



**ANALISIS KEAMANAN SISTEM INFORMASI UNTUK  
MENGETAHUI KERENTANAN KEAMANAN *SERVER* DENGAN  
METODE *PENETRATION TESTING EXECUTION STANDARD*  
(PTES) PADA UNIVERSITAS VWX**

**SKRIPSI**

**ALVITA IZANA KUSUMARINI**

**1710511019**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**FAKULTAS ILMU KOMPUTER**

**PROGRAM STUDI INFORMATIKA**

**2021**



**ANALISIS KEAMANAN SISTEM INFORMASI UNTUK MENGETAHUI  
KERENTANAN KEAMANAN *SERVER* DENGAN METODE  
*PENETRATION TESTING EXECUTION STANDARD (PTES)* PADA  
UNIVERSITAS VWX**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar  
Sarjana Komputer**

**ALVITA IZANA KUSUMARINI**

**1710511019**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**FAKULTAS ILMU KOMPUTER**

**PROGRAM STUDI INFORMATIKA**

**2021**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Alvita Izana Kusumarini

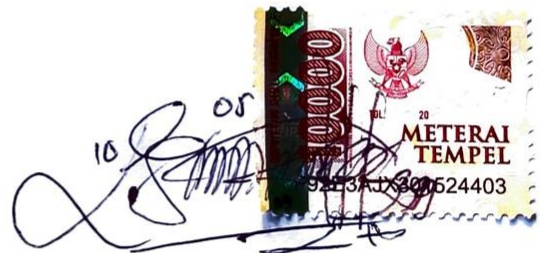
NIM : 1710511019

Tanggal : 2 Juli 2021

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 2 Juli 2021

Yang menyatakan,

A handwritten signature in black ink is written over a 2000 Indonesian postage stamp. The stamp features the Garuda Pancasila emblem and the text '2000 METERAI TEMPEL' and '944341800524403'. The signature includes the numbers '10' and '05' written above it.

Alvita Izana Kusumarini

## PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Alvita Izana Kusumarini

NIM : 1710511019

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (Non-exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

*Analisis Keamanan Sistem Informasi Untuk Mengetahui Kerentanan Keamanan Server*

*Dengan Metode Penetration Testing Execution Standard (PTES) Pada Universitas VWX*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 14 Juli 2021

Yang Menyatakan,



(Alvita Izana Kusumarini)

## LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

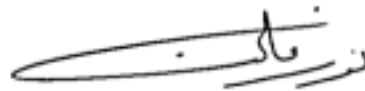
Nama : Alvita Izana Kusumarini  
NIM : 1710511019  
Program Studi : Informatika  
Judul Tugas Akhir : Analisis Keamanan Sistem Informasi Untuk Mengetahui  
Kerentanan Keamanan *Server* Dengan Metode *Penetration  
Testing Execution Standard (PTES)* Pada Universitas VWX

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Yuni Widiastiwi, S.Kom., M.Si

Penguji I



Noor Falih, S.Kom., M.T

Penguji II



Henki Bayu Seta, S.Kom., MTI

Pembimbing I



Ing. Artambo B. Pangaribuan, B.Sc

Pembimbing II



Dr. Ermatita, M.Kom

Dekan

Ditetapkan di : Jakarta

Tanggal Persetujuan : 21 Juli 2021



Yuni Widiastiwi, S.Kom., M.Si

Ketua Program Studi



**Analisis Keamanan Sistem Informasi Untuk Mengetahui Kerentanan  
Keamanan Server Dengan Metode *Penetration Testing Execution Standard*  
(PTES) Pada Universitas VWX**

**Alvita Izana Kusumarini**

**ABSTRAK**

Keamanan *server* sangat diperlukan sebagai bagian dari perlindungan serta pencegahan dari tindakan pencurian informasi. Aspek tersebut sering diabaikan oleh beberapa instansi khususnya pada perguruan tinggi karena mereka sudah merasa aman dengan kondisi keamanan jaringan *server* yang dimiliki dan menganggap permasalahan yang ada belum mengganggu aktivitas kerja dengan memasang *antivirus* maupun *firewall* pada *server*. Masih banyak perguruan tinggi yang masih belum memperketat keamanan informasi pada *server*. Sehingga, perlu dilakukan *penetration testing* untuk mengetahui kerentanan pada *server* dengan menggunakan metode PTES (*Penetration Testing Execution Standard*) untuk menjadi standar dalam menganalisis sistem keamanan informasi dalam menemukan celah keamanan pada sebuah instansi dalam kasus ini yaitu *server* data pegawai pada Universitas VWX dimana pada penelitian ini ditemukan kerentanan berupa serangan *Cross Site Tracing (XST)*, *Sensitive Data Exposure*, *Password Guessing*, *DDoS Attack* dan adanya kegiatan *Sniffing* yang bisa dilakukan pada *server* untuk di eksploitasi.

**Kata Kunci** : Keamanan *Server*, Kerentanan, *Penetration Testing Execution Standard*, *Penetration Testing*, *Cross Site Tracing (XST)*, *Sensitive Data Exposure*, *Password Guessing*, *DDoS Attack*, *Sniffing*

***Information System Security Analysis to Determine Server Security  
Vulnerability with Penetration Testing Execution Standard (PTES) Method at  
VWX University***

**Alvita Izana Kusumarini**

***ABSTRACT***

*Server security is indispensable as well as prevention of information theft measures. This aspect is often ignored by some agencies, especially in universities because they already feel secure with the security conditions of the server network and consider the existing problems have not interfered with work activities by installing antivirus or firewall on the server. There are still many universities that still have not tightened the security of information on servers. Therefore, penetration testing is necessary to determine vulnerabilities in the server by using PTES (Penetration Testing Execution Standard) method to become standard in analyzing information security systems in finding security gaps in an agency in this case, namely employee data server at VWX University where in this study found vulnerabilities in the form of Cross Site Tracing (XST), Sensitive Data Exposure, Password Guessing, DDoS Attack, and Sniffing activities that can be done on the server for exploitation.*

***Keywords:*** *Server Security, Vulnerability, Penetration Testing Execution Standard, Penetration Testing, Cross Site Tracing (XST), Sensitive Data Exposure, Password Guessing, DDoS Attack, Sniffing*

## KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala karunia-Nya, sehingga skripsi ini berhasil diselesaikan. Penulis ingin mengucapkan terima kasih kepada:

1. Orang tua dan seluruh keluarga penulis yang terus selalu mendoakan kelancaran, kemudahan, memberikan dorongan dan nasihat yang terbaik agar dapat menyelesaikan skripsi ini.
2. Bapak Henki Bayu Seta, M.Kom., MTI selaku dosen pembimbing I Skripsi yang membantu memberikan pembelajaran dan saran yang bermanfaat.
3. Bapak Ing. Artambo B. Pangaribuan., B. Sc selaku dosen pembimbing II Skripsi yang membantu memberikan pembelajaran dan saran yang bermanfaat.
4. Ibu, Bapak Dosen Informatika UPN Veteran Jakarta atas segala pembelajaran dan ilmu-ilmu bermanfaat yang telah diajarkan semasa perkuliahan.
5. Teman-teman Informatika 2017 yang selalu mendukung dalam menyelesaikan skripsi ini.
6. Rico Andreas sebagai senior Informatika 2016 yang memberikan dukungan moril semasa perkuliahan sampai skripsi dan membantu dalam menyelesaikan skripsi ini.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 2 Juli 2021

Penulis,

Alvita Izana Kusumarini



## DAFTAR ISI

<b>ANALISIS KEAMANAN SISTEM INFORMASI UNTUK MENGETAHUI KERENTANAN KEAMANAN <i>SERVER</i> DENGAN METODE <i>PENETRATION TESTING EXECUTION STANDARD (PTES)</i> PADA UNIVERSITAS VWX.....</b>	<b>i</b>
<b>PERNYATAAN ORISINALITAS.....</b>	<b>ii</b>
<b>PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS .....</b>	<b>iii</b>
<b>LEMBAR PENGESAHAN .....</b>	<b>iv</b>
<b>ABSTRAK .....</b>	<b>v</b>
<b><i>ABSTRACT</i> .....</b>	<b>vi</b>
<b>KATA PENGANTAR.....</b>	<b>vii</b>
<b>DAFTAR ISI.....</b>	<b>viii</b>
<b>DAFTAR GAMBAR.....</b>	<b>xi</b>
<b>DAFTAR TABEL.....</b>	<b>xiii</b>
<b>DAFTAR SIMBOL .....</b>	<b>xiv</b>
<b>BAB I. PENDAHULUAN.....</b>	<b>1</b>
<b>1.1 Latar Belakang .....</b>	<b>1</b>
<b>1.2 Rumusan Masalah .....</b>	<b>3</b>
<b>1.3 Tujuan Penelitian .....</b>	<b>4</b>
<b>1.4 Manfaat Penelitian .....</b>	<b>4</b>
<b>1.5 Ruang Lingkup .....</b>	<b>5</b>
<b>1.6 Luaran Yang Diharapkan .....</b>	<b>5</b>
<b>1.7 Sistematika Penulisan .....</b>	<b>5</b>
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>7</b>
<b>2.1 Penelitian Terkait .....</b>	<b>7</b>

<b>2.2</b>	<b>Keamanan Server</b> .....	10
<b>2.3</b>	<b>Keamanan Sistem Informasi</b> .....	10
<b>2.3.1</b>	<b>Kerahasiaan (<i>Confidentiality</i>)</b> .....	11
<b>2.3.2</b>	<b>Keutuhan (<i>Integrity</i>)</b> .....	11
<b>2.3.3</b>	<b>Ketersediaan (<i>Availability</i>)</b> .....	11
<b>2.4</b>	<b><i>Ethical Hacking</i></b> .....	12
<b>2.4.1</b>	<b><i>Black Hat Hacker</i></b> .....	12
<b>2.4.2</b>	<b><i>White Hat Hacker</i></b> .....	12
<b>2.4.3</b>	<b><i>Grey Hat Hacker</i></b> .....	12
<b>2.5</b>	<b><i>Penetration Testing</i></b> .....	13
<b>2.5.1</b>	<b><i>Black Box Testing</i></b> .....	13
<b>2.5.2</b>	<b><i>White Box Testing</i></b> .....	14
<b>2.5.3</b>	<b><i>Grey Box Testing</i></b> .....	14
<b>2.6</b>	<b><i>Vulnerability Assessment</i></b> .....	14
<b>2.7</b>	<b><i>Penetration Testing Execution Standard (PTES)</i></b> .....	16
<b>2.7.1</b>	<b><i>Pre-engagement Interactions</i></b> .....	17
<b>2.7.2</b>	<b><i>Intellegence Gathering</i></b> .....	18
<b>2.7.3</b>	<b><i>Threat Modelling</i></b> .....	18
<b>2.7.4</b>	<b><i>Vulnerability Analysis</i></b> .....	18
<b>2.7.5</b>	<b><i>Exploitation</i></b> .....	18
<b>2.7.6</b>	<b><i>Post Exploitation</i></b> .....	19
<b>2.7.7</b>	<b><i>Reporting</i></b> .....	19
<b>2.8</b>	<b><i>Nessus</i></b> .....	19
<b>2.9</b>	<b><i>Metasploit Framework</i></b> .....	20
<b>2.10</b>	<b><i>Nmap (Network Mapper)</i></b> .....	21
<b>2.11</b>	<b><i>Whois</i></b> .....	23

2.12	<i>Wireshark</i> .....	23
2.13	<i>Sniffing</i> .....	24
2.14	<i>Sensitive Data Exposure</i> .....	24
2.15	<i>Password Guessing</i> .....	25
2.16	<i>DDoS (Distributed Denial of Service)</i> .....	25
2.17	<i>XST (Cross-Site Tracing)</i> .....	26
<b>BAB III METODOLOGI PENELITIAN</b> .....		27
3.1	<b>Tahapan Penelitian</b> .....	27
3.2	<b>Metode Penelitian</b> .....	28
3.2.1	<b>Identifikasi Masalah</b> .....	28
3.2.2	<b>Perumusan Masalah</b> .....	28
3.2.3	<b>Studi Literatur</b> .....	29
3.2.4	<b>Pengumpulan Data</b> .....	29
3.3	<b>Metode <i>Penetration Testing Execution Standard (PTES)</i></b> .....	29
3.4	<b>Alat Bantu Penelitian</b> .....	35
3.5	<b>Jadwal Penelitian</b> .....	36
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....		37
4.1	<b>Pengumpulan Data</b> .....	37
4.2	<b><i>Pre-engagement</i></b> .....	37
4.3	<b><i>Intelligence Gathering</i></b> .....	38
4.3.1	<b><i>External Footprinting</i></b> .....	38
4.3.2	<b><i>Internal Footprinting</i></b> .....	43
4.4	<b><i>Threat Modelling</i></b> .....	48
4.5	<b><i>Vulnerability Analysis</i></b> .....	49
4.6	<b><i>Exploitation</i></b> .....	58
4.6.1	<b><i>Exploit</i></b> .....	58

4.6.2	<i>Scanning SSL</i> .....	68
4.6.3	<i>Nmap</i> .....	69
4.6.4	<i>Sniffing</i> .....	71
4.7	<i>Post Exploitation</i> .....	74
4.7.1	<i>Password Guessing</i> .....	74
4.8	<i>Reporting</i> .....	77
<b>BAB V PENUTUP</b> .....		82
5.1	<b>Kesimpulan</b> .....	82
5.2	<b>Saran</b> .....	83
<b>DAFTAR PUSTAKA</b> .....		84
<b>RIWAYAT HIDUP</b> .....		88
<b>LAMPIRAN</b> .....		89

## DAFTAR GAMBAR

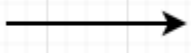

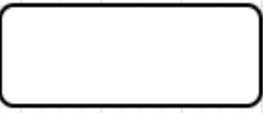
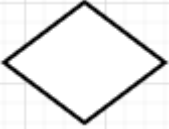

Gambar 2.1 Tahapan Penetration Testing Execution Standard (PTES) .....	17
Gambar 3.1 Flowchart Tahapan Penelitian .....	27
Gambar 4.1 <i>Ping Target</i> .....	38
Gambar 4.2 Perintah Whois .....	40
Gambar 4.3 Whois: Hasil Scanning 1 .....	40
Gambar 4.4 <i>Whois: Hasil Scanning 2</i> .....	41
Gambar 4.5 Nessus: Scanning Port.....	42
Gambar 4.6 Nessus: Scanning OS (Sistem Operasi) .....	43
Gambar 4.7 Perintah Nmap: Versi Layanan .....	43
Gambar 4.8 Hasil Nmap: Versi Layanan .....	44
Gambar 4.9 Perintah Nmap: Reason Status Port .....	45
Gambar 4.10 Hasil <i>Nmap: Reason Status Port</i> .....	46
Gambar 4.11 TCP Three-way handshake .....	46
Gambar 4.12 Perintah <i>Nmap: Scan</i> Protokol IP.....	47
Gambar 4.13 Hasil <i>Nmap: Protokol IP</i> .....	47
Gambar 4.14 Perintah <i>Nmap: Packet Tracer</i> .....	48
Gambar 4.15 Hasil <i>Nmap: Packet Tracer</i> .....	48
Gambar 4.16 Threat Modelling.....	49
Gambar 4.17 <i>Nessus: Scanning Vulnerability</i> .....	50
Gambar 4.18 Perintah <i>Nmap: Vulnerability Scanning</i> .....	55
Gambar 4.19 Hasil Perintah <i>Nmap: Vulnerability Scanning</i> .....	56
Gambar 4.20 <i>Search PHP RCE</i> .....	58
Gambar 4.21 Daftar Modul <i>PHP RCE</i> .....	59
Gambar 4.22 Hasil <i>exploit PHP RCE</i> .....	59
Gambar 4.23 Daftar Modul <i>SSL cert</i> .....	60
Gambar 4.24 Perintah <i>auxiliary SSL cert</i> .....	61
Gambar 4.25 Hasil <i>auxiliary SSL cert</i> .....	61
Gambar 4.26 Daftar Modul <i>HTTP TRACE</i> .....	62
Gambar 4.27 Hasil <i>HTTP TRACE</i> .....	63
Gambar 4.28 Hasil <i>SSL Information</i> .....	63

Gambar 4.29 Akses ke <i>server web</i> .....	64
Gambar 4.30 Daftar Modul DNS .....	65
Gambar 4.31 Hasil <i>DNS Amplification</i> .....	66
Gambar 4.32 Perintah <i>Directory Listing</i> .....	66
Gambar 4.33 Hasil <i>Directory Listing</i> .....	67
Gambar 4.34 Percobaan direktori .....	67
Gambar 4.35 <i>SSL Scanning</i> .....	68
Gambar 4.36 Hasil <i>TLS Heartbleed</i> .....	68
Gambar 4.37 Hasil Status SSL.....	69
Gambar 4.38 PHP Info .....	70
Gambar 4.39 <i>Sensitive Data Exposure</i> .....	70
Gambar 4.40 <i>Unsupported PHP version</i> .....	71
Gambar 4.41 <i>Wireshark: Hasil Sniffing</i> .....	72
Gambar 4.42 <i>Wireshark: Filtering packet</i> .....	72
Gambar 4.43 Alur Proses <i>Sniffing</i> .....	73
Gambar 4.44 Sebelum <i>Password Guessing</i> Berhasil.....	75
Gambar 4.45 Setelah <i>Password Guessing</i> Berhasil .....	75
Gambar 4.46 Daftar Data Pegawai.....	75
Gambar 4.47 Daftar Penghargaan Pegawai .....	76
Gambar 4.48 Statistik Karyawan .....	76

## DAFTAR TABEL

Tabel 2.1 Modul Metasploit Framework .....	21
Tabel 2.2 Status Port pada Nmap .....	22
Tabel 3.1 Pertanyaan Network Penetration Testing.....	30
Tabel 3.2 Pertanyaan Physical Penetration Testing .....	30
Tabel 3.3 Pertanyaan Administrator System.....	31
Tabel 3.4 Tindakan Kriminal Berdasarkan ID-SIRTII/CC.....	32
Tabel 3.5 Jadwal Penelitian.....	36
Tabel 4.1 Nessus: Scanning Vulnerability .....	51
Tabel 4.2 NSE (Nmap Scripting Engine): Scanning Vulnerability .....	56
Tabel 4.3 Laporan Hasil Penetration Testing.....	78

## DAFTAR SIMBOL

Simbol	Nama	Deskripsi
	Simbol Arus ( <i>Flow Direction Symbol</i> )	Penghubung antara simbol satu dengan simbol lainnya atau bisa dikatakan sebagai alur dalam suatu proses. Sering disebut <i>connecting line</i> .
	Simbol Terminal ( <i>Terminal Symbol</i> )	Permulaan ( <i>start</i> ) atau akhir ( <i>stop</i> ) dari suatu kegiatan.
	Simbol Proses ( <i>Processing Symbol</i> )	Menunjukkan proses yang dilakukan oleh komputer.
	Simbol Keputusan ( <i>Decision Symbol</i> )	Untuk memilih proses berdasarkan kondisi yang ada.
	Simbol Dokumen ( <i>Document Symbol</i> )	Menyatakan masukan ( <i>input</i> ) dari suatu dokumen atau keluaran ( <i>output</i> ) yang dicetak ke kertas.