai Metrik

No	Metrics	Value Metrics	Numerical Value
1	*Attack Vector*	*Network*	0.85
		Adjacent	0.62
		Local	0.55
		Physical	0.2
2	*Attack Complexity*	*Low*	0.77
		High	0.44
3	*Privileges Required*	*None*	0.85
		Low	0.62 atau 0.68 jika *modified scope* di set *changed*
		High	0.27 atau 0.5 jika *modified scope* di set *changed*
4	*User Interaction*	*None*	0.85
		Required	0.62
5	*Confident/Integrity/Availability*	*High*	0.56
		Low	0.22
		None	0

Dalam membantu proses hitung tingkat keparahan kerentanan kini CVSS telah menyediakan alat bantu kalkulator berbasis web secara gratis yang dapat di akses melalui https://www.first.org/cvss/calculator/3.0. Tampilan kalkulator dapat dilihat pada Gambar II.3.



Gambar II.3 Kalkulator *Base Metrics Group* (FIRST, 2019)

II.2.7 *Penetration Testing*

Penetration testing adalah serangkaian metode dan prosedur yang dilakukan untuk menguji dan melindungi sebuah keamanan organisasi. Menurut Baloch dalam buku *Ethical Hacking and Penetration Testing Guide* menyatakan bahwa *Penetration Testing* terbukti dapat membantu dan menemukan celah keamanan yang terdapat di dalam sebuah organisasi dan mampu memeriksa apakah penyerang mendapatkan akses yang tidak sah terhadap suatu informasi (Baloch, 2017). Dalam hal ini, pengujian suatu sistem pada instansi/organisasi harus memiliki izin dari pemilik objek sehingga diperlukan persetujuan dalam menentukan batasan-batasan dalam ruang lingkup terhadap metode dan target yang akan dilakukan *penetration testing*. Adapun di dalam *Penetration Testing* terdapat beberapa jenis teknik yang digunakan sebagai berikut (Setiawan dkk., 2022):

II.2.7.1 *Black Box Testing*

Black box testing adalah suatu kegiatan pengujian yang dilakukan untuk mengetahui cara kerja eksternal dari suatu sistem. Dalam pengujian ini hanya melihat *interface* dan fungsionalitas tanpa mengetahui proses yang terjadi didalam sistem. Selain itu, penguji hanya dibekali dengan alamat *Internet Protocol* (IP) dari target uji sehingga perlu melakukan pengumpulan informasi melalui *Search Engine* dan *Tools* khusus pengumpulan informasi guna menganalisis serta menentukan jenis eksploitasi yang dilakukan dalam tahapan *penetration testing*. Dengan demikian, pada penelitian ini peneliti menjadikan ini sebagai pendekatan dalam melakukan *penetration testing*. Karena pihak universitas hanya memberikan data berupa alamat IP target tanpa mengetahui detail proses didalamnya.

II.2.7.2 *White Box Testing*

White box testing adalah suatu kegiatan pengujian yang dilakukan tentang bagaimana sistem diimplementasikan. Dimana teknik pengujian internal ini hampir semua informasi tentang target disediakan. Hal ini mencakup analisis dalam penanganan pengecualian dan kesalahan bertujuan untuk memvalidasi apakah implementasi sistem mengikuti fungsionalitas. Sehingga pengujian *white box testing* ini memerlukan akses lebih ke sebuah sistem. Misalkan penguji melihat keseluruhan *source code* sebuah program untuk menemukan *bug*.

II.2.7.3 *Grey Box Testing*

Grey box testing adalah teknik pengujian yang dilakukan dari sudut pandang subjek yang terdapat di dalam sistem sehingga dapat mengetahui permasalahan dan kekurangan dalam sebuah sistem. Hal ini *grey box testing* merupakan bagian dari kombinasi dari *white box testing* dan *black box testing*. Artinya, penguji akan menggunakan cara kerja dari dalam sistem pada *source code* program.

II.2.8 NIST SP 800-15

NIST SP 800-115 adalah panduan yang diterbitkan pada tahun 2008 oleh *National Institute of Standards and Technology* (NIST) yang berdiri pada tahun 1901 dan sekarang telah menjadi bagian departemen perdagangan Amerika Serikat. NIST mengeluarkan beberapa seri publikasi salah satunya NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, metode yang dikeluarkan khusus membantu organisasi dalam menentukan seberapa efektif suatu entitas untuk dinilai dalam memenuhi tujuan keamanan serta pemberian rekomendasi dalam menangani permasalahan keamanan. Metode ini dapat dilakukan secara berkala dan didokumentasikan untuk meminimalkan risiko serta mengatasi kendala sumber daya yang terkait dengan penilaian keamanan (van den Hout, 2019). Dengan demikian, simpulan dari metode ini dapat membantu suatu organisasi dalam hal pengujian sistem guna menemukan kerentanan terhadap sistem serta memberikan rekomendasi dalam mengatasi kelemahan sistem tersebut. Selain itu, NIST 800-115 menyediakan metode *Penetration Testing* yang akan

digunakan dalam penelitian ini. Adapun tahapan metode NIST SP 800-115 terdapat pada Gambar II.4.

Gambar II.4 Tahapan NIST SP 800-11 (van den Hout, 2019)

II.2.8.1 *Planning*

Tahap ini dilakukan untuk menentukan aturan yang akan disepakati untuk melakukan *Penetration Testing* dan persiapan terkait *tools*, sistem operasi yang digunakan selama pengujian serta didokumentasikan. Dengan demikian, tahapan perencanaan untuk menetapkan dasar dalam melakukan *Penetration Testing* dapat berjalan sesuai syarat dan ketentuan. Namun, biasanya pada tahap ini dikumpulkan data dari pihak instansi/organisasi yang ingin dilakukan pengujian sistem keamanan. Data yang diperoleh akan digunakan pada tahap *Discovery*, sehingga tujuan akhir dari pengujian ini harus diterapkan untuk berjalannya *penetration testing*.

II.2.8.2 *Discovery*

Dalam tahap ini akan digunakan untuk mengetahui informasi yang terdapat pada target berdasarkan penggunaan *tools*, sehingga mempunyai dua tahapan yang harus dilakukan yaitu:

1. *Information Gathering*

Information Gathering adalah pengumpulan informasi mengenai target yang akan diuji. Pengumpulan informasi ini menggunakan ping, whois, dan SSLScan. Setelah dilakukan tahapan *Information Gathering* maka tahap selanjutnya *Vulnerability Scanning* guna melihat apakah target mempunyai kerentanan atau tidak serta seberapa parah kerentanan yang dimiliki oleh target tersebut.

2. *Vulnerability Scanning*

Vulnerability Scanning adalah melakukan pemindaian kerentanan terhadap target uji dengan *tools* NMAP, Nessus dan Wireshark.

II.2.8.3 *Attack*

Dalam tahap ini akan dilakukan eksploitasi terhadap kerentanan yang telah ditemukan pada tahap *Discovery* guna untuk memperoleh hak akses serta memvalidasi kerentanan yang ditemui. Dengan begitu, kerentanan yang ditemui pada sistem memiliki karakteristik dan dampak yang berbeda-beda.

II.2.8.4 *Reporting*

Tahap akhir ini mendeskripsikan hasil yang ditemui dari target uji untuk membuat laporan dengan menggambarkan kerentan yang teridentifikasi, menyajikan skor tingkat keparahan, dan memberikan rekomendasi perbaikan kerentanan.

II.2.9 Kali Linux *Tools*

Kali linux adalah sistem operasi berbasis debian linux yang digunakan oleh para ahli keamanan teknologi maupun pemula serta memiliki jangkauan spesialisasi yang luas, termasuk penetrasi pada jaringan, *forensics*, dan *vulnerability assessment*. Kali linux dikembangkan oleh *Offensive Security* di tahun 2012 dan juga penerus dari sistem operasi Backtrack, hal ini mempunyai kualitas yang baik, stabil, dan pilihan *software* dan aplikasi yang luas berdasarkan dari perancangan *Debian distribution*.

Pada sistem operasi kali linux menggunakan Debian *testing* sebagai sumber *repository* sehingga semua aplikasi yang berada di dalam Debian dapat langsung diinstal di dalam kali. Sehingga *tools* di kali linux dikategorikan menjadi 13 bagian berdasarkan tujuan dan fungsinya. Dalam mengajukan pengujian dapat dilakukan menggunakan *tools* yang sudah terinstal secara *default* atau dapat mendownload dari website dimana kali linux telah menyediakan lebih dari 600 *tools* yang dapat digunakan untuk kegiatan keamanan komputer (Cisar & Pinter, 2019).

II.2.9.1 PING

PING (*Packet Internet Network Groper*) merupakan perintah yang digunakan untuk melihat sebuah *host* dalam keadaan aktif di jaringan internet. Hal ini ditandai dengan status *packet* yang dikirimkan oleh *client* ke server mendapat kembali respon yang dikirimkan, maka dapat dinyatakan *host* dalam keadaan aktif dan jika tidak aktif *packet* yang dikirimkan tidak diterima kembali oleh *client* (Ratna Patria, 2022).

II.2.9.2 Whois

Whois merupakan *database* yang berisi informasi pengguna yang telah mendaftar dalam sebuah sumber internet seperti nama domain lokal indonesia .id dan .co.id ataupun nama domain internasional seperti .com, .net, maupun .org. Informasi yang disajikan mudah dimengerti yaitu nama domain, alamat IP dan informasi lainnya (Hussain dkk., 2017).

II.2.9.3 SSLScan

SSLScan adalah sebuah *command-line tool* yang dapat melakukan penilaian keamanan dengan mengqueri layanan yang diterima oleh server SSL/TLS dengan tujuan memberikan daftar kelemahan berdasarkan kode warna. Kode warna level tingkat bahaya berwarna merah, level tingkat menengah berwarna orange, dan warna hijau ataupun putih adalah yang direkomendasikan (Sslscan, 2022).

II.2.9.4 Wireshark

Wireshark adalah sebuah *tools* yang digunakan untuk menganalisa paket data yang terdapat pada lalu lintas jaringan. Hal ini wireshark juga termasuk *Network Packet Analyzer* yang berfungsi untuk menangkap semua data informasi yang melewati lalu lintas data di jaringan internet secara detail (Luthfansa & Rosiani, 2021).

II.2.9.5 NMAP

Network Mapper (NMAP) adalah sebuah *tool open source* untuk melakukan eksplorasi dan audit keamanan jaringan dalam mengidentifikasi *port* sebuah *host*. *Port* adalah mekanisme yang digunakan untuk mengizinkan sebuah perangkat dapat berinteraksi di dalam jaringan dan terdapat layanan untuk berkomunikasi menggunakan sebuah *protocol*. *Protocol* adalah sebuah sistem yang

mengatur proses pertukaran data antara pengirim dan penerima di dalam jaringan. Sehingga NMAP akan mengidentifikasi kondisi dari *port* menggunakan database, berdasarkan tiga kondisi yang dikenali yaitu *open, filtered,* dan *closed.*

Dalam hal ini, dari ketika kondisi yang dapat dikenal oleh NMAP, pada kondisi *open* menandakan *port* dapat bertukar informasi oleh perangkat luar di dalam jaringan. *Filtered* kondisi yang cukup susah ditelaah dan muncul ketika NMAP tidak dapat menentukan jenis servis yang sedang bekerja di dalam sebuah *port* yang terbuka. Dan *closed* menandakan *port* tidak dapat bertukar informasi. Karena *port* digunakan untuk menjalankan servis yang dibutuhkan oleh sistem, oleh karenanya *open port* menjadi salah satu jalur yang dimanfaatkan peretas salam mengakses sebuah sistem (Wardaya, 2019).

II.2.9.6 Nessus

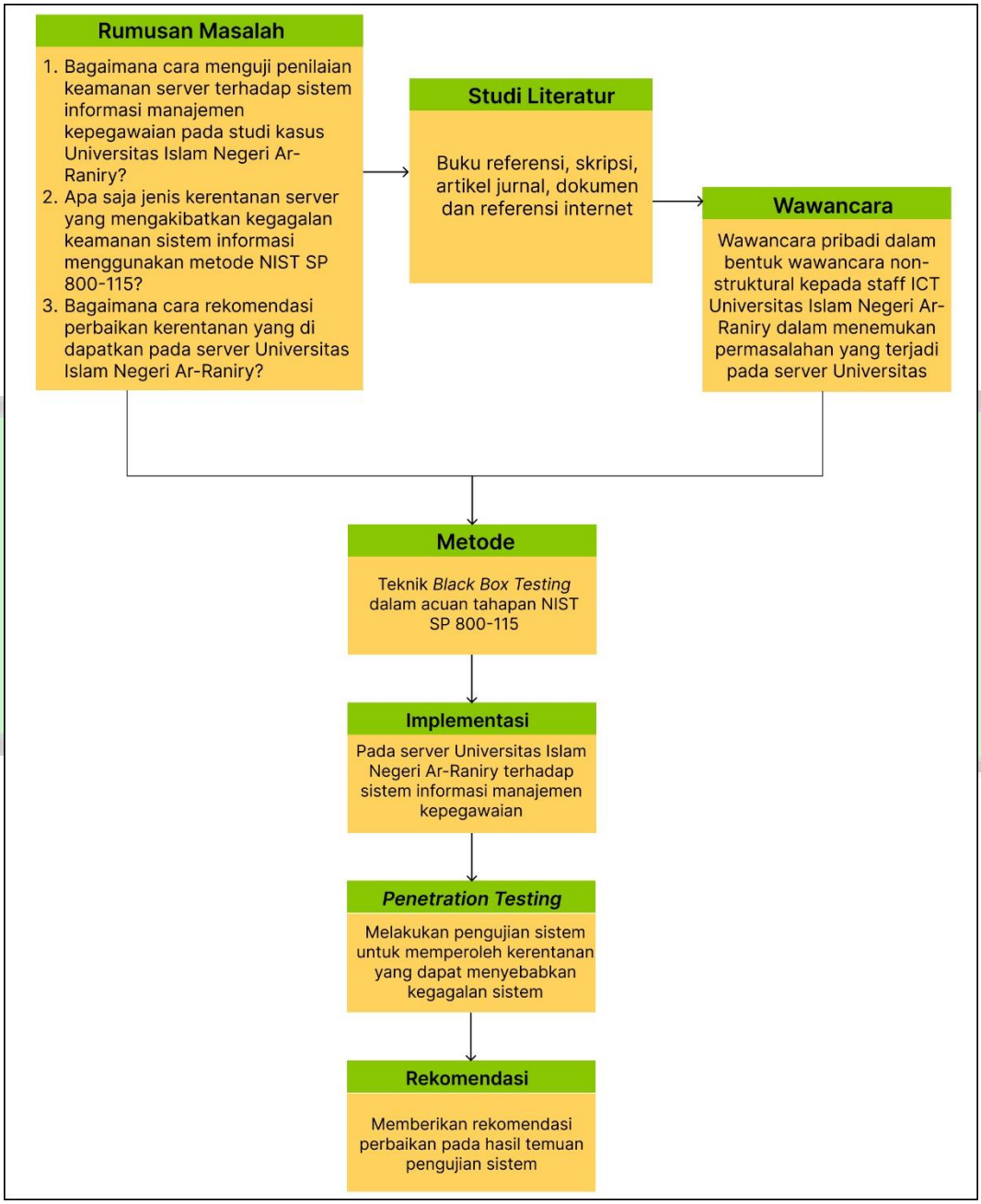
Nessus adalah salah satu *tool* yang digunakan untuk melakukan evaluasi terhadap jaringan dan layanan dari suatu sistem. *Tool* ini memiliki beberapa fungsi yang dapat digunakan yaitu *Vulnerability Scanning*, *Configuration Editing*, dan lain-lain. Hal ini *tool* nessus akan melakukan analisa terhadap protokol yang tersedia di jaringan lalu kan melakukan pengujian untuk menemukan celah keamanan yang terdapat pada suatu sistem. Dengan begitu, berbagai potensi kelemahan yang terdapat pada suatu sistem seperti celah keamanan, kelemahan sistem dan lainnya dapat ditemukan dengan menggunakan nessus yang melakukan evaluasi pada 1200 pengujian terhadap 1 layanan (Tan & Soewito, 2022).

II.2.9.7 Metasploit

Metasploit adalah sebuah *framework* yang digunakan untuk melakukan pengujian kelemahan sistem yang dimiliki. Dalam hal ini, metasploit *framework* akan menjalankan modul serta mengkonfigurasi modul *exploit* untuk dijalankan pada target yang dituju. Sehingga keberhasilan eksploitasi akan dimanfaatkan penyerang sebagai tindak kejahatan dunia maya (Prakoso, 2019).

II.3 Kerangka Berpikir

Dalam melakukan penelitian ini peneliti menggambarkan kegiatan penilaian keamanan server yang tertuang dalam kerangka pemikiran. Kerangka pemikiran yang digunakan peneliti dapat dilihat pada Gambar II.5.

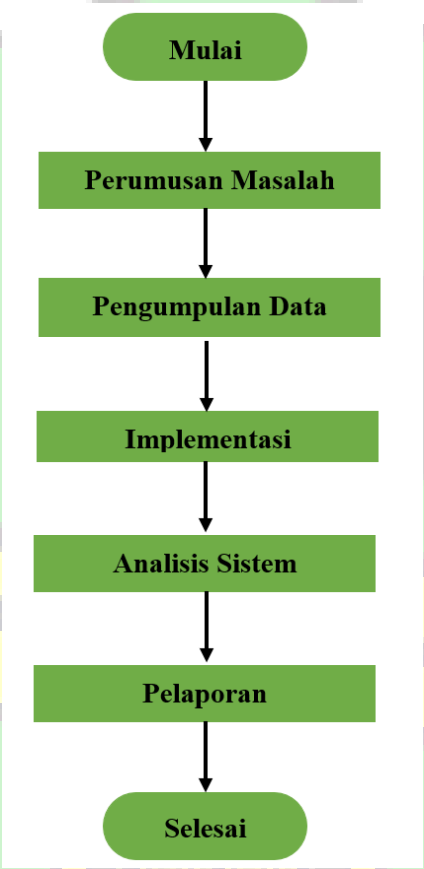


Gambar II.5 Kerangka Pemikiran

BAB III
METODE PENELITIAN

III.1 Tahapan Penelitian

Adapun tahapan penelitian yang akan dilakukan dalam penulisan tugas akhir dapat dilihat pada Gambar III.1.



Gambar III.1 Tahapan Penelitian

III.1.1 Perumusan Masalah

Perumusan masalah adalah sebuah pernyataan mengenai ruang lingkup masalah yang akan diteliti bertujuan untuk memperoleh hasil yang di ingin oleh peneliti.

III.1.2 Pengumpulan Data

Dalam penyusunan penelitian dilakukan pengumpulan data yang mendukung penyelesaian tugas akhir ini yaitu:

1. Studi Literatur

   Studi literatur adalah pengumpulan data dari sumber buku, jurnal, referensi internet, skripsi, dan dokumen dengan tujuan untuk menyusun dasar teori kerangka penelitian yang berhubungan dengan topik dalam suatu penelitian.

2. Wawancara

   Wawancara adalah suatu kegiatan percakapan antara dua pihak dalam bentuk tanya jawab dengan tujuan memperoleh suatu informasi terkait suatu isu tertentu. Pada penelitian ini wawancara dilakukan dalam bentuk non-struktural kepada staff ICT Universitas Islam Negeri Ar-Raniry. Dari wawancara tersebut ditemukan permasalahan bahwa penting melakukan *penetration testing* terhadap suatu sistem mengingat tindak kejahatan *cybercrime* sangat merebak sampai saat ini. Oleh karena itu, disimpulkan bahwa akan dilakukan pengujian Sistem Informasi Manajemen Kepegawaian menggunakan *black box testing* dengan metode NIST SP 800-115.

III.1.3 Implementasi

Implementasi adalah suatu kegiatan penerapan perencanaan pada penelitian yang dibuat. Sehingga implementasi dalam penelitian ini pada sistem informasi manajemen kepegawaian yang terdapat di dalam server universitas dengan cara penerapan *black box testing* dari tahapan NIST SP 800-115

III.1.4 Analisis Sistem

Analisis adalah suatu kegiatan penyelidikan terhadap suatu objek penelitian untuk memperoleh fakta yang tepat. Pada penelitian ini dilakukan analisis penilaian keamanan server terhadap Sistem Informasi Manajemen Kepegawaian untuk menemukan kerentanan dari proses pengujian sistem dengan menggunakan *tools*.

III.1.5 Pelaporan

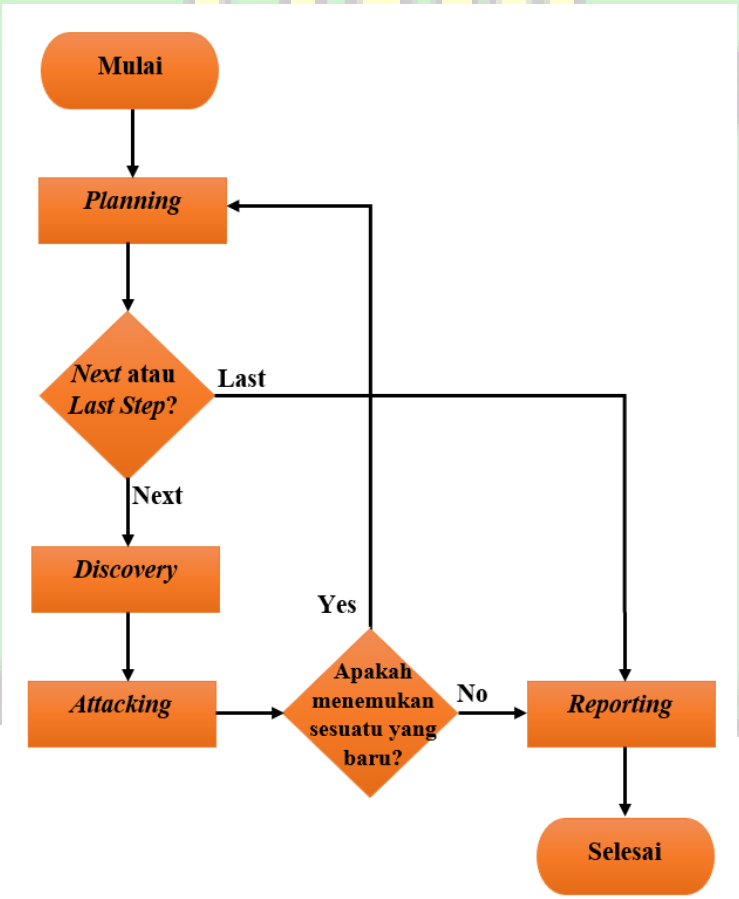
Pelaporan adalah suatu kegiatan yang diakhiri dengan pembuatan laporan secara detail dari hasil analisis yang telah diproses. Sehingga hasil penelitian yang diperoleh akan dibuat dalam bentuk laporan untuk mengetahui kerentanan dari server.

III.2 Data Penelitian

Adapun data penelitian diambil dari hasil pengujian pada *utility* dan *tools* saat melakukan kegiatan pengujian Sistem Informasi Manajemen Kepegawaian. Hasil yang didapatkan memiliki kondisi dan dampak yang berbeda-beda. Sehingga studi literatur sejenis digunakan sebagai panduan untuk mengkategorikan dan menentukan skor kerentanan sesuai jenis data.

III.3 Alur Penelitian

Alur penelitian ini menggunakan beberapa tahapan dimulai dari *planning* setelah itu *Discovery* dibagi menjadi dua yaitu *information gathering* dan *vulnerability scanning*, lalu *attack* serta pembuatan *reporting* dari hasil pengujian dan pemberian rekomendasi. Adapun gambar alur penelitian dapat dilihat pada Gambar III.2.



Gambar III.2 Alur Penelitian

III.3.1 *Planning*

Pada tahap ini dilakukan perencanaan dengan menentukan target dan ruang lingkup pengujian serta tujuannya. Dalam hal ini, target dari pengujian adalah Sistem Informasi Manajemen Kepegawaian yang berada di dalam server universitas. Pengujian ini menggunakan metode *Black Box Testing* sehingga informasi yang diberikan kepada peneliti yaitu domain sistem informasi. Hal ini untuk melihat target dapat diakses dengan melakukan *test ping*. Apabila kondisi target dalam keadaan aktif maka dilakukan tahap selanjutnya yaitu *discovery*.

III.3.2 *Discovery*

Pada tahap ini menggunakan *utility* dan *tools* untuk mengumpulkan informasi mengenai sistem. Untuk menentukan kondisi dari sistem informasi dilakukan pengiriman paket menggunakan ping, jika paket diterima maka diketahui *host* dalam keadaan aktif dan dapat terhubung. Selanjutnya menggunakan whois guna mengetahui informasi domain serta informasi pribadi pendaftar domain. Dan SSLScan digunakan untuk melihat layanan pada server SSL/TLS dengan memberikan daftar kelemahan dan kerentanan berdasarkan kode warna.

Pengumpulan informasi menggunakan beberapa *tools* untuk menemukan kerentanan-kerentanan pada sistem informasi. NMAP digunakan untuk eksplorasi dalam mengidentifikasi *port* dari sebuah *host* yang berstatus *open, filtered,* dan *closed*. Apabila port yang terbuka dan tanpa autentikasi salah satu jalur untuk *hacker* mengakses sistem. Wireshark yang digunakan untuk menganalisa paket yang melewati lalu lintas data. Nessus digunakan untuk pengujian *Vulnerability Scanning* dalam mencari kerentanan pada target uji. Dengan demikian, tahap *discovery* mempunyai sifat fleksibilitas karena mampu kembali ke tahap awal dalam melakukan perencanaan terhadap penemuan baru saat proses pengujian.

III.3.3 *Attack*

Pada tahap ini merupakan bagian dari metode NIST SP 800-115 untuk melakukan pengujian terhadap sistem informasi yang terdapat pada server Universitas Islam Negeri Ar-Raniry guna melakukan serangan yang telah dikumpulkan pada tahap *discovery*. Adapun serangan yang dilakukan menyesuaikan dengan celah yang telah diketahui dari tahap sebelumnya. Tujuan

dari tahap ini untuk membuktikan seberapa parah ancaman dari celah kerentanan terhadap sistem jika dieksploitasi.

III.3.4 *Reporting*

Pada tahap akhir ini akan mempresentasikan data mengenai rangkuman dari hasil dari pengujian. Hal ini pembuatan laporan pada tahap ini menggunakan tabel untuk merangkum hasil yang telah ditemui dari masing-masing proses sehingga dapat diambil kesimpulan.

III.4 Alat Bantu Penelitian

Alat yang digunakan dalam melakukan penelitian ini adalah *hardware* dan *software*. *Hardware* yang digunakan adalah laptop dan *software* yang digunakan sistem operasi kali linux dan *tools* pendukung melakukan pengujian keamanan. Adapun alat bantu penelitian yang digunakan terdapat pada Tabel III.1 dan Tabel III.2.

Tabel III.1 Spesifikasi *Hardware*

Komponen	**Komponen**	
Main OS	*Processor*	AMD Ryzen 7-6800 CPU
	Random Access Memory (RAM)	16 GB
	Storage Memory	512 GB
	Video Graphics Array (VGA)	NVIDIA GeForce RTX 3060-6GB GDDR6
	Operating System (OS)	Windows 11 *Home Single Language*

Tabel III.2 Spesifikasi *Software*

Komponen	**Software**	**Versi**
Dual OS	Kali Linux	2022.4
Information Gathering	Ping	-
	Whois	5.5.14
	SSLScan	2.0.15
Vulnerability Scanning	NMAP	7.93
	Nessus	10.4.2
	Wireshark	4.0.4
Attack	Metasploit	6.2.31
Reporting	Microsoft Word	2021

III.5 Tempat dan Waktu Penelitian

Adapun tempat dan waktu penelitian dalam mengumpulkan data penelitian ini sebagai berikut:

III.5.1 Tempat Penelitian

Lokasi penelitian dilaksanakan pada Universitas Islam Negeri Ar-Raniry yang beralamat Jl. Syeikh Abdul Rauf Kopelma Darussalam, Banda Aceh.

III.5.2 Waktu Penelitian

Waktu pelaksanaan kegiatan dalam proses pengujian sistem informasi manajemen kepegawaian dibutuhkan dalam melakukan penelitian ini mulai dari 1 Oktober 2022 s.d 15 Februari 2023.

BAB IV
HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada penelitian ini meliputi pembahasan hasil pengujian teknik *black box testing* menggunakan metode NIST SP 800-115. Adapun Tahapan yang digunakan yaitu *planning*, *discovery*, *attack*, dan *reporting*.

IV.1 *Planning*

Tahapan awal untuk menentukan perencanaan dan persiapan *penetration testing*. Tahap ini harus dilakukan sesuai dengan metode NIST SP 800-115. Maka dari itu, dibutuhkan pemaparan mulai dari perencanaan dan persiapan sebagai berikut:

A. Ruang Lingkup

Komunikasi dengan pihak staff ICT universitas untuk menentukan proses yang akan dilakukan di dalam penelitian ini. Adapun kesepakatan yang dihasilkan pada tahap ini ialah:

1. Identifikasi kontak peneliti dan staff ICT;
2. Konfirmasi terkait pendekatan dan penjelasan metode *penetration testing* berdasarkan acuan NIST SP 800-115 yang akan digunakan dalam melakukan pengujian kerentanan sistem;
3. Persetujuan pengujian kasus, meliputi:
   a. Penggunaan teknik *Black Box Testing* dalam melakukan *penetration testing*;
   b. Target uji Sistem Informasi Manajemen Kepegawaian; dan
   c. Penggunaan beberapa *tools* untuk melakukan *penetration testing* serta dapat menyesuaikan *tools* lainnya sesuai kebutuhan penelitian dari perolehan kerentanan.
4. Penyerahan hasil *report* kepada pihak staff *Information and Communication Technology* (ICT) Center; dan
5. Data yang diberikan kepada peneliti hanya berupa DNS target uji.

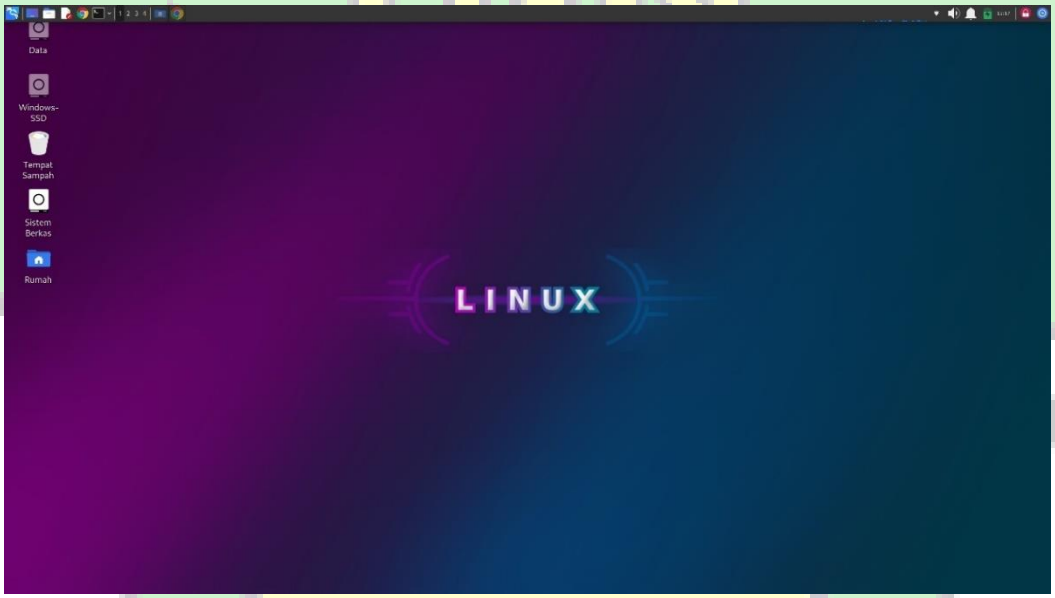
B. Persiapan Pemasangan *Software*

Pada penelitian ini membutuhkan pesangangan sistem operasi kali linux secara *dual booting* dan *tools* pendukung pengujian sebagai alat bantu penelitian untuk melakukan *penetration testing*. Berikut spesifikasi sistem operasi kali linux yang terpasang secara dual booting dapat dilihat pada Tabel IV.1.

Tabel IV.1 Spesifikasi OS Kali Linux

Komponen	**Informasi**	
Dual OS	*Processor*	AMD Ryzen 7-6800 CPU
	Random Access Memory (RAM)	16 GB
	Storage Memory	100 GB
	Video Graphics Array (VGA)	NVIDIA GeForce RTX 3060-6GB GDDR6

Adapun tampilan desktop sistem operasi kali linux dapat dilihat pada Gambar IV.1.



Gambar IV.1 Sistem Operasi Kali Linux

Pada sistem operasi kali linux terdapat beberapa *tools* yang sudah terpasang langsung pada saat pemasangan sistem operasi kali linux seperti ping, *whois*, wireshark, nmap, sslscan, dan metasploit. Adapun untuk pasangangan *tool* Nessus dengan perintah **dpkg -i** nama paket.deb, untuk paket Nessus dapat di download melalui https://www.tenable.com/downloads/.

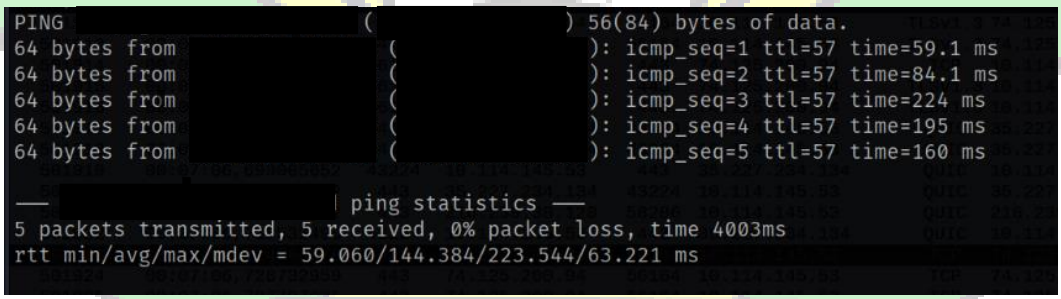
IV.2 *Discovery*

Tahap *Discovery* dapat dilakukan setelah tahapan *planning* selesai dilaksanakan. Dalam hal ini, tahap *Discovery* akan melakukan *information gathering* dan *vulnerability scanning* pada sistem informasi yang diuji. Oleh karena itu, teknik *black box testing* memerlukan *tools* dalam mengumpulkan informasi mengenai target uji. *Tools* yang digunakan yaitu ping, whois, dan SSLScan untuk mengetahui informasi publik. Sedangkan untuk mencari kerentanan *port scanning* yaitu NMAP dan *vulnerability scanning* menggunakan Nessus, dan Wireshark.

A. *Information Gathering*

Pada tahap ini akan dilakukan pencarian informasi dari data DNS target yang telah diberikan oleh pihak ICT Universitas Islam Negeri Ar-Raniry. Informasi dikumpulkan dengan cara penggunaan *tools* baik berupa *hostname*, *database* domain, lokasi, maupun *protocol security* yang digunakan.

PING digunakan dalam *information gathering* sebagai penanda *host* dalam keadaan *alive*. Dalam hal ini, ping dilakukan dengan perintah **ping -c 5** "*Domain Name System*", pengujian ping dilakukan sebanyak 3 kali untuk mengetahui apakah dengan uji ping dalam waktu yang berbeda terdapat perubahan IP *Address*. Adapun tampilan hasil ping dari salah satu pengujian dapat dilihat pada Gambar IV.2.



Gambar IV.2 Hasil PING

Dari gambar tersebut dapat diketahui bahwa ping berhasil dilakukan ditandai dengan mendapat *respon* dari web server. Penggunaan parameter **-c 5** untuk menentukan batasan ping yang dilakukan pada *host* ditandai dengan icmp_seq=5, *Time to Live* (TTL) merupakan durasi paket data dalam jaringan dalam hitungan detik, *time* merupakan waktu *respon* dari *host* dalam satuan *milisecond* (ms) sehingga waktu ping yang bagus dibawah 100 ms, dan *bytes* jumlah

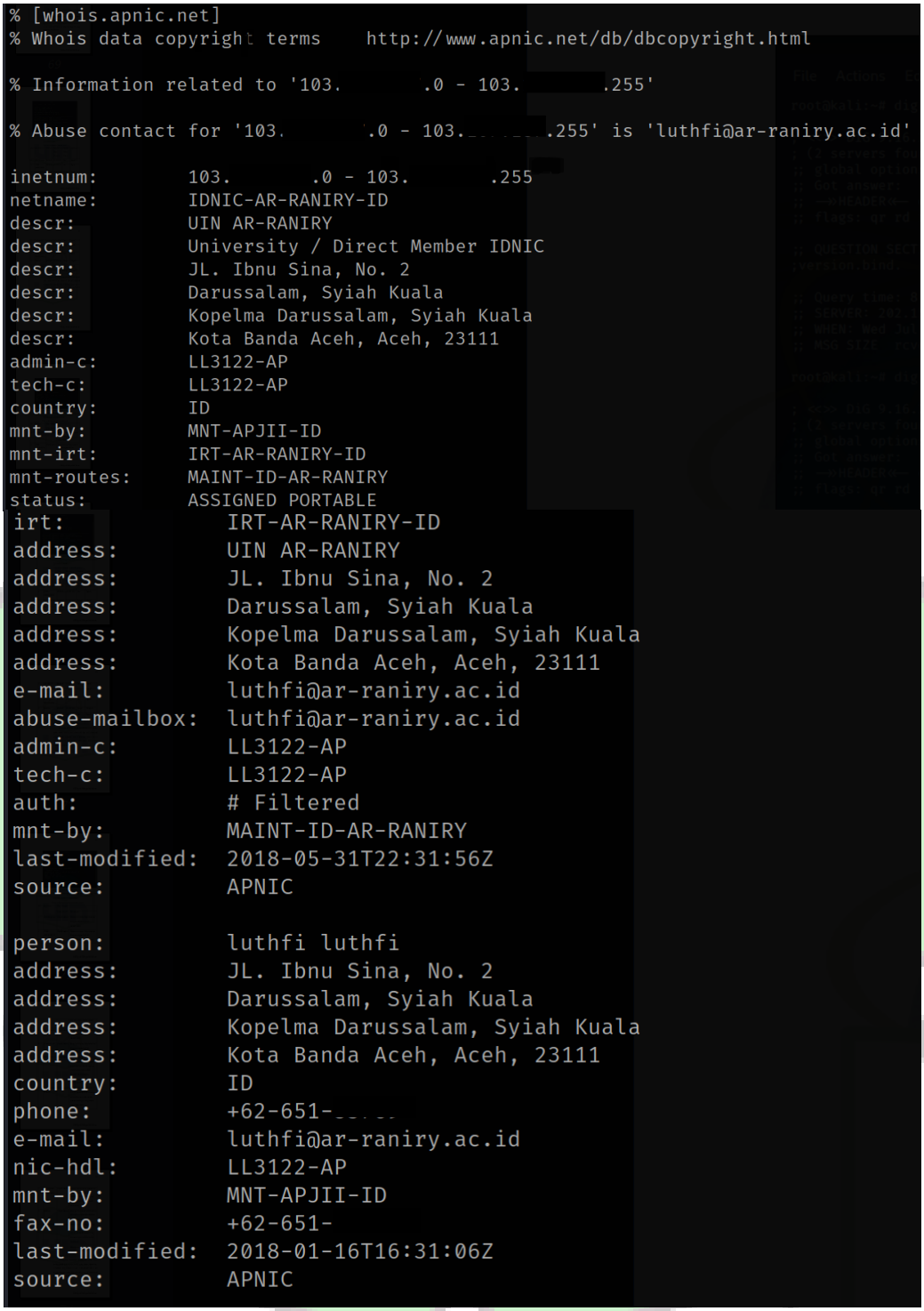
data yang dikirimkan. Berikut ini dapat dilihat tabel dari hasil pengujian yang dilakukan menggunakan *tool* ping.

Tabel IV.2 Pengujian PING

No	*Domain Name System*	Waktu PING	IP *Address*	*Bytes*	ICMP *Sequence*	*Time to Live*	*Time*
1	xxxxx.ar-raniry.ac.id	20.00	103.xx.xx.236	64	1	57	59.1 ms
			103.xx.xx.236	64	2	57	84.1 ms
			103.xx.xx.236	64	3	57	224 ms
			103.xx.xx.236	64	4	57	195 ms
			103.xx.xx.236	64	5	57	160 ms
2	xxxxx.ar-raniry.ac.id	22.00	103.xx.xx.236	64	1	57	95.2 ms
			103.xx.xx.236	64	2	57	154 ms
			103.xx.xx.236	64	3	57	101 ms
			103.xx.xx.236	64	4	57	347 ms
			103.xx.xx.236	64	5	57	219 ms
3	xxxxx.ar-raniry.ac.id	00.00	103.xx.xx.236	64	1	57	95.8 ms
			103.xx.xx.236	64	2	57	140 ms
			103.xx.xx.236	64	3	57	81.2 ms
			103.xx.xx.236	64	4	57	123 ms
			103.xx.xx.236	64	5	57	68.8 ms

Dari hasil Tabel IV.*2* bahwa perolehan IP *Address* dari penggunaan *tool* ping dengan inputan *Domain Names System* tidak terjadi perubahan dalam jangka waktu ping 2 jam berlalu akan tetap memperoleh IP *Address* 103.xx.xx 236.

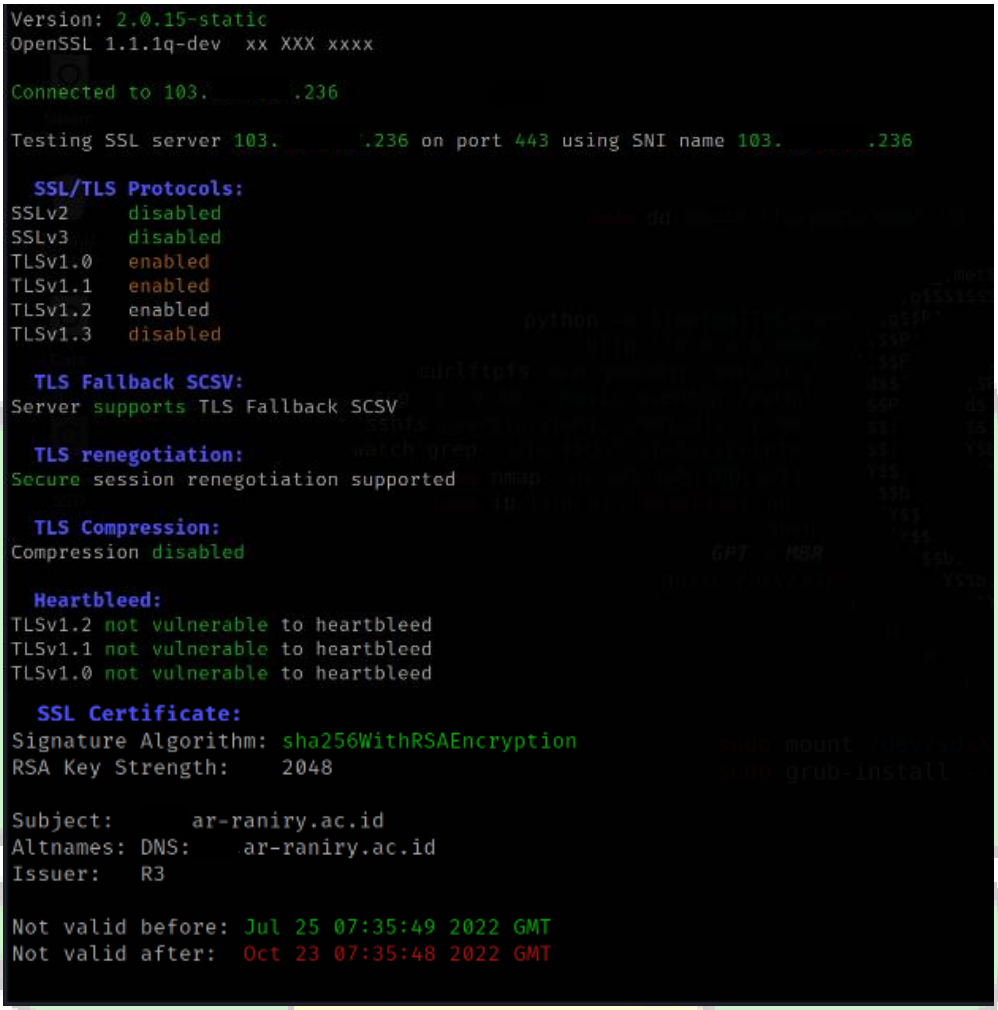
Selanjutnya *whois* digunakan untuk menemukan informasi terkait *Domain Names System* (DNS) dari IP *Address* yang menjadi target. Dalam hal ini, penggunaan *tool whois* dilakukan yang kedua setelah penggunaan *tool* ping untuk menemukan IP *Address* terlebih dahulu, hal ini disebabkan tidak dapat dilakukan menggunakan DNS langsung karena target ini bagian dari sub domain. Adapun tampilan hasil *whois* dapat dilihat pada Gambar IV.3.



Gambar IV.3 Hasil Whois

Dalam hal ini, *whois* berhasil dilakukan dengan perintah **whois** "IP *Address*". Hasil yang didapatkan berupa data pribadi pendaftar domain seperti nama luthfi; Kontak: +62-651-xxxxx; Email: luthfi@ar-raniry.ac.id; dan *Block* IP *Address*: 103.xx.xx.0 – 103.xx.xx.255.

Proses selanjutnya akan melakukan pemindaian SSL/TLS protokol keamanan pada web server. Pemindaian ini menggunakan tool SSLScan untuk mendeteksi protokol keamanan komunikasi melalui internet. Adapun tampilan hasilnya dapat dilihat pada Gambar IV.4.



Gambar IV.4 Hasil SSLScan

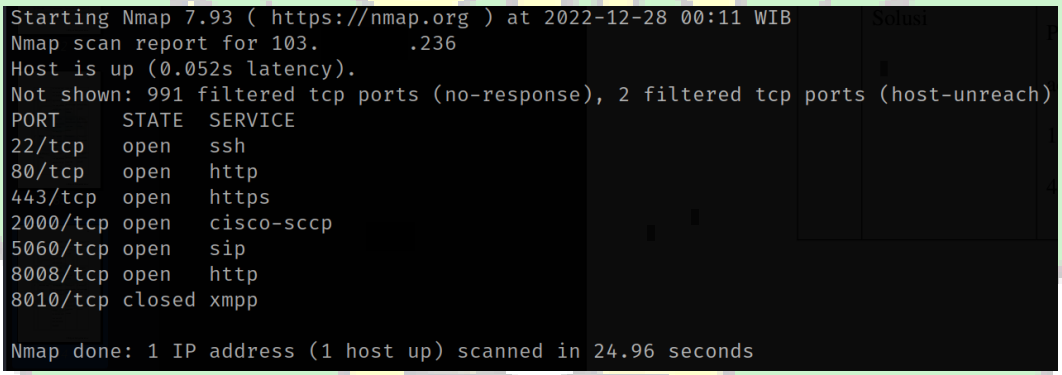
Hal ini seperti yang terlihat pada gambar di atas bahwa TLSv1.3 statusnya *disabled*. *Secure Sockets Layer* (SSL) dan penerusnya *Transport Layer Security* (TLS) adalah sebuah protokol untuk mengamankan komunikasi di internet. Dalam hal ini, di web server telah menerapkan *Hypertext Transfer Protocol Secure* (HTTPS) tetapi masih menggunakan protokol versi 1.0 dan 1.1 sehingga terdeteksi warna orange yang menandakan harus diganti ke versi terbaru dengan men-non-aktifkan TLSv1.0 dan TLSv1.1 dan mengaktifkan TLSv1.3 yang lebih baru untuk mengamankan data di internet. Kemudian ditemukan DNS Server yang SSL

Certificate Expiry sehingga harus membeli/mengganti sertifikat SSL baru pada DNS Server tersebut.

B. *Vulnerability Scanning*

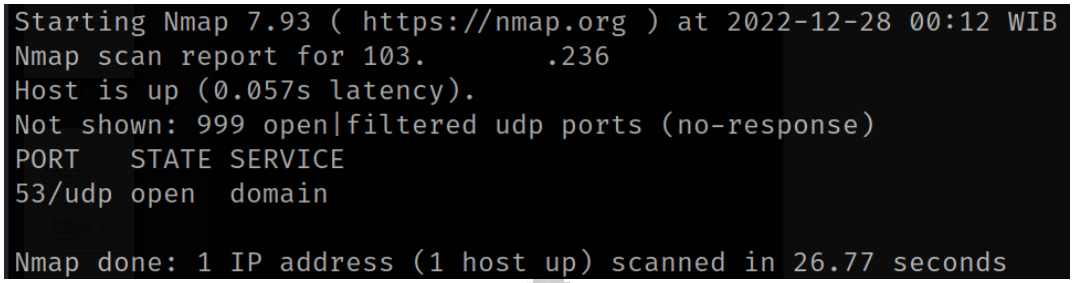
Pada tahap ini akan dilakukan pemindaian kerentanan pada target uji untuk mengetahui apakah sistem informasi yang diuji terdapat kerentanan atau tidak serta seberapa parah tingkat kerentanan yang dimiliki oleh sistem informasi tersebut. Pengujian ini menggunakan *tools* NMAP, dan Nessus.

Pada tahap awal dilakukan *scanning port* pada target uji dengan menggunakan *Network Mapping* (NMAP) untuk mengetahui apakah terdapat *open port* pada target uji tersebut. Dalam hal ini, *tool* NMAP berhasil melakukan *port scanning Transmission Control Protocol* (TCP) yang ada pada server dengan perintah **nmap -sT** "IP *Address*". Hasil pemindaian *port* TCP terdapat pada Gambar IV.5.



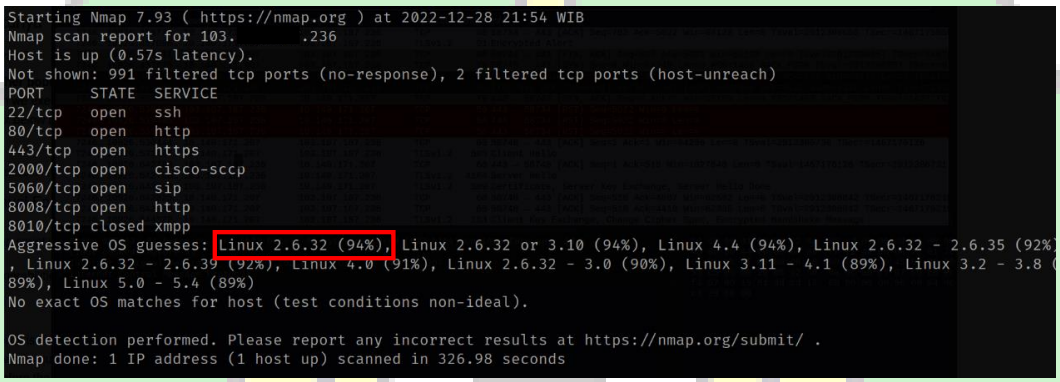
Gambar IV.5 Hasil TCP *Scan* NMAP

Dari hasil TCP *scan* dapat diketahui bahwa ditemukan *port Extensible Messaging and Presence Protocol* (xmpp) dengan *state close* yang artinya tidak ada pertukaran informasi dari *port* tersebut. Kemudian ditemukan *port* selain HTTP dan HTTPS maka dari itu perlu dilakukan *scan* untuk mengetahui kebenaran *state* dari *open port*. Hal ini dilakukan *User Datagram Protocol* (UDP) *scan* yang dapat menentukan *state* dari *port*. Adapun hasil pemindaian *port* UDP terdapat pada Gambar IV.6.



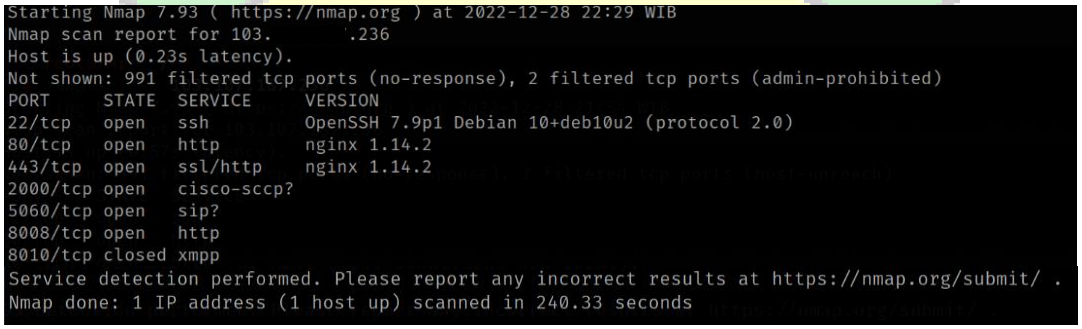
Gambar IV.6 Hasil UDP *Scan* NMAP

Hasil *scan* dengan parameter **-sU** menunjukkan daftar *open port* UDP yaitu *port* domain. Selanjutnya akan deteksi *System Operation* (OS) yang digunakan oleh server 103.xx.xx.236. Adapun hasilnya dapat dilihat pada Gambar IV.7.



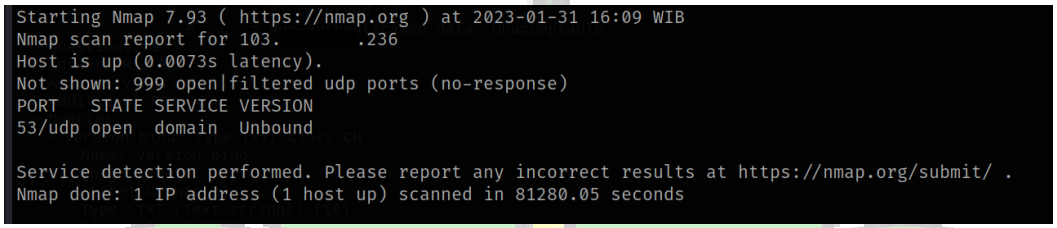
Gambar IV.7 Hasil OS *Fingerprinting*

Perolehan hasil pemindaian OS *Fingerprinting* menggunakan parameter **-O** sehingga menunjukkan bahwa sistem operasi yang digunakan ialah Linux 2.6.32 dengan tingkat akurasi 94%. Kemudian selanjutnya akan deteksi *service version* yang ada pada *port* dengan parameter **-sV** untuk mengetahui *service fingerprinting* pada *ports* tersebut. Adapun hasilnya dapat dilihat pada Gambar IV.8.



Gambar IV.8 Hasil *Service Fingerprinting* TCP

Dari gambar IV.8 hasil yang didapatkan berupa informasi jenis web server yang digunakan nginx 1.14.2, layanan OpenSSH 7.9p1 (*protocol* 2.0). Hal ini dari hasil yang diperoleh hanya menampilkan *service fingerprinting* TCP maka akan dilakukan *scanning* pada *port* UDP dengan perintah **nmap -sU -sV** "IP *Address*". Berikut hasilnya dapat dilihat pada Gambar IV.9.



Gambar IV.9 Hasil *Service Fingerprinting* UDP

Perolehan hasil pemindaian *service fingerprinting* UDP pada *port* domain menggunakan unbound sebagai penyelesai DNS yang memvalidasi, rekursif, dan caching. Dengan demikian, seluruh hasil *scan* NMAP berhasil menemukan beberapa *open ports* dalam target uji yang dirangkum pada Tabel IV.3.

Tabel IV.3 Hasil Pemindaian *Ports* NMAP

No.	*Port*	*Protocol*	*Service*
1	22	TCP	SSH
2	80	TCP	HTTP
3	443	TCP	HTTPS
4	2000	TCP	Cisco-SCCP
5	5060	TCP	SIP
6	8008	TCP	HTTP
7	53	UDP	Domain

Dari hasil pemindaian *ports* NMAP menunjukkan terdapat 7 *port* TCP/UDP yang berstatus *open port* dengan fungsi yang berbeda. *Port* 22 memberikan kerahasiaan dan integritas dalam mengirimkan data melalui jaringan secara terenkripsi serta bisa diakses dari jarak jauh. *Port* 80 untuk memungkinkan terhubung ke halaman web sehingga terjadi komunikasi antara *client* dan server web. *Port* 443 untuk melakukan pertukaran data dengan aman antara *client* dan server. *Port* 2000 bagian dari perangkat jaringan yang digunakan sebagai kontrol eksklusif dan protokol komunikasi berbasis IP dengan Cisco. *Port* 5060 untuk

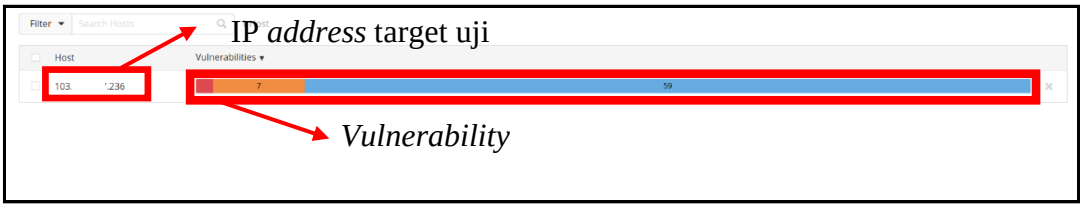
signaling dan kontrol sesi panggilan dalam memodifikasi, menetapkan dan mengakhiri sesi komunikasi IP. *Port* 8008 untuk menyeimbangkan muatan, pengoptimalan protokol dan segmentasi klien yang diterapkan di browser seluler dan desktop. Dan *port* 53 yang menyimpan informasi nama *host* maupun domain dalam bentuk database di dalam jaringan.

Proses selanjutnya dilakukan pemindaian kerentanan terhadap target uji menggunakan nessus. Pengujian dilakukan secara otomatis untuk memperoleh kerentanan dengan melakukan *scanning* secara terus-menerus terhadap IP *address* target 103.xx.xx.236. Sehingga waktu yang dibutuhkan selama pengujian tergantung jaringan dan *respond*. Bukti pengujian nessus yang telah dilakukan dengan status *completed* dapat dilihat pada Lampiran 1 Gambar 1.1. Sehingga total keseluruhan pengujian diolah dalam sebuah tabel seperti yang terlihat pada Tabel IV.4.

Tabel IV.4 Pengujian Nessus

No	Tanggal Pengujian	Waktu Mulai	Waktu Selesai
1	29/12/2022	21.04	21.21
2	29/12/2022	22.31	22.39
3	02/01/2023	19.56	20.52
4	02/01/2023	21.48	22.41
5	02/01/2023	23.48	00.06
6	08/01/2023	20.06	20.53
7	08/01/2023	22.11	22.20
8	08/01/2023	22.41	22.51
9	15/01/2023	21.14	21.47
10	15/01/2023	21.50	22.29
11	21/01/2023	12.45	14.05
12	28/01/2023	15.10	15.57

Dari hasil pengujian dengan menggunakan nessus maka hasil uji yang diambil di dalam penelitian ini pada tanggal 02 Januari 2023 pada jam 21.48 s.d 22.41. Hasil uji tersebut yang diperoleh telah mencakup seluruh *vulnerability* dari setiap pengujian yang dilakukan. Adapun hasil *scanning* dengan nessus ditunjukkan secara rinci *vulnerability* seperti pada Gambar IV.10.



Gambar IV.10 *Vulnerability Scanning* dengan Nessus

Dari hasil *scanning* yang telah dilakukan nessus ditemukan *vulnerability*, dalam icon *vulnerability* ditandai dengan keterangan warna dari setiap *threat level*. *Threat level High* ditandai dengan warna merah, *medium* ditandai dengan warna *orange*, dan *none* ditandai dengan warna biru. Hal ini hasil detail *vulnerability scanning* dapat dilihat pada Lampiran 1 Gambar 1.2. Sehingga didapat informasi *vulnerability*-nya yang diolah dalam sebuah tabel guna mempermudah pengolahan data. Adapun data *vulnerability* yang diperoleh dari hasil *scan* berdasarkan *threat level* seperti pada Tabel IV.5.

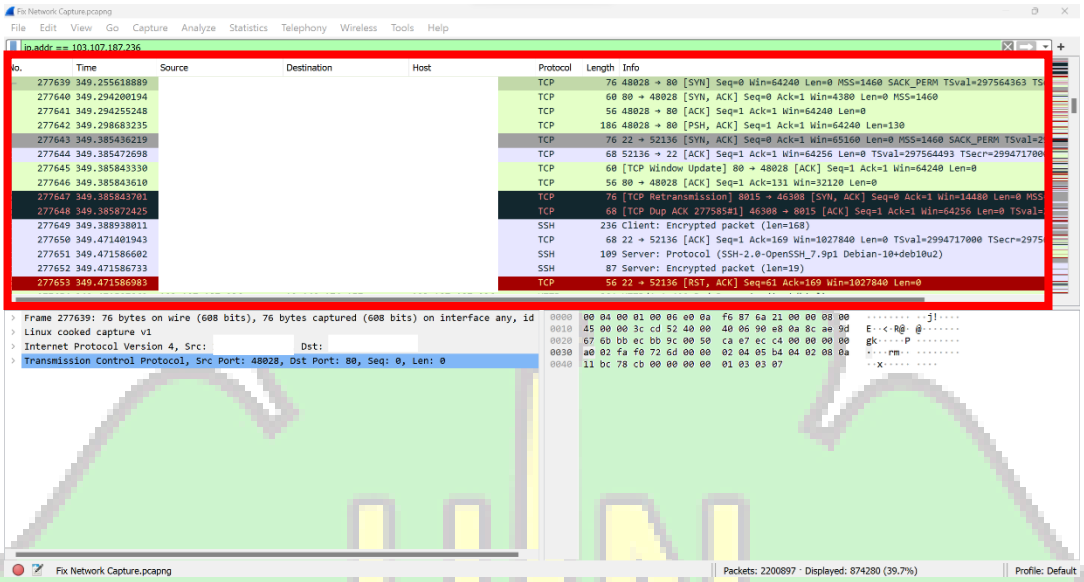
Tabel IV.5 Hasil *Vulnerability* dengan Nessus

No	***Vulnerability***	CVSS	***Threat Level***	Analisis
1	DNS Server *Spoofed Request Amplification* DDoS	CVSS:3.0 /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	*High*	Kerentanan ini akan menjawab permintaan dari *remote* DNS Server dengan memanfaatkan amplifikasi untuk melakukan serangan *Distributed Denial of Service* (DDoS).
2	TLS *Version* 1.0 *Protocol Detection*	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	*Medium*	Terdeteksi masih menggunakan protokol TSL versi lama (1.0) dalam mengenkripsi lalu lintas data. Sehingga harus di nonaktifkan TLSv1.0.
3	TLS *Version* 1.1 *Protocol Detection*	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	*Medium*	Terdekrisi masih menggunakan protokol TSL versi lama (1.1) dalam mengenkripsi lalu lintas data. Sehingga harus di nonaktifkan TLSv1.1.
4	SSL *Certificate Cannot Be Trusted*	CVSS:3.0/AV:N/AC:L/PR	*Medium*	Kerentanan ini didapatkan akibat rantai SSL sertifikat *remote host* tidak dapat

No	*Vulnerability*	CVSS	*Threat Level*	Analisis
		:N/UI:N/ S:U/C:L/ I:L/A:N		dipercaya dari DNS nbv.ar-raniry.ac.id sehingga sertifikat perantara hilang akan menghubungkan bagian atas rantai sertifikat ke otoritas sertifikat yang dikenal.
5	SSL *Certificate Expiry*	CVSS:3. 0/AV:N/ AC:L/PR :N/UI:N/ S:U/C:N/ I:L/A:N	*Medium*	Kerentanan dari SSL sertifikat *remote host* telah kadaluarsa dari DNS nbv.ar-raniry.ac.id.
6	SSL/TLS *Protocol Initialization VectorImplement ation Information Disclosure*	CVSS:3. 0/AV:N/ AC:L/PR :N/UI:N/ S:U/C:L/ I:N/A:N	*Medium*	Kerentananyang memungkinkan mendapatkan informasi sensitif dari *remote host* SSL/TLS yang terdapat pada TLS 1.0 di dalam server. Sehingga rentan terhadap *Browser Exploit Against* SSL/TLS (BEAST).
7	Nginx < 1.17.7 *Information Disclosure*	CVSS:3. 0/AV:N/ AC:L/PR :N/UI:N/ S:U/C:L/ I:N/A:N	*Medium*	Web server yang digunakan sekarang versi lama yaitu 1.14.2 sehingga rentan dalam pengungkapan informasi dengan mudah.
8	DNS Server *Recursive Query Cache Poisoning Weakness*	CVSS:3. 0/AV:N/ AC:L/PR :N/UI:N/ S:U/C:N/ I:L/A:N	*Medium*	Kerentanan yang memberi izin *query recursive name* server sehingga pihak ketiga mampu meminta *Name* Server (NS) dengan menggunakan alamat palsu ke dalam DNS.

Selanjutnya penggunaan *tool* wireshark untuk melakukan *sniffing* paket data pada jaringan. *Sniffing* merupakan proses memonitor dan menangkap semua lalu lintas jaringan yang lewat. Pada percobaan ini penguji akan melakukan *sniffing* untuk mendapatkan informasi penting dari memonitoring dan menganalisa paket yang lewat di jaringan. Dalam hal ini, tingkat keamanan juga dapat dilihat dari proses komunikasi antara klien dan web server pada jaringan. Sehingga akan melakukan penyaringan paket data *address bar filter* dengan perintah **ip.addr ==**

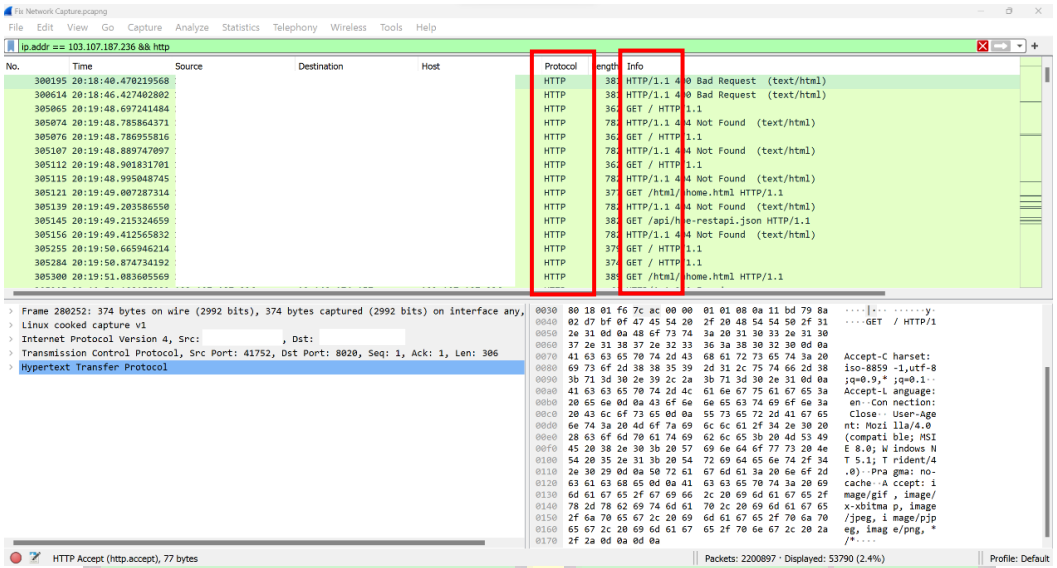
103.xx.xx.236 maka akan menampilkan paket data yang terfilter dari IP *address* tersebut.



Gambar IV.11 Hasil *Filter* Paket Data

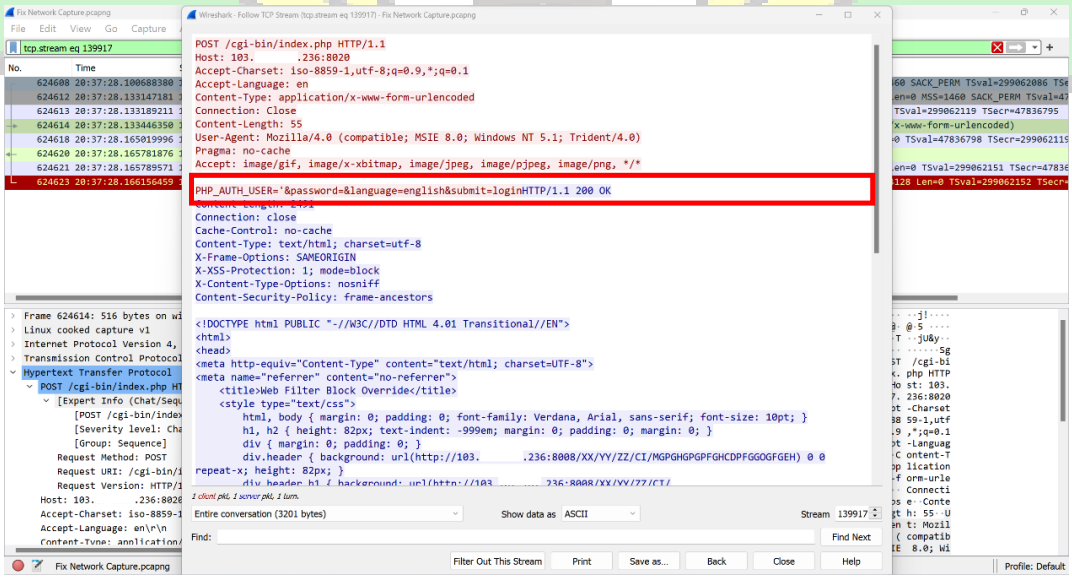
Pada Gambar IV.11 dapat dilihat bahwa seluruh paket data yang memiliki IP *address* 103.xx.xx.236 terdapat pada *Source* ataupun *Destination* yang saling bertukar tempat. Kemudian dapat dilihat juga warna dari paket data, paket yang warna hijau muda menunjukkan paket menggunakan protokol TCP pada *port* 80, paket yang berwarna abu gelap menunjukkan paket menggunakan protokol TCP untuk merespons permintaan mengirimkan segmen dengan *acknowledgment* dan juga SYN, paket yang berwarna abu muda menunjukkan paket menggunakan protokol TCP pada *port* 22, paket yang memiliki warna hitam dengan tulisan merah menandakan bahwa paket tersebut bermasalah dan paket data harus dikirim ulang, dan paket yang memiliki warna merah dengan tulisan kuning menandakan bahwa paket tersebut gagal pada koneksi TCP dengan *flag* RST yang dikirimkan sebagai *respons* dari *request*.

Dalam penelitian ini karena hanya menganalisis keamanan sistem informasi, maka akan dilakukan penyaringan dengan mengetik perintah **ip.addr == 103.xx.xx.236 && http** maka tampilan paket data dari protokol HTTP seperti pada Gambar IV.12.



Gambar IV.12 *Filter* Paket Data Protokol HTTP

Dari gambar diatas menunjukkan bahwa bagian bagian paket data yang di *filter* dari protokol HTTP. Hasil *filter* tersebut menunjukkan beberapa info seperti Get, HTTP/1.1, dan POST dengan sisa penyaringan protokol HTTP sebanyak 53790 paket. Dalam hal ini, untuk menganalisa paket data dengan memilih paket tersebut pada *listing packet panel* yang ingin dianalisis serta pilih *Follow* TCP *Stream*. Berikut tampilan paket data protokol HTTP yang berisi info POST.



Gambar IV.13 Hasil Paket Data POST

Pada Gambar IV.13 menunjukkan detail paket data protokol HTTP dengan teks berwarna merah bagian dari *request* sedangkan teks berwarna biru bagian dari

respons. Paket data POST tersebut mendapat informasi *key PHP_AUTH_USE*R=&*password=*&*language=english*&*submit=login* dari *form url encoded* serta menganalisis beberapa informasi sebagai berikut:

- POST

  Client melakukan permintaan dengan memanfaatkan badan pesan dalam mengirim data ke server web.
- HOST: 103.xxx.xxx.236

  Client sedang terhubung dengan IP *address* target.
- Connection: Close

  Parameter yang menjelaskan batas waktu koneksi.
- Content-Type: application/x-www-form-urlencoded

  Client mengirimkan data dengan *Form Uniform Resource Locator* (URL).
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

  Web browser yang dipakai oleh *client*.
- Accept-Language: en

  Bahasa yang dipakai oleh *web browser* bahasa inggris.
- HTTP/1.1 200 OK

  Dapat diketahui permintaan telah berhasil dilakukan

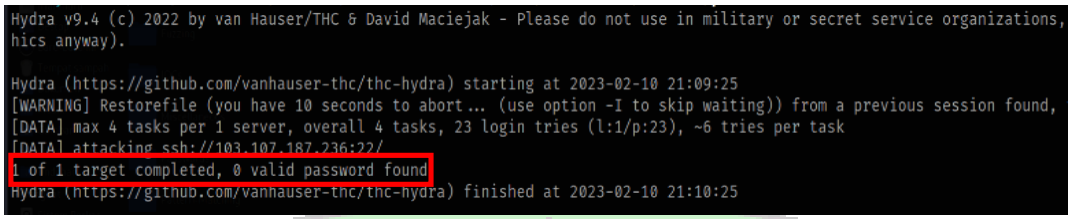
IV.3 *Attack*

Pada tahap ini merupakan tahapan inti yang ada dalam penelitian ini yang terdapat dalam metode NIST SP 800-115 untuk melakukan *penetration testing* terhadap hasil temuan yang diperoleh dari tahap *discovery*. Adapun kerentanan yang di uji sebagai berikut:

1. *Brute Force Attack*

Hasil dari pemindaian menggunakan NMAP terdapat *service* SSH yang berjalan pada *port* 22 untuk mencoba *brute force login* pada server melalui layanan SSH yang memungkinkan untuk melakukan serangan dan memperoleh informasi yang lebih akurat ke dalam sistem target. Dalam percobaan melakukan *brute force login* harus menyediakan asumsi berbagai *password* dan *username* secara acak untuk dilakukan *session* pencarian. Pada tahap ini peneliti mendapatkan *username*

dan *password* dengan cara pengumpulan informasi yang dilakukan pada objek penelitian serta penggunaan *username* dan *password* yang sering dipakai dapat dilihat pada Lampiran 2.

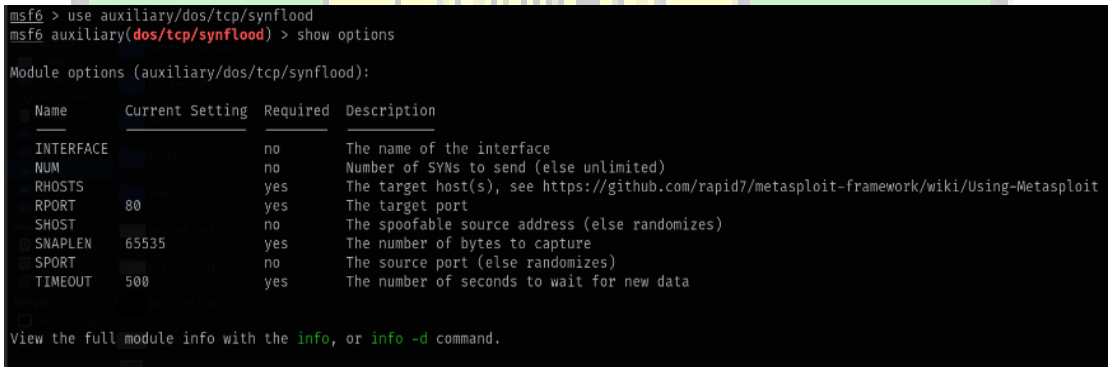


Gambar IV.14 *Brute Force Attack*

Dalam pencarian *username* dan *password* dengan melakukan pencarian secara bergantian terhadap beberapa asumsi *user* yang telah diberikan, tahap ini menggunakan hydra sebagai pencarian *username* dan *password* pada SSH server. Dari hasil pencarian tersebut menunjukkan 0 *valid password found* yang artinya tidak memperoleh hasil yang valid. Sehingga pengujian terhadap *brute force login* pada SSH tidak rentan.

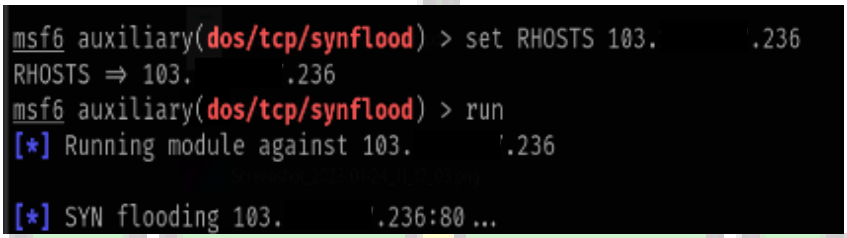
2. *Denial of Service SynFlood*

Eksploitasi *Denial of Service* (DoS) dengan mengimplementasikan eksploitasi Dos *SynFlood*. Dos *SynFlood* adalah serangan pada sebuah jaringan yang akan dibanjiri *fake traffic* sangat banyak. Hal ini server atau jaringan yang diserang akan tidak mampu menyediakan lalu lintas, sehingga menyebabkan sistem *down* serta tidak dapat beroperasi dengan baik. Pengujian ini menggunakan Metasploit *Framework* sebagai serangan DoS *SynFlood* dan penggunaan Wireshark untuk menganalisis detail lalu lintas jaringan pada saat proses eksploitasi DoS.



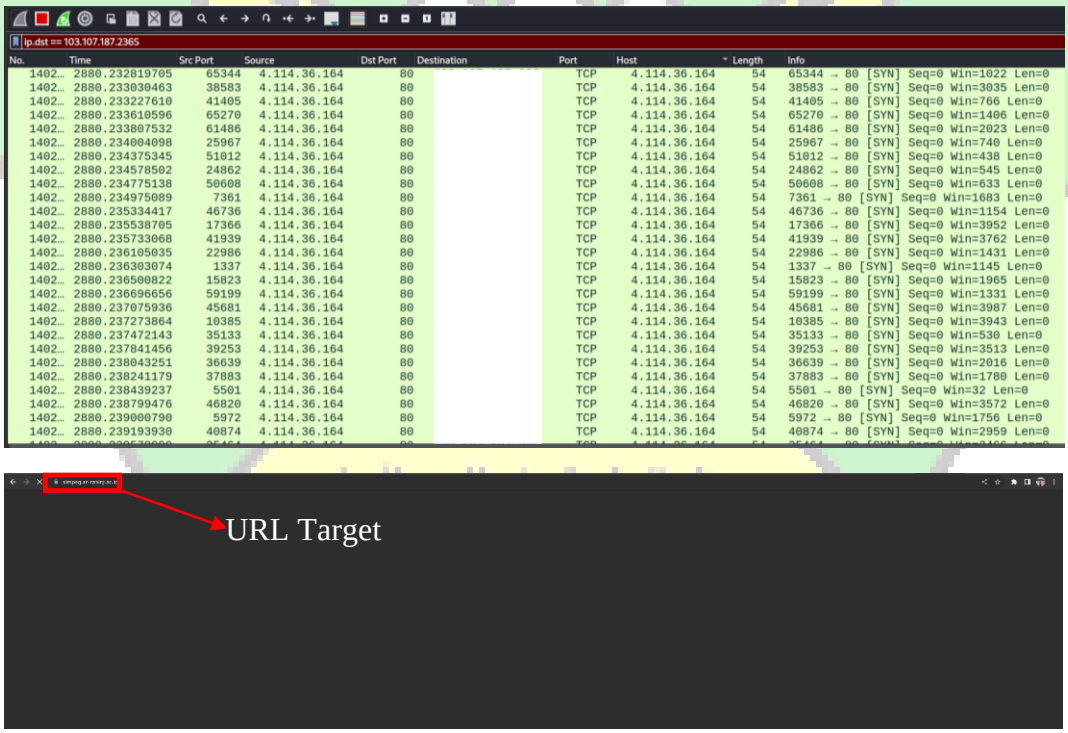
Gambar IV.15 Modul DoS *SynFlood*

Dari Gambar IV.15 akan dilakukan proses eksploitasi dengan Metasploit *Framework* yang sudah menyediakan *module* auxiliary untuk melakukan penyerangan dengan perintah ***use*** auxiliary/dos/tcp/synflood untuk masuk ke dalam modul tersebut. Namun, untuk mengetahui langkah penggunaan modul tersebut maka mengetik perintah *show options.*



Gambar IV.16 DoS *SynFlood*

Dari gambar di atas dapat dilihat sudah berhasil masuk ke dalam modul DoS *SynFlood*, dalam melakukan penyerangan diperlukan konfigurasi mulai dari input ***set*** *RHOSTS* 103.xx.xx.236 sebagai IP *address* target, dan *port* yang akan di serang. Maka dari itu diperlukan wireshark untuk merekam aktivitas paket data, tampilan dapat dilihat pada Gambar IV.17.



Gambar IV.17 *Capture* dan Efek DoS *SynFlood*

Dari efek DoS dapat diketahui hampir mustahil dapat diakses oleh pengguna dengan *traffic* yang dikirimkan secara terus-menerus yang membuat

sistem menjadi sibuk. Hal ini dengan banjirnya *traffic* membuat pengguna lain tidak dapat dilayani selama serangan berlangsung. Eksploitasi yang terjadi pada TCP dengan mengirimkan paket SYN dan *spoof* IP *address* sehingga koneksi yang masuk ditanggapi oleh server, namun koneksi tersebut tidak pernah berjalan. Sehingga mengakibatkan proses pada server melebihi kapasitas yang ditangani oleh server. Dengan demikian, penyerangan DoS dapat dilakukan pada target uji dengan menggunakan IP *Address* palsu untuk terhubung ke DNS target.

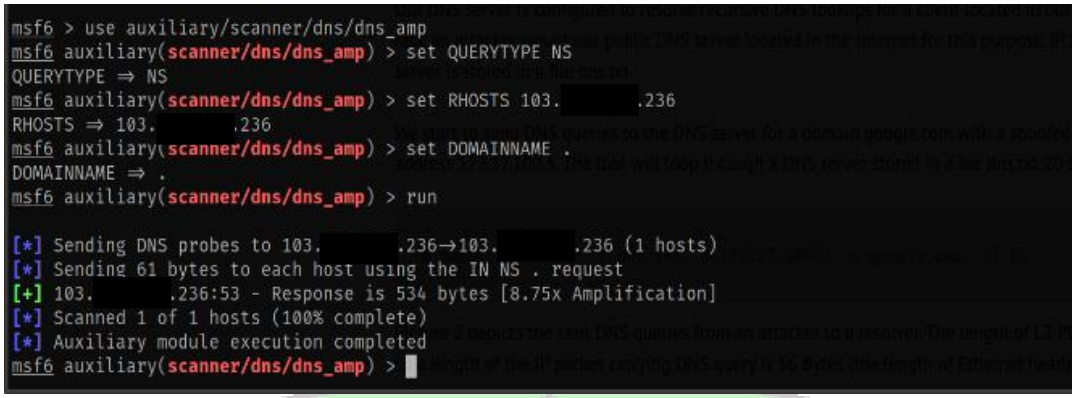
3. DNS Server *Request Amplification*

Eksploitasi DNS *amplification* bagian dari serangan *Distributed Denial of Service* (DDoS) di DNS server dengan mengubah *query* kecil menjadi muatan yang lebih besar untuk membuat server *down*. Pengujian ini menggunakan Metasploit *Framework* sebagai serangan DNS *amplification*.

```
msf6 > use auxiliary/scanner/dns/dns_amp
msf6 auxiliary(scanner/dns/dns_amp) > show options

Module options (auxiliary/scanner/dns/dns_amp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to probe in each set
   DOMAINNAME  isc.org          yes       Domain to use for the DNS request
   FILTER                       no        The filter string for capturing traffic
   INTERFACE                    no        The name of the interface
   PCAPFILE                     no        The name of the PCAP capture file to process
   QUERYTYPE   ANY              yes       Query type(A, NS, SOA, MX, TXT, AAAA, RRSIG, DNSKEY, ANY)
   RHOSTS                       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Us
                                          ing-Metasploit
   RPORT       53               yes       The target port (UDP)
   SNAPLEN     65535            yes       The number of bytes to capture
   THREADS     10               yes       The number of concurrent threads
   TIMEOUT     500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.
```

Gambar IV.18 Modul DNS *Amplification*

Proses eksploitasi dari *module* auxiliary untuk melakukan penyerangan dengan perintah ***use*** auxiliary/scanner/dns/dns_amp untuk masuk ke dalam modul tersebut. Dalam penggunaan modul dibutuhkan konfigurasi untuk melakukan penyerangan dengan mengetik perintah *show options* akan menampilkan langkah konfigurasi yang diperlukan seperti pada Gambar IV.18.



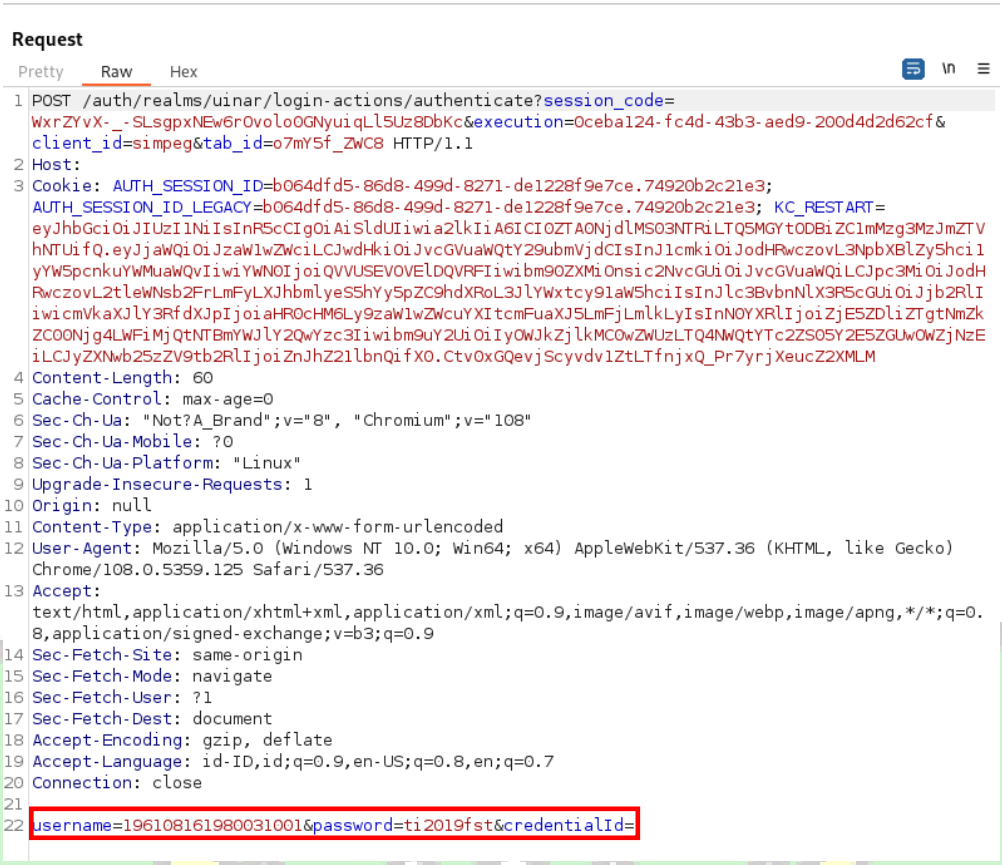
Gambar IV.19 DNS *Amplification*

Dari Gambar IV.19 dapat dilihat bahwa sudah berhasil masuk ke dalam modul DNS Amp, untuk melakukan penyerangan diperlukan konfigurasi mulai dari *query type* yang diatur ialah Name Server (NS) yang dapat dilakukan pada kerentanan ini dengan input ***set*** *QUERYTYPE* NS, kemudian mengatur IP *address* target dengan input ***set*** *RHOSTS* 103.xx.xx.236, selanjutnya akan mengatur *domain name* dengan DNS *Root* Server untuk memperoleh puncak hirarki dari *root zone* dengan input ***set*** *DOMAINNAME* **.**, dan kerentanan ini berfokus pada DNS maka *port* yang diatur ialah 53.

Hasil dari DNS *amplification* dapat dilihat pengiriman *request* dengan panjang paket data 64 *bytes* terhadap target uji, lalu server merespon dengan panjang paket data 8.75x *Amplification* yaitu 534 *bytes*. Sehingga penyerangan yang dilakukan berhasil melakukan *remote name server query*.

4. *Interception Attack*

Hasil dari *sniffing* wireshark dan penggunaan protokol keamanan komunikasi SSL/TLS versi lama dicurigai adanya kebocoran informasi pada *form url encoded* yang telah memperoleh *key* dan tidak ditemui informasi sensitif disebut juga sebagai *Cleartext Logins Permitted*. Dalam hal ini, dilakukan pengujian menggunakan *tool* BurpSuite sebagai percobaan *interception*. *Interception* adalah suatu ancaman terhadap kerahasian yang didapatkan secara tidak sah untuk mengakses informasi dari sistem komputer. Penyerangan yang dilakukan untuk mengetahui apakah terdapat komunikasi yang tidak terenkripsi dengan baik oleh SSL/TLS sehingga menimbulkan masalah kebocoran informasi.



Gambar IV.20 *Interception Attack*

Pada Gambar IV.20 dapat dilihat bahwa eksploitasi terjadi pada saat proses *request login* ke dalam sistem. Hasil dari *interception* dengan *tool* BurpSuite memperlihatkan informasi sensitif berupa *username* dan *password* pada saat proses *request login* yang tidak terenkripsi. Dengan demikian, penyerang akan sangat mudah eksplor ketika mendapat informasi berupa *username* dan *password*.

Pengujian yang telah dilakukan pada target 103.xx.xx.236 akan direpresentasikan menggunakan *Common Vulnerability Scoring System* (CVSS) dengan memperoleh 10 sistem yang berhasil terdeteksi dapat mengakibatkan data atau sistem dieksploitasi yang disebabkan oleh kelemahan pada server tersebut. Adapun hasil analisis kerentanan dapat dilihat pada Tabel IV.6.

Tabel IV.6 Hasil Analisis Kerentanan

No	*Vulnerability*	Vektor String	*Base Score*	*Threat Level*
1	DNS Server *Spoofed Request Amplification* DDoS	CVSS:3.0 /AV:N/AC:L/PR:N/UI:N /S:U/C:N/I:N/A:H	7.5	*High*
2	*Interception Attack*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N	7.5	*High*
3	TLS *Version* 1.0 *Protocol Detection*	CVSS:3.0/AV:N/AC:H/P R:N/UI:N/S:U/C:H/I:L/A :N	6.5	*Medium*
4	TLS *Version* 1.1 *Protocol Detection*	CVSS:3.0/AV:N/AC:H/P R:N/UI:N/S:U/C:H/I:L/A :N	6.5	*Medium*
5	SSL *Certificate Cannot Be Trusted*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:L/I:L/A :N	6.5	*Medium*
6	SSL *Certificate Expiry*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/A :N	5.3	*Medium*
7	SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:L/I:N/A :N	5.3	*Medium*
8	Nginx < *1.17.7 Information Disclosure*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:L/I:N/A :N	5.3	*Medium*
9	DNS Server *Recursive Query Cache Poisoning Weakness*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/A :N	5.3	*Medium*
10.	*Brute Force Attack*	CVSS:3.0/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:N	0.0	*None*

Pada hasil analisis *Interception attack* melalui *Common Vulnerability Scoring System* (CVSS) yang memperoleh *threat level high* dengan *base score* 7.5. Dalam hal ini, dikarenakan pada *Attack Vektor* menunjukkan teknis dalam mengeksploitasi kerentanan, pada penilaian kerentanan akan dilihat seberapa jauh kemampuan penyerang untuk masuk ke dalam sistem yang menandakan *Network*

(N) dapat menyerang sistem melalui jaringan dengan mudah, namun akan berbeda jika *metrics value* menandakan *Adjacent* (A) dengan *base score* 6.5 yang termasuk dalam *threat level medium*, demikian juga jika *metrics value* menandakan *Local* (L) dengan *base score* 6.2 yang termasuk dalam *threat level medium* dan *metrics value Physical* (P) memperoleh *base score* 4.6 yang berarti *threat level medium*.

Selanjutnya *Attack Complexity* (AC) kondisi yang berpengaruh pada tingkat kerentanan disebabkan menandakan *Low* (L) yang tidak mempunyai kondisi khusus serangan ketika penyerangan mendapatkan akses pada sistem dengan mudah. Artinya semakin rendah kompleksitas yang dibutuhkan maka semakin tinggi *base score* kerentanannya, begitu juga pada *Privileges Required* (PR) yang berfungsi sebagai penentuan nilai tingkat hak istimewa/akses yang dimiliki penyerang sebelum berhasil mengeksploitasi kerentanan yang terdapat pada sistem menandakan *metrics value None* (N) dengan ini penyerang mampu mengeksploitasi sistem sehingga *base score* mencapai 7.5 yang termasuk dalam *threat level high*.

Pada *User Interaction* komponen penilaian persyaratan pengguna jika menandakan *metrics value None* (N) yang berarti dapat dieksploitasi tanpa memerlukan interaksi pengguna lain, hal ini jika menandakan *metrics value Required* (R) termasuk ke dalam tingkat keamanan lebih kuat karena penyerang atau pengguna lain yang berkaitan dengan komponen rentan. Sehingga tingkat kerentanan akan lebih tinggi ketika tidak akan interaksi pengguna lain. Kemudian pada *Scope* (S) akan mempengaruhi terhadap dampak dari perubahan kerentanan yang terjadi, jika menandakan *metrics value Unchanged* (U) memberikan tidak ada cakupan keamanan yang berdampak pada perubahan komponen rentanan, namun jika menandakan *metrics value Changed* (C) artinya tingkat kerentanan yang dimiliki sangat rawan dilakukan perubahan oleh penyerang. Dengan demikian, dampak dari eksploitasi komponen rentan dapat terjadi berupa *confidentiality*, *integrity*, dan *availability* hal ini sangat berpengaruh pada tingkat kerentanan dikarenakan menandakan *metrics value None* (N) yang berarti serangan yang dilakukan penyerang tidak mempengaruhi dampak dari aspek keamanan informasi sehingga menandakan tidak memiliki komponen rentan, namun jika menandakan *metrics value Low* (L) dengan *base score* 5.3 yang termasuk dalam *threat level*

medium dan *metrics value High* (H) memperoleh *base score* 7.5 yang berarti *threat level high*.

IV.4 *Reporting*

Tahap akhir penelitian ini menganalisis hasil kerentanan yang teridentifikasi. Pada tahap *reporting*, selain menganalisis hasil, juga memberikan rekomendasi tentang cara mengatasi kelemahan yang ditemukan. Namun, untuk mempermudah dalam melihat keseluruhan temuan kerentanan yang diakibatkan dari kegagalan *confidentiality*, *integrity*, dan *availability* sebagai berikut:

1. Kegagalan *Confidentiality*

Tabel IV.7 Hasil Uji Kegagalan *Confidentiality*

No	*Vulnerability*	Rekomendasi	*Base Score*	*Threat Level*
1	*Interception Attack*	Memperbaiki enkripsi lalu lintas dengan SSL/TLS menggunakan stunnel.	7.5	*High*
2	SSL *Certificate Cannot Be Trusted*	Memperbaharui sertifikat SSL.	6.5	*Medium*
3	TLS *Version* 1.0 *Protocol Detection*	Nonaktifkan TLS 1.0 dengan mengaktifkan TLS 1.2 dan 1.3.	6.5	*Medium*
4	TLS *Version* 1.1 *Protocol Detection*	Nonaktifkan TLS 1.1 dengan mengaktifkan TLS 1.2 dan 1.3	6.5	*Medium*
5	Nginx < 1.17.7 *Information Disclosure*	Memperbaharui server nginx ke versi 1.17.7	5.3	*Medium*
6	SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure*	Konfigurasi SSL/TLS server hanya menggunakan TLS 1.2 dan 1.3	5.3	*Medium*
Rata-Rata Skor Kerentanan			6.3	*Medium*

2. Kegagalan *Integrity*

Tabel IV.8 Hasil Uji Kegagalan *Integrity*

No	*Vulnerability*	Rekomendasi	*Base Score*	*Threat Level*
1	DNS Server *Recursive Query Cache Poisoning Weakness*	Membatasi *query* rekursif ke *host* yang menggunakan nama server dengan mengelompokkan alamat internal.	5.3	*Medium*
2	SSL *Certificate Expiry*	Memperbaharui sertifikat SSL.	5.3	*Medium*
Rata-Rata Skor Kerentanan			5.3	*Medium*

3. Kegagalan *Availability*

Tabel IV.9 Hasil Uji Kegagalan *Availability*

No	*Vulnerability*	Rekomendasi	*Base Score*	*Threat Level*
1	DNS Server *Spoofed Request Amplification* DDoS	Membatasi akses DNS server dari jaringan publik ataupun konfigurasi ulang menolak *query* tersebut.	7.5	*High*

Dari perhitungan rata-rata hasil pengujian kerentanan yang disebabkan oleh kegagalan *confidentiality*, *integrity*, dan *availability*, dapat diketahui bahwa Sistem Informasi Manajemen Kepegawain Universitas Islam Negeri Ar-Raniry memiliki tingkat keparahan kerentanan 6.4 yang tergolong ke dalam *threat level medium*.

BAB V
PENUTUP

V.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut:

1. Pengujian penilaian keamanan server terhadap Sistem Informasi Manajemen Kepegawaian pada Universitas Islam Negeri Ar-Raniry menggunakan metode NIST 800-115 dengan teknik pengujian *black box testing* untuk mencari informasi dan kerentanan pada target yang meliputi tahapan sebagai berikut:
   a. *Planning*
   b. *Discovery*
   c. *Attack*
   d. *Reporting*
2. Kerentanan yang diperoleh dari hasil pengujian adalah ditemukan 9 kerentanan yang dapat dieksploitasi dengan rincian 2 kerentanan yang berada dalam *threat level high* yaitu:
   a. DNS Server *Spoofed Request Amplification* DDoS, dapat melakukan DDoS pada bagian *query* Name Server (NS).
   b. *Interception Attack*, penyerang dapat membaca informasi sensitif melalui lalu lintas jaringan sistem. Kemudian juga terdapat 7 kerentanan yang berada dalam *threat level medium* yaitu:
   a. TLS *Version* 1.0 *Protocol Detection*, terdeteksi menggunakan protokol keamanan versi lama.
   b. TLS *Version* 1.1 *Protocol Detection*, terdeteksi menggunakan protokol keamanan versi lama.
   c. SSL *Certificate Cannot Be Trusted*, terjadi akibat rantai sertifikat SSL telah kadaluarsa.
   d. SSL *Certificate Expiry*, terjadi akibat rantai sertifikat SSL telah kadaluarsa.

e. SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure*, terjadi pengungkapan informasi sensitif yang diakibatkan oleh TLS 1.0 di dalam sistem.
f. Nginx < 1.17.7 *Information Disclosure*, terdeteksi menggunakan web server lama versi 1.14.2.
g. DNS Server *Recursive Query Cache Poisoning Weakness*, mengizinkan *query recursive Name* Server (NS).

3. Dari temuan kerentanan yang telah diperoleh maka mempunyai cara perbaikan yang berbeda-beda pula. Adapun rekomendasi sebagai berikut:
   a. DNS Server *Spoofed Request Amplification* DDoS yaitu dengan membatasi akses DNS server dari jaringan publik ataupun konfigurasi ulang menolak *query* tersebut.
   b. *Interception Attack* yaitu dengan memperbaiki protokol SSL/TLS menggunakan stunnel.
   c. TLS *Version* 1.0 *Protocol Detection* yaitu dengan menonaktifkan protokol TLS versi 1.0 dengan mengaktifkan protokol TLS versi 1.2 dan versi 1.3.
   d. TLS *Version* 1.1 *Protocol Detection* yaitu dengan menonaktifkan protokol TLS versi 1.1 dengan mengaktifkan protokol TLS versi 1.2 dan versi 1.3.
   e. SSL *Certificate Cannot Be Trusted* yaitu dengan melakukan pembaharuan sertifikat SSL.
   f. SSL *Certificate Expiry* yaitu dengan melakukan pembaharuan sertifikat SSL.
   g. SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure* yaitu dengan melakukan konfigurasi SSL/TLS server hanya menggunakan TLS 1.2 dan 1.3.
   h. Nginx < 1.17.7 *Information Disclosure* yaitu dengan melakukan pembaharuan pada server Nginx menjadi versi 1.17.7.
   i. DNS Server *Recursive Query Cache Poisoning Weakness* yaitu dengan membatasi *query* rekursif ke *host* yang menggunakan nama server dengan mengelompokkan alamat internal.

Dengan demikian, Sistem Informasi Manajemen Kepegawain Universitas Islam Negeri Ar-Raniry memiliki tingkat keparahan kerentanan 6.4 yang tergolong ke dalam *threat level medium*. Dalam hal ini, peneliti hanya memberikan rekomendasi untuk melakukan perbaikan terhadap kerentanan yang ditemukan. Penerapan dari rekomendasi perbaikan kerentanan akan diserahkan sepenuhnya kepada pihak instansi Universitas Islam Negeri Ar-Raniry.

V.2 Saran

Berdasarkan kesimpulan dan analisis yang telah dilakukan, diperlukan pengujian dan pengembangan lebih lanjut mengenai penilaian keamanan server. Berikut adalah saran pada penelitian ini:

1. Proses pengujian selanjutnya dapat melakukan penyelidikan keamanan secara proaktif dengan menambah metode *threat hunting life cycle*.
2. Dengan ditemukan kerentanan pada tahapan pelaporan maka disarankan kepada instansi terkait untuk dapat melakukan proses evaluasi keamanan terhadap server yang memuat sistem informasi tersebut. Hal ini bertujuan untuk memastikan tindakan pengamanan sistem tetap terjaga. Namun demikian juga dapat berpedoman pada publikasi NIST 800-44 tentang pengamanan publik server web.

DAFTAR PUSTAKA

Astriani, T., Budiyono, A., Widjajarto, A., Informasi, J. S., Rekayasa, F., & Universitas, I. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar NIST 800-115. *Jurnal Teknik Informatika dan Sistem Informasi*, *8*(4), 2041–2050.

Aziz, M. (2021). Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz. *Jecsit*, *1*(1), 101–109.

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. CRC Press.

Cardwell, K. (2016). *Building Virtual Pentesting Labs for Advanced Penetration Testing*. Packt Publishing Ltd.

Cisar, P., & Pinter, R. (2019). Journal of Applied Technical and Educational Sciences jATES Some ethical hacking possibilities in Kali Linux environment. *Journal of applied tehnical and educational sciences jATES*, *9*(4), 129–149. http://doi.org/10.24368/jates.v9i4.139http://jates.org

Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver menggunakan Penetration Test. *Jurnal Informatika*, *8*(2), 183–190. https://doi.org/10.31294/ji.v8i2.10854

FIRST. (2019). *Common Vulnerability Scoring System*. 1–24. https://www.first.org/cvss/

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Hanifah, F., Budiyono, A., & Widjajarto, A. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan Framework CIS Control. *e-Proceeding of Engineering*, *8*(5), 8879–8885. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/

article/view/15914

Hussain, M. Z., Hasan, M. Z., Taimoor, M., & Chughtai, A. (2017). Penetration Testing In System Administration. *International Journal of Scientific & Technology Research*, *6*(6), 275–278.

Kasau, M. I., Aminah, S. T., Ghani, D., Liklikwatil, R. D., Lldikti, D., Dpk, I. X., Makassar, D., & Makassar, U. D. (2021). Sistem Keamanan " Pesan " Berbasis Pretty Good Privacy. *SISITI: Seminar Ilmiah Sistem …*, *X*(1), 108–116. http://ejurnal.dipanegara.ac.id/index.php/sisiti/article/view/793

Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal of Information Engineering and Educational Technology*, *5*(1), 34–39. https://doi.org/10.26740/jieet.v5n1.p34-39

Marta, I. K. K. A., Hartawan, I. N. B., & Satwika, I. K. S. (2020). Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort. *INSERT : Information System and Emerging Technology Journal*, *1*(1), 25. https://doi.org/10.23887/insert.v1i1.25874

Prakoso, D. C. (2019). *Investigasi Forensik RAM untuk Mendeteksi Serangan Exploit Framework Metasploit*. Universitas Islam Indonesia.

Prasetio, N. (2017). Sistem Informasi Penyewaan Kendaraan Berbasis Web (Studi Kasus Chandra Trans Bali). *Jurnal Ilmiah Methonomi*, *3*(2), 28–29.

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Ratna Patria. (2022, Juni 15). *Memahami Apa Itu Ping dan Fungsinya Saat Jaringan Internet Lambat - DomaiNesia*. https://www.domainesia.com/berita/ping-adalah/

Rochmadi, T., & Pasa, I. Y. (2021). *Menggunakan Indeks Keamanan Informasi Di Bkd Xyz Measurement of Risk and Evaluation of Information Security Using the Information Security Index in Bkd Xyz Based on Iso 27001 / Sni*. *4*(1), 38–43.

Rusdiana, M. (2014). Sistem Informasi Manajemen. *Sistem Informasi Manajemen*, 1–387.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *8*(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05

Setiawan, M. F., Saedudin, R. R., & ... (2022). Penutupan Celah Keamanan Menggunakan Metode Hardening Studi Kasus: Cloudfri Closing Security Vocations Using The Hardening Method Case Study: Cloudfri. *e-Proceeding of Engineering*, *9*(2), 656–663. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17635%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17635/17379

Sslscan. (2022, Agustus 5). *sslscan | Kali Linux Tools*. https://www.kali.org/tools/sslscan/

Tan, T., & Soewito, B. (2022). *MENGGUNAKAN FRAMEWORK NIST CYBERSECURITY DI UNIVERSITAS ZXC*. *6*(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781

Tidy J. (2020). *How hackers extorted $1.14m from University of California, San Francisco*. https://www.bbc.com/news/technology-53214783

Utami, M. P. (2017). *Efektivitas Sistem Informasi Manajemen Kepegawaian (Simpeg) Di Badan Pendidikan Dan Pelatihan Pemerintah Provinsi Bali* [Universitas Warmadewa]. http://repository.warmadewa.ac.id/id/eprint/276

van den Hout, N. J. (2019). *Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies*. *August*, 70.

Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, *5*(1). https://doi.org/10.32672/jnkti.v5i1.3962

Wardana, W., Almaarif, A., & Widjajarto, A. (2022). Vulnerability Assessment And Penetration Testing On The XYZ Website Using Nist 800-115 Standard.

Jurnal Ilmiah Indonesia, *7*(8.5.2017), 2003–2005.

Wardaya, M. S. S. (2019). Penetration Testing terhadap Website Asosiasi Pekerja Profesional Informasi Sekolah Indonesia (APISI). In *Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta* (Vol. 8, Nomor 5). http://repository.uinjkt.ac.id/dspace/handle/123456789/48282

LAMPIRAN

Lampiran 1 Pengujian Nessus

Search History | 12 Histories

Start Time	Last Scanned	Status
January 28 at 3:10 PM	January 28 at 3:57 PM	Completed
January 21 at 12:45 PM	January 21 at 2:04 PM	Completed
January 15 at 9:50 PM	January 15 at 10:29 PM	Completed
January 15 at 9:14 PM	January 15 at 9:47 PM	Completed
January 8 at 10:41 PM	January 8 at 10:51 PM	Completed
January 8 at 10:11 PM	January 8 at 10:20 PM	Completed
January 8 at 8:06 PM	January 8 at 8:53 PM	Completed
January 2 at 11:48 PM	January 3 at 12:06 AM	Completed
January 2 at 9:48 PM	January 2 at 10:41 PM	Completed
January 2 at 7:56 PM	January 2 at 8:52 PM	Completed
Current 2022-12-29 at 10:31 PM	2022-12-29 at 10:39 PM	Completed
2022-12-29 at 9:04 PM	2022-12-29 at 9:21 PM	Completed

Gambar 1.1 Bukti Pengujian Nessus

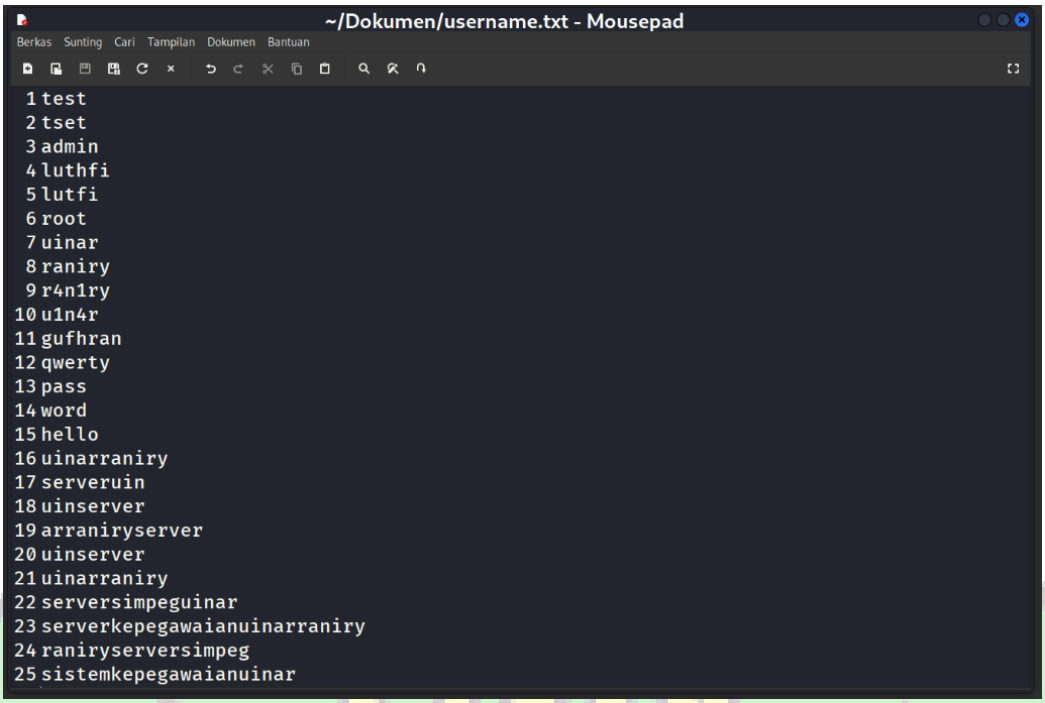
Filter | Search Vulnerabilities | 50 Vulnerabilities

Sev	Score	Name	Family	Count
HIGH	7.5	DNS Server Spoofed Request Amplification DDoS	DNS	1
MEDIUM	6.5	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	6.5	TLS Version 1.1 Protocol Deprecated	Service detection	1
MEDIUM	5.3	nginx < 1.17.7 Information Disclosure	Web Servers	1
MEDIUM	5.3	SSL Certificate Expiry	General	1
MEDIUM	5.3	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	General	1
MEDIUM	5.0 *	DNS Server Recursive Query Cache Poisoning Weakness	DNS	1
INFO		Nessus SYN scanner	Port scanners	8
INFO		Service Detection	Service detection	6
INFO		HTTP Methods Allowed (per directory)	Web Servers	3
INFO		HyperText Transfer Protocol (HTTP) Information	Web Servers	3
INFO		Web Server No 404 Error Code Check	Web Servers	2
INFO		Common Platform Enumeration (CPE)	General	1
INFO		Deprecated SSLv2 Connection Attempts	General	1
INFO		Device Type	General	1
INFO		DNS Server Detection	DNS	1
INFO		DNS Server UDP Query Limitation	DNS	1

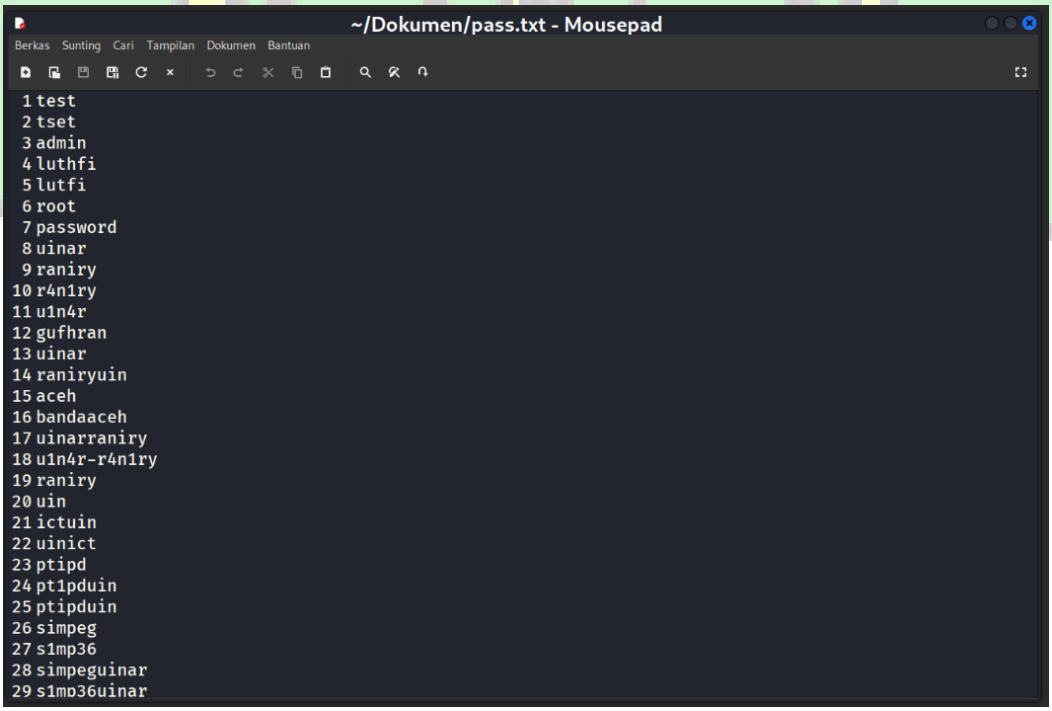
INFO	DNS Server UDP Query Limitation	DNS	1	
INFO	HTTP Server Type and Version	Web Servers	1	
INFO	HyperText Transfer Protocol (HTTP) Redirect Information	Web Servers	1	
INFO	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	CGI abuses	1	
INFO	Nessus Scan Information	Settings	1	
INFO	nginx HTTP Server Detection	Web Servers	1	
INFO	OpenSSL Detection	Service detection	1	
INFO	OS Identification	General	1	
INFO	OS Security Patch Assessment Failed	Settings	1	
INFO	Patch Report	General	1	
INFO	Reverse NAT/Intercepting Proxy Detection	Firewalls	1	
INFO	SSH Algorithms and Languages Supported	Misc.	1	
INFO	SSH Password Authentication Accepted	Service detection	1	
INFO	SSH Protocol Versions Supported	General	1	
INFO	SSH Server Type and Version Information	Service detection	1	
INFO	SSH SHA-1 HMAC Algorithms Enabled	Misc.	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	
INFO	SSL/TLS Recommended Cipher Suites	General	1	
INFO	Target Credential Status by Authentication Protocol - Failure for Provided Credentials	Settings	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	TLS ALPN Supported Protocol Enumeration	Misc.	1	
INFO	TLS Next Protocols Supported	General	1	
INFO	TLS NPN Supported Protocol Enumeration	Misc.	1	
INFO	TLS Version 1.1 Protocol Detection	Service detection	1	
INFO	TLS Version 1.2 Protocol Detection	Service detection	1	
INFO	Traceroute Information	General	1	
INFO	Web Application Sitemap	Web Servers	1	

Gambar 1.2 Hasil *Vulnerability Scanning*

Lampiran 2 Pengujian Brute Force Attack



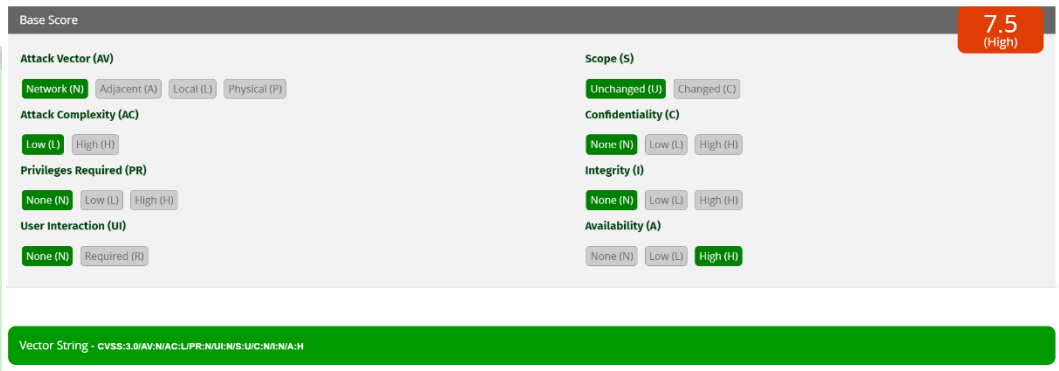
Gambar 2.1 File Username



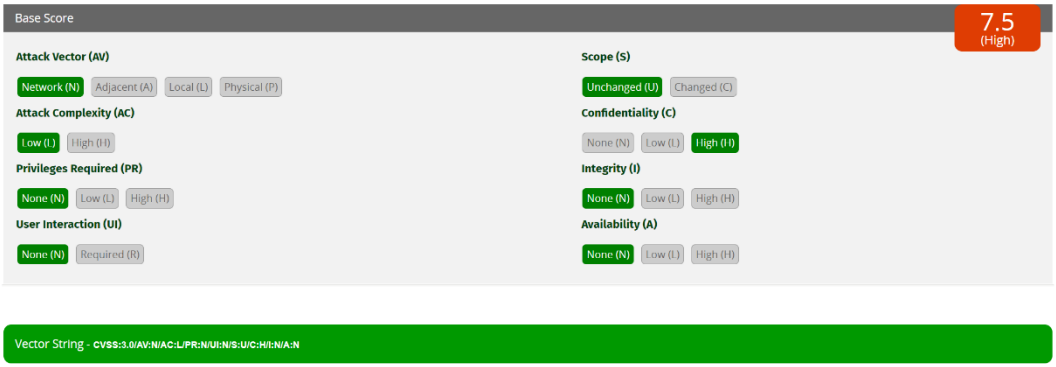
```
30 ranirysimpeg
31 uinarsimpeg
32 kepegawaianuinar
33 ranirypegawai
34 serverdatauinar
35 dataserverranirysimpeg
36 bnauinarserver
37 sistemkepegawaianuinar
38 sistemuiar
39 arranirykepegawaian
40 serveruin123
41 uinranirysimpeg
42 12345678
43 54321arraniry
44 321simpeguinar
45 !serversimpeg
46 serversimpeguinarraniry!
47 serversimpeguinarraniry?
48 passserversimpegraniry321!
49 uinardatapegawaisimpegsistem
50 kepegawaiansistemar-raniry
```

Gambar 2.2 *File Password*

Lampiran 3 Pengukuran Kerentanan CVSS



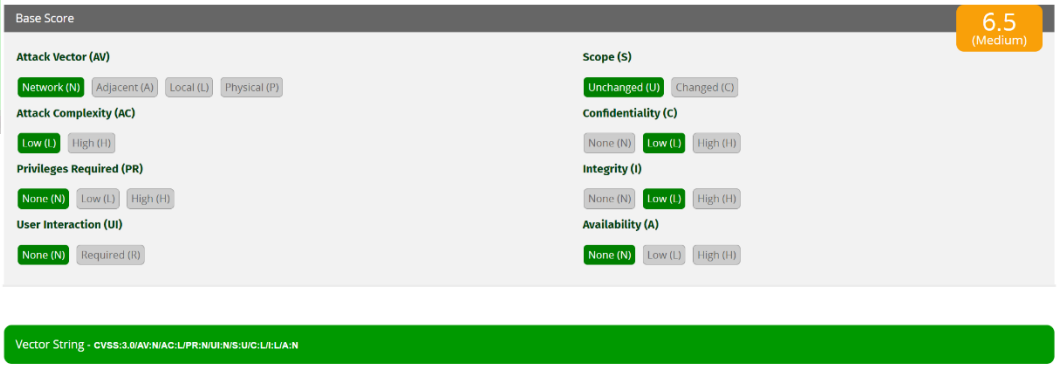
Gambar 3.1 DNS Server *Spoofed Request Amplification* DDoS



Gambar 3.2 *Interception Attack*

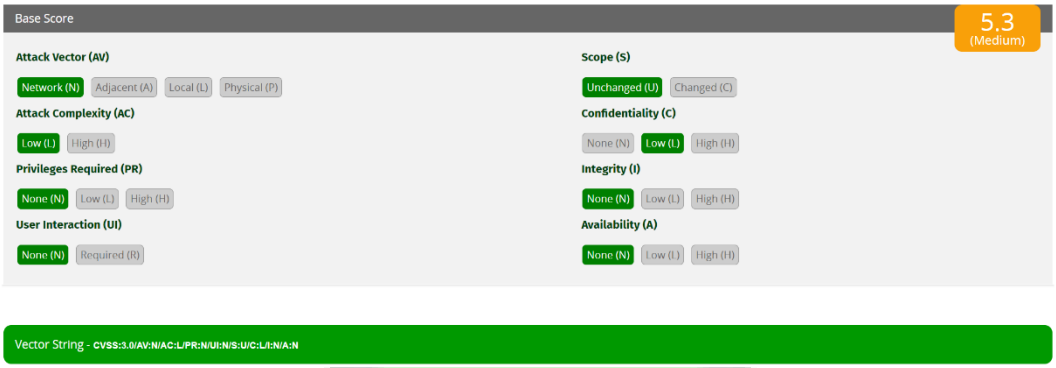
Gambar 3.3 TLS *Version* 1.0 *Protocol Detection*

Gambar 3.4 TLS *Version* 1.1 *Protocol Detection*

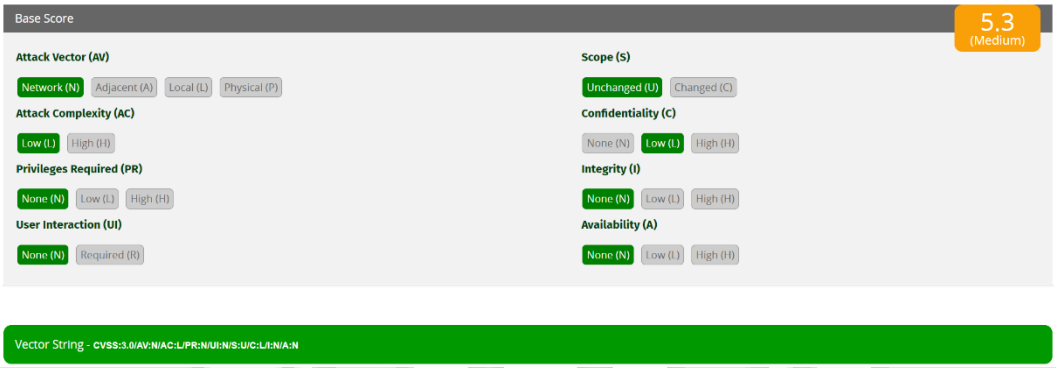


Gambar 3.5 SSL *Certificate Cannot Be Trusted*

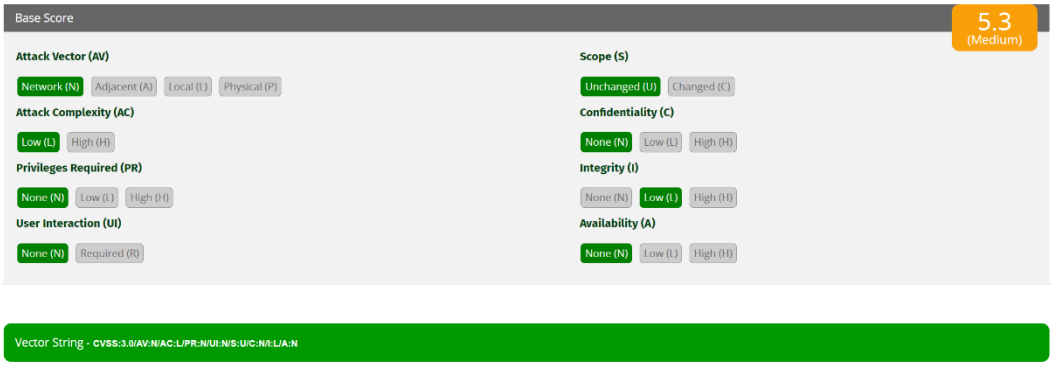
Gambar 3.6 SSL *Certificate Expiry*



Gambar 3.7 SSL/TLS *Protocol Initialization Vector Implementation Information Disclosure*



Gambar 3.8 CVSS Nginx > 1.17.7 *Information Disclosure*



Gambar 3.9 DNS Server *Recursive Query Cache Poisoning Weakness*

RIWAYAT PENULIS

Irfan Murti Raazi, lahir di Banda Aceh pada tanggal 03 Mei 2001. Menyelesaiakn pendidikan formal di MIN Lambhuk Banda Aceh pada tahun 2013. Kemudian melanjutkan sekolah menengah pertama di SMPN 6 Banda Aceh tamat pada tahun 2016. Selanjutnya penulis melanjutkan sekolah menengah atas pada SMAN 12 Banda Aceh dan lulus pada tahun 2019. Pada tahun yang sama penulis terdaftar sebagai salah satu mahasiswa di Prodi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Ar-Raniry Banda Aceh melalui jalur seleksi SNMPTN. Selama Selama menjadi mahasiswa, penulis mampu menerbitkan 3 (tiga) jurnal riset sains dan teknologi yang bekerjasama dengan dosen ataupun mahasiswi Prodi Teknologi Informasi dengan fokus penelitian di bidang sistem keamanan informasi serta juga aktif berorganisasi di Himpunan Mahasiswa Teknologi Informasi (HIMA-TI) dengan jabatan ketua divisi minat dan bakat dan bendahara umum.