TUGAS AKHIR

PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE PENETRASI TESTING

Oleh:

YUVENTUS SELLY ULLU

NIM: 213310037

PROGRAM STUDI TEKNOLOGI KOMPUTER

PROGRAM DIPLOMA TIGA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIAYOG

YAKARTA 2024

TUGAS AKHIR

PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE PENETRASI TESTING

Diajukan sebagai salah satu syarat untuk menyelesaikan studi

Program Diploma Tiga

Program Studi Teknologi Komputer

Fakultas Teknologi Informasi Universitas Teknologi Digital Indonesia

Yogyakarta

Oleh:

YUVENTUS SELLY ULLU

NIM: 213310037

PROGRAM STUDI TEKNOLOGI KOMPUTER

PROGRAM DIPLOMA TIGA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIAYOG

YAKARTA 2024

HALAMAN PERSETUJUAN
TUGAS AKHIR

Judul	**: Pengujian Keamanan Jaringan Menggunakan MetodePenetrasi Testing**
Nama	**: Yuventus Selly Ullu**
NIM	**: 213310037**
Program Studi	**: Teknologi Komputer**
Program	**: Diploma Tiga**
Semester	**: Genap**
Tahun Akademik	**: 2023/2024**

Telah diperiksa dan disetujui untuk diujikan di hadapan Dewan Penguji Tugas

AkhirYogyakarta, 24 Juli 2024

Dosen Pembimbing,

(Dr. L.N. Harnaningrum, S.Si., M.T.)

NIDN : (0513057101)

HALAMAN PENGESAHAN

TUGAS AKHIR PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODEPENETRASI TESTING

Telah dipertahankan di depan Dewan Penguji Tugas Akhir dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh Gelar Ahli Madya Komputer Program Studi Teknologi Komputer

Fakultas Teknologi Informasi

Universitas Teknologi Digital IndonesiaYogyakarta

Yogyakarta, Juli 2024

Dewan Penguji	NIDN	Tandatangan
1. Dr. L.N. Harnaningrum, S.Si., M.T.	0513057101	.....
2. Yudhi Kusnanto, S. T., M. T.	0531127002	.....
3. Adiyuda Prayitna, S.T, M.T.	0506067901	.....

Mengetahui

Ketua Program Studi Teknologi Komputer

(Adi Kusiani, S.T., M.Eng.)

NPP : (0515067501)

PERNYATAAN KEASLIAN

Dengan ini dinyatakan bahwa tugas akhir ini belum pernah diajukan untuk memperoleh gelar Ahli Madya Komputer di Perguruan Tinggi manapun dan sepanjang pengetahuan penulis, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam tugas akhir ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 24 Juli 2024

Yuventus Selly Ullu

NIM : 213310037

HALAMAN PERSEMBAHAN

Segala puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya Tugas Akhir yang berjudul “Pengujian Keamanan Jaringan Menggunakan Metode Penetrasi Testing” ini.

Pada Tugas Akhir ini, ucapan terima kasih sebesar-besarnya disampaikan kepada.

1. Kedua orang tua saya, kaka dan adik Joriston, Efolison, Yohanes yang memberikan doa terbaik dan semangat tak hentinya.
2. Dr. L.N. Harnaningrum, S.Si., M.T. Selaku pembimbing yang telah memberikan bimbingan, saran, dan dorongan selama proses penyusunantugas akhir ini. Salam bagimu.

HALAMAN MOTO

Kuatkanlah hatimu dan berpeganglah teguh, janganlah takut dan janganlah gentar karena mereka, sebab TUHAN, Allahmu, Dia sendiri yang berjalan menyertai engkau, Dia tidak akan membiarkan engkau dan tidak akan meninggalkan engkau. - Ulangan 31:6

KATA PENGANTAR

Puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa, karena atas limpahan rahmat dan karunia-Nya, tugas akhir ini dapat diselesaikan dengan baik. Tugas akhir ini disusun untuk memenuhi persyaratan studi di Program Studi Teknologi Komputer, Universitas Teknologi Digital Indonesia.

Mengapa pengujian keamanan jaringan sangat penting? Ketika berada di internet, tidak ada yang sepenuhnya aman. Selalu ada celah dalam jaringan yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, untuk mengatasi potensi ancaman ini, pengujian keamanan (penetration test) diperlukan untuk mengevaluasi seberapa kuat jaringan yang digunakan, guna meminimalkan ancaman dan meningkatkan keamanan jaringan tersebut.

Dalam penyusunan tugas akhir ini, banyak pihak yang telah memberikan dukungan dan bantuan, baik secara langsung maupun tidak langsung. Oleh karena itu, rasa terima kasih yang sebesar-besarnya disampaikan kepada semua pihak yang telah berkontribusi.

1. Sri Redjeki, S.Si, M.Kom., Ph.D. sebagai Rektor Universitas Teknologi Digital Indonsia dan Dr. L.N. Harnaningrum, S.Si., M.T sebagai Warek 1 Universitas Teknologi Digital Indonsia salam bagimu.
2. Dr. L.N. Harnaningrum, S.Si., M.T. selaku pembimbing yang telah memberikan bimbingan, saran, dan dorongan selama proses penyusunan tu- gas akhir ini salam bagimu.
3. Adi Kusjani, S.T, M.Eng, selaku Kaprodi Teknologi Komputer terimakasi atas bimbingannya salam bagimu.
4. Keluarga tercinta yang selalu memberikan dukungan moral dan materi.

Semoga tugas akhir ini dapat memberikan manfaat dan kontribusi positif bagi pembaca serta pengembangan ilmu pengetahuan.

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

INTISARI

Melakukan pengujian keamanan jaringan penting untuk mengidentifikasi dan memperbaiki kerentanan yang dapat dieksploitasi oleh penyerang sebelum mereka dapat menyebabkan kerusakan. Port 445, yang digunakan oleh protokol SMB (Server Message Block) pada Windows, merupakan target umum bagi serangan karena sering kali terbuka untuk mengizinkan berbagi file dan printer dalam jaringan. Kerentanan pada port ini dapat memungkinkan penyerang mengakses file sensitif, menyebarkan malware seperti ransomware,oleh karena itu, port 445 memerlukan pengamanan khusus untuk mencegah eksploitasi yang dapat merugikan keamanan sistem.

Pengujian dilakukan menggunakan metode penetration testing (pentes) pada sistem target, dengan fokus pada port 445 yang digunakan untuk akses file sharing. Dalam pengujian ini, port 445 ditemukan dalam kondisi aktif dan terbuka (open), menunjukkan potensi kerentanan yang dapat dieksploitasi. Untuk menguji lebih lanjut, dilakukan serangan DDoS (Distributed Denial of Service) yang bertujuan memperlambat atau mengganggu akses file sharing melalui port tersebut, sehingga dapat menilai sejauh mana serangan ini dapat mempengaruhi kinerja dan keamanan sistem.

Dari hasil penelitian, bahwa serangan DDoS terhadap laptop target melalui port 445 menunjukkan variasi hasil. Serangan pertama menggunakan metode TCP dengan 3.857.503 permintaan gagal, dan serangan kedua menggunakan metode UDP dengan 33.735 permintaan yang juga gagal. Namun, serangan ketiga dengan metode HTTP pada port yang sama berhasil mengunduh 65 file dari 653 permintaan yang dilakukan.

Kata Kunci: pentest, simulasi serangan, DDoS attack, keamanan system

Abstract

Performing network security testing is essential to identify and fix vulnerabilities that can be exploited by attackers before they can cause damage. Port 445, used by the SMB (Server Message Block) protocol on Windows, is a common target for attacks because it is often open to allow file and printer sharing on a network. Vulnerabilities on this port can allow attackers to access sensitive files, spread malware such as ransomware, and therefore, port 445 requires special security to prevent exploits that can compromise system security.

Testing was conducted using the penetration testing (pentes) method on the target system, focusing on port 445 which is used for file sharing access. In this test, port 445 was found to be active and open, indicating a potential vulnerability that could be exploited. To further test, a DDoS (Distributed Denial of Service) attack was carried out which aimed to slow down or disrupt file sharing access through this port, so that it could assess the extent to which this attack could affect system performance and security.

From the research results, that DDoS attacks on target laptops via port 445 showed variations in results. The first attack used the TCP method with 3,857,503 failed requests, and the second attack used the UDP method with 33,735 requests that also failed. However, the third attack with the HTTP method on the same port successfully downloaded 65 files from 653 requests made.

Keywords: pentest, attack simulation, DDoS attack, system security