# ANALISIS KERENTANAN KEAMANAN SISTEM PADA WINDOWS SERVER 2022 MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD

**SKRIPSI**

**M FARHAN NAUFAL FERMANA**

**1907422005**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER POLITEKNIK NEGERI JAKARTA**

**2023**

# ANALISIS KERENTANAN KEAMANAN SISTEM PADA WINDOWS SERVER 2022 MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD

**SKRIPSI**

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukanuntuk Memperoleh Diploma Empat Politeknik**

**M FARHAN NAUFAL FERMANA**

**1907422005**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER POLITEKNIK NEGERI JAKARTA**

**2023**

## SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini :

| | |
|---|---|
| Nama | : M Farhan Naufal Fermana |
| NIM | : 1907422005 |
| Program Studi | : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan |
| Judul Skripsi | : Analisis Kerentanan Keamanan Sistem Pada *Windows Server* 2022 Menggunakan Metode Penetration Testing Execution Standard |

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara Penelitian karya ilmiah yang berlaku. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 20 Agustus 2023

Yang Membuat Pernyataan


(M Farhan Naufal Fermana)

NIM. 1907422005

## LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : M Farhan Naufal Fermana

NIM : 1907422005

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Kerentanan Keamanan Sistem Pada *Windows server* 2022 Menggunakan Metode Penetration testing Execution Standard

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis, Tanggal 10, Bulan Agustus, Tahun 2023, dan dinyatakan LULUS.

Disahkan oleh:

Pembimbing I : Asep Kurniawan, S.Pd.,M.Kom.

Penguji I : Maria Agustin, S.Kom., M.Kom. ( )

Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom. ( )

Penguji III : Syamsi Dwi Cahya, S.S.T., M.Kom. ( )



Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S. Kom., M. Kom.

NIP. 197908032003122003

## KATA PENGANTAR

Dengan penuh rasa syukur, saya bersyukur kepada Allah SWT. atas kehadirat-Nya yang telah memberikan rahmat dan ridho-Nya sehingga saya dapat menyelesaikan Pendidikan, perkuliahan, dan skripsi ini dengan sukses. Tidak lupa, saya juga ingin mengucapkan terima kasih kepada banyak pihak yang telah memberikan dukungan, masukan, dan bimbingan selama perjalanan pendidikan, perkuliahan, dan penyusunan skripsi ini. Penulis mengucapkan banyak terima kasih kepada:

a. Bapak Asep Kurniawan, S.Pd., M.Kom. selaku pembimbing penulis yang telah banyak membantu, mendukung dan memberi masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai.
b. Orang tua dan Keluarga besar yang telah memberi kepercayaan dan motivasi yang diberikan keluarga merupakan pendorong utama bagi penulis untuk tetap semangat dalam menyelesaikan skripsi ini.
c. Terima kasih kepada teman-teman yang selalu memberikan semangat, dukungan, dan kerjasama selama masa perkuliahan dan penelitian.

Penulis mengakui adanya kekurangan dalam penyusunan dan penelitian Tugas Akhir/Skripsi ini. Saran dan kritik yang membangun dari para pembaca sangat diharapkan untuk membantu perbaikan dan penyempurnaan penelitian ini. Semoga laporan ini bermanfaat bagi penulis dan para pembaca. Penulis yakin bahwa bantuan yang diberikan oleh berbagai pihak dalam menyelesaikan Tugas Akhir/Skripsi ini akan mendapat balasan yang baik dari Tuhan Yang Maha Esa.

Depok, 24 Juli 2023

Penulis

## ABSTRAK

*Windows server adalah sistem operasi server yang banyak digunakan di lingkungan perusahaan dan organisasi. Keamanan jaringan menjadi faktor pentingdalam menjaga integritas dan kerahasiaan data yang diolah dalam sistem tersebut. Namun, rentannya sistem terhadap serangan cyber yang semakin canggih membuatsistem harus memiliki keamanan yang kuat. Oleh karena itu, analisis kerentanan keamanan jaringan pada Windows server 2022 perlu dilakukan dengan menggunakan metode penetration testing. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan sistem pada Windows server 2022 dengan menggunakan metode penetration testing. Penetration testing merupakan cara efektif untuk menguji keamanan jaringan dengan mengidentifikasi celah keamanan dan mengeskploitasi kelemahan sistem yang ditemukan. Penelitian ini memfokuskan pengujian pada Windows server 2022 dengan menggunakan teknik dan alat-alat khusus untuk mengidentifikasi kerentanan dan celah keamanan pada sistem. Hasil pengujian dan penilaian digunakan untuk membuat rekomendasi perbaikan dan tindakan pencegahan untuk memperkuat keamanan sistem. Penelitian ini dilakukan dengan tujuan untuk memberikan wawasan yang lebih dalam tentang sistem dan keamanannya sehingga dapat digunakan sebagai bahan evaluasi dalam meningkatkan keamanan sistem pada masa yang akan datang. Hasil analisis terdapat ada beberapa kerentanan dalam sistem operasi Windows server dan beberapa port yang terbuka, namun semua bisa diatasi dengan memperbarui sistem keamanan dari Windows server 2022.*

***Kata Kunci:*** Windows Server 2022, Keamanan Sistem, Penetration Sistem

# DAFTAR ISI

## DAFTAR GAMBAR

## DAFTAR TABEL

# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

Dalam era digital saat ini, penggunaan jaringan komputer semakin meluas dan menjadi semakin kompleks. *Windows server* 2022 adalah salah satu sistem operasi *server* paling populer yang digunakan untuk mengelola jaringan komputer. Saat ini, tidak ada sumber yang secara spesifik menyatakan jumlah pengguna *Windows server* 2022 di Indonesia. Namun, berdasarkan laporan dari IDC pada tahun 2019, *Windows server* adalah sistem operasi server paling populer di Indonesia dengan pangsa pasar sebesar 60,2%. Sementara itu, *Windows server* 2022 adalah versi terbaru dari sistem operasi *server Windows* dan diperkenalkan pada tahun 2022. (IDC, 2019)

Seperti halnya sistem operasi lainnya, *Windows server* 2022 juga rentan terhadap serangan *cyber* dan kerentanan keamanan. Oleh sebab itu, analisis kerentanan keamanan jaringan pada *Windows server* 2022 sangat penting untuk melindungi sistem dari serangan *cyber*.

Metode *pentest* atau *penetration testing* adalah salah satu cara yang paling efektif untuk menguji keamanan jaringan. Penetration testing melibatkan upaya aktif untuk menemukan celah keamanan dalam sistem dan mengeskploitasinya seperti yang akan dilakukan oleh penyerang. Penetration testing memberikan informasi yang sangat penting tentang kerentanan sistem dan membantu organisasi untuk mengambil tindakan untuk melindungi sistem dari serangan *cyber*.

Oleh karena itu, penelitian ini akan membahas tentang analisis kerentanan keamanan jaringan pada *Windows server* 2022 menggunakan metode penetration testing. Penelitian ini akan fokus pada mengidentifikasi kerentanan dan celah keamanan pada *Windows server* 2022 dan memberikan rekomendasi untuk memperbaiki sistem agar lebih aman dan terhindar dari serangan cyber. Hasil dari penelitian ini akan memberikan wawasan yang lebih dalam tentang keamanan

jaringan pada *Windows server* 2022 dan dapat membantu organisasi dalam meningkatkan keamanan jaringan mereka.

Dalam penelitian ini, fokus diberikan pada analisis keamanan terhadap *Windows server* 2022 dengan pendekatan yang melibatkan replikasi konfigurasi dan fitur yang umumnya digunakan oleh perusahaan yang mengandalkan *Windows server* 2022. Melalui pendekatan ini, tujuan utama adalah mengidentifikasi potensi kerentanan dan celah keamanan yang mungkin muncul dalam skenario nyata. Dengan mereplikasi konfigurasi dan fitur yang umumnya ada di lingkungan perusahaan, penelitian ini bertujuan untuk mendapatkan wawasan yang lebih akurat tentang seberapa kuatnya keamanan *Windows server* 2022 dalam menghadapi ancaman dan risiko yang mungkin dihadapi oleh perusahaan.

## 1.2 Perumusan Masalah

Dengan pemapaan latar belakang diatas, maka untuk rumusan masalah dari Penelitian ini adalah:

1 Bagaimana cara menemukan kerentanan pada *Windows server* 2022?

2 Bagaimana melakukan uji kerentanan keamanan pada *Windows server* 2022 dengan metode *Penetration testing* Execution Standard?

3 Bagaimana hasil analisis pengujian keamanan *Windows server* 2022?

## 1.3 Batasan Masalah

Batasan Masalah dari Penelitian yang dibuat adalah sebagai berikut:

1. Penelitian ini hanya akan berfokus pada analisis kerentanan keamanan pada sistem operasi *Windows server* 2022 dengan menggunakan jaringan lokal.
2. Penelitian ini hanya akan melakukan *Penetration testing* menggunakan Sistem Operasi *Kali Linux dan Windows server* secara *virtual* untuk melakukan analisis kerentanan keamanan.

3. Penelitian ini berfokus pada konfigurasi dan fitur yang terdapat pada perusahaan yang telah memberi izin untuk mereplikasi.

## 1.4 Tujuan dan Manfaat

Berikut merupakan tujuan dan manfaat Penelitian:

### 1.4.1 Tujuan

Berdasarkan pemaparan masalah diatas, Penelitian ini memiliki tujuansebagai berikut:

1. Menemukan kerentanan pada *Windows Server* 2022
2. Menguji kerentanan pada *Windows Server* 2022 dengan metode *Penetration Testing Execution Standard*
3. Menganalisis keamanan *Windows Server* 2022

### 1.4.2 Manfaat

Manfaat dari Penelitian ini adalah sebagai berikut:

1. Membantu user mengidentifikasi kerentanan dan celah keamanan dalam *Windows server* 2022.
2. Memberikan pemahaman mendalam tentang metode Penetration testing Execution Standard yang dilakukan oleh peneliti terhadap *Windows server* 2022.
3. User mendapat wawasan untuk meningkatkan keamanan sistem berdasarkan celah kerentanan yang ditemukan.

## 1.5 Sistematika Penelitian

**BAB I PENDAHULUAN**

Pada bab ini berisikan uraian latar belakang, rumusan masalah, Batasan masalah, tujuan dan manfaat dari penelitian yang dilakukan.

**BAB II TINJAUAN PUSTAKA**

Pada bab ini berisi materi dan dasar-dasar teori yang mendukung penelitian yang

diuraikan berdasarkan sumber dan referensi yang digunakan.

**BAB III METODE PENELITIAN**

Pada bab ini berisi beberapa pembahasan diantaranya rancangan penelitian , tahapan penelitian, objek penelitian, Teknik analisis dan pengumpulan data

**BAB IV PEMBAHASAN**

Pada bab ini berisi pembahasan proses dan hasil kegiatan penelitian yang dilakukan sesuai dengan tahapan dan metode yang telah dituliskan dalam pengimplementasian kerjanya.

**BAB V PENUTUP**

Pada bab ini berisi kesimpulan dan saran dari hasil penelitian yang dilakukan

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Berdasarkan pengujian kerentanan pada *Windows server* 2022 dan analisis yang dilakukan, dapat disimpulkan sebagai berikut.

1. Celah kerentanan pada *windows server* 2022 dapat ditemukan dengan melakukan scanning *port* menggunakan nmap dan *vulnberability scanning* menggunakan nessus. Hasil dari scanning *port* terdapat ada 13 *port* yang terbuka pada protokol tcp beserta service dari *Windows Server 2022*. Lalu dengan menggunakan *nessus* terdapat ada 13 *alerts* dengan tingkatan *critical, high dan info*. Oleh karena itu, Pengguna dapat meningkatkan keamanan sistem mereka dengan mengambil langkah-langkah proaktif, seperti melakukan memperbarui sistem keamanan secara rutin.
2. Hasil dari pengujian keamanan sistem pada *windows server* 2022 dengan menggunakan metode *penetration testing execution standard* mendapatkan hasil bahwa pengujian eksploitasi menggunakan metasploit pada *service IIS*, *Microsoft* kerberos dan *LDAP* dengan menggunakan *port* yang terbuka mendapatkan hasil bahwa tidak berhasil terkoneksi dengan sistem karena koneksi antara penyerang dan target telah diputus oleh target. Namun eksploitasi menggunakan *evil-winrm* berhasil masuk kedalam sistem dan bisa mengakses direktori dari target.
3. Tingkat kerentanan terhadap eksploitasi relatif rendah, karena sistem keamanan pada *Windows Server 2022* memiliki keamanan yang kuat. Meskipun begitu, langkah-langkah proaktif tetap diperlukan untuk melindungi *server* dari ancaman potensial. Salah satu tindakan yang dapat diambil adalah dengan menutup *port* yang terbuka dan rentan melalui pengaturan *Windows Defender Firewall*. Ini akan membantu mengurangi risiko akses tidak sah oleh penyerang yang mungkin berupaya mengeksploitasi kerentanan di *port* tersebut.

## 5.2 Saran

Berdasarkan pengujian yang telah dilakukan, berikut saran yang dapat digunakan untuk pengujian berikutnya:

1. Melakukan pengujian kerentanan pada *Windows server* 2022 yang ditemukan dengan metode yang lain.
2. Memiliki jaringan internet dan spek perangkat yang cukup memadai dalam kegiatan pengujian.
3. Menambah *tools vulnerability scanning* dan *exploiting tools* yang lain untuk dapat menemukan kerentanan yang lebih banyak.

# DAFTAR PUSTAKA

Adi Adrian, A. S. (2019). ANALISIS KEAMANAN JARINGAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) DI DINAS KESEHATAN PROVINSI JAWA BARAT.

Alamsyah, H., -, R. and Al Akbar, A. (2020) "Analisa Keamanan Jaringan Menggunakan network intrusion detection and prevention sistem," JOINTECS (Journal of Information Technology and Computer Science), 5(1), p. 17. Available at: https://doi.org/10.31328/jointecs.v5i1.1240.

IDC (2019), IDC Publishes Its Annual Server Operating Systems Market Share and Forecast Reports; Research Highlights Critical Role of Operating Systems in 3rd Platform IT, https://www.idc.com/getdoc.jsp?containerId=prUS49563622 (2023. August 02)

Andhika, D.A., Slamet and Ningsih, N. (2022) "Pengujian Penetrasi Pada Windows 10 Menggunakan model penetration testing execution standard (PTES)," Journal of Technology and Informatics (JoTI), 3(2), pp. 55–61. Available at: https://doi.org/10.37802/joti.v3i2.222.

Asep (2023) ASEP, – Belajarbacaandoa.com. Available at: https://belajarbacaandoa.com/bisakah-nessus-memindai-linux.html (2023, May 11).

Dwiyatno, S. (2020) "Analisis monitoring Sistem JARINGAN Komputer Menggunakan software nmap," PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 7(2), pp. 108–115. Available at: https://doi.org/10.30656/prosisko.v7i2.2522.

Dayan Singasatia, M. H. (n.d.). PENETRATION TESTING UNTUK MENGUJI KERENTANAN PADA. Penetration Test.

Dede Sudirman, A. N. (2021). Network Penetration dan Security Audit Menggunakan Nmap. sains dan Teknologi Informasi.

Dayan Singasatia, M. H. (2017). PENETRATION TESTING UNTUK MENGUJI KERENTANAN PADA SISTEM INFORMASI AKADEMIK DI SEKOLAH TINGGI XYZ. PENETRATION TESTING.

Esi Putri Silmina, A. F. (2022). ANALISIS KEAMANAN JARINGAN SISTEM

INFORMASI SEKOLAH . JURNAL ILMIAH TEKNIK ELEKTRO, 9.

Fatimah, T. M. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di . Wi-Fi Network Security Analysis.

Ginting, J.A. and Ngurah Suryantara, I.G. (2021) "Pengujian Kerentanan Sistem Dengan menggunakan metode penetration testing di universitas XYZ," Infotech: Journal of Technology Information, 7(1), pp. 41–46. Available at: https://doi.org/10.37365/jti.v7i1.105.

Hafiz (2022) Penetration testing:Tujuan,Strategi Dan Toolnya, aliyhafiz.com. Available at: https://aliyhafiz.com/penetration-testing/ (2022, March 27).

I Kadek Aldy Oka Ardita, ,. I. (2022). Analisis Keamanan Aplikasi Android Dengan Metode . Jurnal Elektronik Ilmu Komputer Udayana.

Pengertian *Windows server* Dan Fungsinya (2022) ImJuna Project. Available at: https://imjuna.com/memahami-fungsi-dan-pengertian-windows-server/ (2022, April 19).

Reza (2023) Pengertian penetration testing Dan Manfaatnya bagi perusahaan anda, Fourtrezz. Available at: https://fourtrezz.co.id/artikel/pengertian- penetration-testing-dan-manfaatnya-bagi-perusahaan-anda/ (2023, February 29).

Ridho, M.Y. (2022) APA ITU penetration testing?, Biztech. Available at: https://biztech.proxsisgroup.com/apa-itu-penetration-testing/ (2023, February 27).

Silmina, E.P., Firdonsyah, A. and Amanda, R.A. (2022) "Analisis Keamanan Jaringan Sistem informasi sekolah menggunakan penetration test Dan Issaf," Transmisi, 24(3), pp. 83–91. Available at: https://doi.org/10.14710/transmisi.24.3.83-91.