DOI: https://doi.org/xx.xxxxx/ilung.v3i2

Edukasi Kesadaran Keamanan Data Pegawai pada PT. Persona Optima Indonesia dengan contoh Exploit Windows XP Menggunakan Parrot OS

Robertus Laipaka1, Hady Wijaya2, Lidia Terecia3, Dennis Destrio4, Kevin Lysander5, Theresia Widji Astuti6
STMIK Pontianak; Jl. Merdeka No. 372 Pontianak, Telp. (0561) 735555, Fax. (0561) 737777
Jurusan Teknik Informatika, STMIK Pontianak, 6Politeknik Negeri Sambas, Prodi Manajemen Informatika
e-mail: robertus.laipaka@stmikpontianak.ac.id, hadywijaya171103@gmail.com, lidiatereciaa@gmail.com, dennisdestrio@gmail.com, kevin.lysander888@gmail.com, theresiawidji@gmail.com

Received: 31 01 2025/ Accepted: 14 02 2025

Abstract

Education Awareness Data Awareness for Employees of PT. Persona Optima Indonesia is crucial given the increasing cyber threat and low data security literacy. This PKM activity aims to increase employee understanding and capability in protecting data, creating a safe work environment, and preventing losses due to cyber attacks. The implementation of education involves a demonstration of system exploitation using Parrot OS to illustrate the mechanism of cyber attacks significantly, thereby increasing employee vigilance. The method used in this PKM activity includes a literature study to provide an understanding of the importance of understanding data security, this practice demonstration provides an overview of discussing the process of exploiting the Windows XP operating system using Parrot OS by utilizing the vulnerability of MS17-010 found in the SMBV1 protocol. Hands on Practice Participants can practice the tools used, discussions and questions and answers participants can provide feedback on PKM activities carried out then make a report as proof of conducting this PKM activity. The results of this PKM activity are expected to create a safe work environment and prevent potential losses due to cyber attacks.Abstract A maximum of 150-250 Indonesian words printed in italics with Cambria 10 point. The abstract should be clear, descriptive and should provide a brief overview of community service issues undertaken / researched. Abstracts include reasons for the selection of topics or the importance of research topics / community service, methods of research / devotion and outcome summary. The abstract should end with a comment about the importance of the result or a brief conclusion.

Keywords*: Security awareness; Exploitation; Windows xp; Parrot OS; MS17-010; Metasploit*

Abstrak

Edukasi kesadaran keamanan data bagi pegawai PT. Persona Optima Indonesia menjadi krusial mengingat meningkatnya ancaman siber dan rendahnya literasi keamanan data. Kegiatan pkm ini bertujuan untuk meningkatkan pemahaman dan kapabilitas pegawai dalam melindungi data, menciptakan lingkungan kerja yang aman, dan mencegah kerugian akibat serangan siber. Implementasi edukasi melibatkan demonstrasi exploitasi sistem menggunakan Parrot OS untuk mengilustrasikan mekanisme serangan siber secara nyata, sehingga meningkatkan kewaspadaan pegawai. Metode yang digunakan dalam kegiatan Pkm ini meliputi studi literatur untuk memberi pemahaman tentang pentingnya memahami keamanan data, Demonstrasi praktik ini memberikan gambaran membahas proses eksploitasi sistem operasi Windows XP menggunakan Parrot OS dengan memanfaatkan kerentanan MS17-010 yang ditemukan pada protokol SMBv1. Hands on Practice peserta dapat mempraktekan tool yang digunakan, Diskusi dan tanya jawab peserta dapat memberikan feedback terhadap kegiatan pkm yang dilaksanakan kemudian membuat laporan sebagai bukti telah melakukan kegiatan pkm ini. Hasil dari kegiatan pkm ini diharapkan dapat menciptakan lingkungan kerja yang aman dan mencegah potensi kerugian akibat serangan siber.

Kata kunci*: Kesadaran Keamanan; Eksploitasi; Windows XP; Parrot OS; MS17-010; Metasploit Framework .*

1. PENDAHULUAN

Edukasi kesadaran keamanan data bagi pegawai PT. Persona Optima Indonesia menjadi krusial mengingat meningkatnya ancaman siber(Ananda Khairunnisa et al., 2024) dan

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

rendahnya literasi keamanan data(Putri, Sari, Fajrina, & Aisyah, 2024). Kegiatan pkm ini bertujuan untuk meningkatkan pemahaman dan kapabilitas pegawai dalam melindungi data, menciptakan lingkungan kerja yang aman, dan mencegah kerugian akibat serangan siber. Implementasi edukasi melibatkan demonstrasi exploitasi sistem menggunakan Parrot OS(Raúl Ortiz-Serrano & Cruz-Triana, 2024) untuk mengilustrasikan mekanisme serangan siber secara nyata, sehingga meningkatkan kewaspadaan pegawai. Berbagai ancaman siber terus muncul, termasuk eksploitasi terhadap sistem operasi yang sudah usang seperti Windows XP. Windows XP, yang dirilis pada tahun 2001, telah dihentikan dukungannya oleh Microsoft sejak tahun 2014. Meskipun demikian, sistem operasi ini masih digunakan di berbagai sektor, terutama dalam perangkat keras legacy yang tidak kompatibel dengan sistem operasi modern. Kondisi ini menjadikannya target yang rentan bagi penyerang, terutama karena banyak kerentanan keamanan yang tidak akan pernah diperbaiki. Salah satu kerentanan yang paling terkenal pada Windows XP adalah MS17-010, yang terkait dengan protokol SMBv1. Kerentanan ini memungkinkan penyerang untuk mengeksekusi kode berbahaya dari jarak jauh, sehingga dapat mengambil alih sistem target sepenuhnya. Kerentanan ini menjadi dasar dari serangan besar seperti WannaCry dan EternalBlue, yang menyebabkan kerugian besar di berbagai negara. Eksploitasi MS17-010 menunjukkan bagaimana kelemahan dalam satu komponen sistem dapat dimanfaatkan untuk melancarkan serangan siber skala besar(Fitrisia & Saragih, 2024).

Kegiatan Pengabdian pada masyarakat ini bertujuan untuk dapat menciptakan lingkungan kerja yang aman dan mencegah potensi kerugian akibat serangan siber menurut(Hendra Wicaksana et al., 2020) diantaranya Phishing: Serangan ini bertujuan untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Penyerang biasanya menyamar sebagai pihak yang tepercaya melalui email, pesan teks, atau situs web palsu. Contohnya, email yang tampak seperti dari bank meminta Anda untuk mengklik tautan dan memasukkan informasi akun Anda; Ransomware: Serangan ini mengenkripsi data perusahaan dan menuntut tebusan untuk mengembalikan akses. Penyerang dapat mencuri data sebelum mengenkripsi untuk meningkatkan tekanan. Contohnya, varian ransomware WannaCry yang menyerang sistem komputer di seluruh dunia; Serangan DDoS (Distributed Denial of Service): Serangan ini membanjiri server atau jaringan perusahaan dengan lalu lintas palsu, membuatnya tidak dapat diakses oleh pengguna yang sah. Tujuannya adalah untuk mengganggu operasional perusahaan. Contohnya, serangan terhadap situs web e-commerce saat musim belanja yang menyebabkan situs web tidak dapat diakses; Malware: Perangkat lunak berbahaya ini dapat merusak sistem komputer, mencuri data, atau memberikan akses kepada penyerang. Malware dapat menyebar melalui email, lampiran, atau unduhan dari internet. Contohnya, virus komputer yang merusak file atau Trojan yang mencuri informasi perbankan; Serangan Man-in-the-Middle (MITM): Penyerang mencegat komunikasi antara dua pihak dan mencuri informasi yang sedang ditransmisikan. Contohnya, penyerang yang masuk ke dalam koneksi Wi-Fi publik dan mencuri data login dari pengguna yang terhubung.

2. METODE

Metode yang digunakan dalam kegiatan Pkm ini dalam bentuk workshop yang meliputi studi literatur untuk memberi pemahaman tentang pentingnya kesadaran memahami keamanan data dan informasi yang di sajikan materi dalam bentuk presentasi, Demonstrasi praktik ini memberikan gambaran membahas proses eksploitasi sistem operasi Windows XP menggunakan Parrot OS dengan memanfaatkan kerentanan MS17-010 yang ditemukan pada protokol SMBv1 dengan melalui beberapa tahap diantaranya melakukan seperti instalasi sistem, konfigurasi jaringan, dan validasi koneksi antara penyerang (Parrot OS) dan target

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

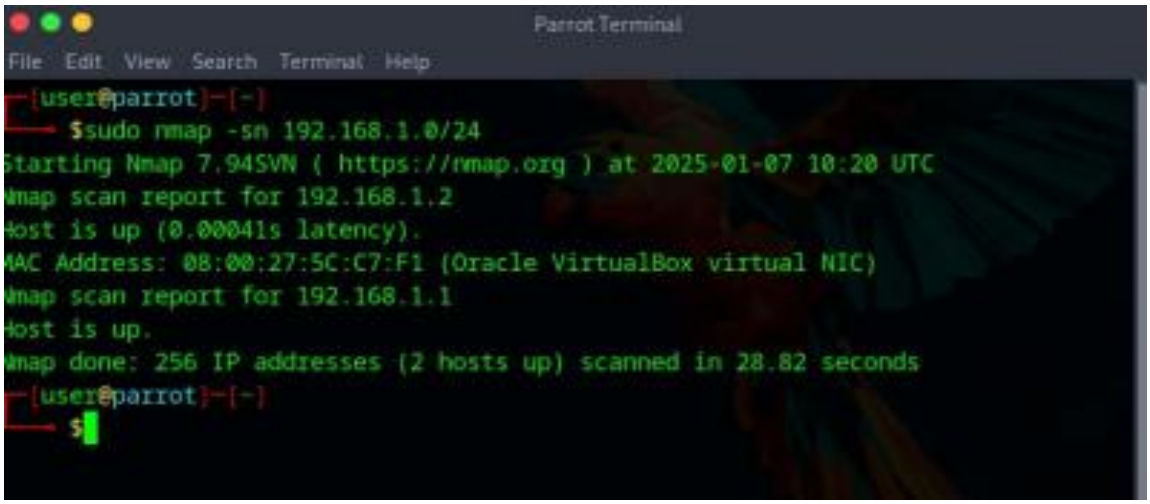
(Windows XP). Selanjtnya melakukan pengintaian (reconnaissance) menggunakan nmap untuk memindai port, layanan, dan sistem operasi target. Setelah itu, dilakukan scanning dan enumeration untuk mendeteksi kerentanan, seperti MS17-010, menggunakan Metasploit. Eksploitasi dilakukan dengan memanfaatkan modul eksploitasi SMB (MS17-010) untuk mendapatkan akses ke sistem target, diikuti dengan sesi post-exploitation untuk mengakses file, mengambil tangkapan layar, atau menjalankan perintah sistem. Aktivitas ini diakhiri dengan pembersihan jejak, seperti menghapus log menggunakan perintah clearev. Hands on Practice peserta dapat mempraktekan tool yang digunakan (nmap, Metasploit, Wireshark), serta data sekunder dari sumber eksternal seperti database CVE. Diskusi dan tanya jawab peserta dapat memberikan feedback terhadap kegiatan pkm yang dilaksanakan dengan mempraktekan ilmu yang di dapat selama kegiatan Pkm ini, kemudian membuat laporan sebagai bukti telah melakukan kegiatan pkm ini.

3. HASIL DAN PEMBAHASAN Cambria, Bold, 11 pt

Pengabdian masyarakat merupakan salah satu bentuk penerapan ilmu pengetahuan dan teknologi yang dilakukan oleh Dosen STMIK Pontianak untuk memberikan manfaat bagi masyarakat secara langsung. Dalam kontek workshop Edukasi Kesadaran Keamanan Data Pegawai pada PT. Persona Optima Indonesia dengan contoh Exploit Windows XP Menggunakan Parrot OS. Adapun tahapan-tahapan sebagai berikut;

3.1 Reconnaissance (Pengintaian)

Pada tahap pengintaian, dilakukan pemindaian jaringan menggunakan perintah nmap -sn 192.168.1.0/24 untuk mendeteksi perangkat aktif dalam jaringan lokal. Hasil pemindaian menunjukkan keberadaan perangkat target dengan alamat IP 192.168.1.2. Pemindaian ini dilakukan dengan metode ping sweep untuk memastikan perangkat tersebut aktif dan dapat diakses. Keberhasilan identifikasi perangkat target merupakan langkah awal yang sangat penting dalam serangan siber, karena memberikan landasan bagi penyerang untuk memfokuskan eksploitasi hanya pada perangkat yang relevan. Tahap ini juga menunjukkan pentingnya pengetahuan tentang topologi jaringan untuk melanjutkan ke langkah berikutnya. Jika informasi awal tidak ditemukan atau target tidak dapat diakses, langkah eksploitasi akan gagal. Dengan demikian, pengintaian yang efektif membantu menghemat waktu dan sumber daya saat melanjutkan ke tahap scanning dan enumeration.



Gambar 1. Pemindaian Perangkat

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

3.2 Scanning dan Enumeration (Pemindaian dan Enumerasi)

Setelah perangkat target teridentifikasi, dilakukan pemindaian mendalam menggunakan perintah nmap -T4 -O -A -sT -v 192.168.1.2. Pemindaian ini bertujuan untuk mendapatkan informasi yang lebih rinci tentang perangkat target, termasuk port terbuka, layanan aktif, sistem operasi yang digunakan, dan versi perangkat lunak yang berjalan. Hasil pemindaian menunjukkan bahwa port 445 (SMB) terbuka, yang mengindikasikan bahwa protokol SMBv1 masih aktif pada sistem target. Selain itu, pemindaian mengonfirmasi bahwa target menjalankan Windows XP SP3, sebuah sistem operasi yang tidak lagi mendapatkan dukungan dari Microsoft. Tahap scanning ini memberikan data penting yang digunakan untuk menentukan strategi eksploitasi. Identifikasi port 445 sebagai titik lemah membuka kemungkinan untuk mengeksploitasi kerentanan MS17-010, yang merupakan kerentanan kritis pada protokol SMBv1. Enumeration lebih lanjut juga menunjukkan bahwa layanan yang berjalan di port tersebut rentan terhadap serangan berbasis remote code execution (RCE). Informasi ini menjadi dasar bagi langkah eksploitasi berikutnya dan menunjukkan pentingnya pemindaian menyeluruh dalam mengidentifikasi titik masuk serangan.

3.3 Gaining Access (Mendapatkan Akses)

Setelah mengidentifikasi kerentanan target, eksploitasi dilakukan menggunakan Metasploit Framework. Setelah penginstallan cari modul terkait kerentanan MS17-010 dalam basis data Metasploit dengan "search MS17-010". MS17-010 adalah kerentanan yang ditemukan pada protokol SMBv1 di sistem operasi Windows, yang memungkinkan penyerang mengeksekusi kode berbahaya secara jarak jauh. Kerentanan ini dieksploitasi dalam serangan terkenal seperti WannaCry dan EternalBlue. Modul eksploitasi yang dipilih adalah exploit/windows/smb/ms17_010_psexec, yang dirancang khusus untuk memanfaatkan kerentanan MS17-010. Modul ini memanfaatkan kerentanan tersebut untuk mengeksekusi perintah secara jarak jauh dengan PsExec, sebuah mekanisme untuk menjalankan proses di sistem Windows melalui jaringan. Memakai Modul Eksploitasi Sebelum menjalankan eksploitasi, parameter seperti alamat IP target (RHOST: 192.168.1.2) dan alamat IP penyerang (LHOST: 192.168.1.10) dikonfigurasi Gambar 6. Set RHOST dan LHOST, Selanjutnya memilih target eksploitasi dalam rangkaian exploit yang disediakan Metasploit. Nilai 0 pada perintah set target 0 menunjukkan pemilihan target default atau target yang pertama dalam daftar target yang didukung oleh eksploit yang sedang digunakan. Biasanya, ini berarti bahwa eksploit akan menggunakan pengaturan target yang paling umum atau paling kompatibel dengan berbagai sistem tanpa penyesuaian khusus.

Setelah konfigurasi selesai, perintah exploit dijalankan, dan hasilnya adalah terbukanya sesi Meterpreter pada sistem target. Sesi Meterpreter ini memberikan akses penuh kepada penyerang untuk mengontrol sistem target. Kemampuan untuk mendapatkan akses ini menunjukkan bahwa kerentanan pada Windows XP dapat dieksploitasi dengan mudah menggunakan alat yang sudah tersedia. Hal ini juga menyoroti pentingnya pembaruan sistem operasi, karena kerentanan seperti MS17-010 telah lama diketahui dan dapat dicegah dengan pembaruan keamanan yang tepat.

3.4 Maintaining Access (Mempertahankan Akses)

Setelah mendapatkan akses, langkah berikutnya adalah memastikan bahwa koneksi kesistem target dapat dipertahankan. Dalam penelitian ini, payload windows/ meterpreter/ reverse_tcp digunakan untuk menciptakan koneksi balik (reverse shell) dari sistem target ke sistem penyerang. Payload ini memungkinkan penyerang untuk terus memantau dan mengontrol sistem target tanpa harus melakukan eksploitasi ulang.

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

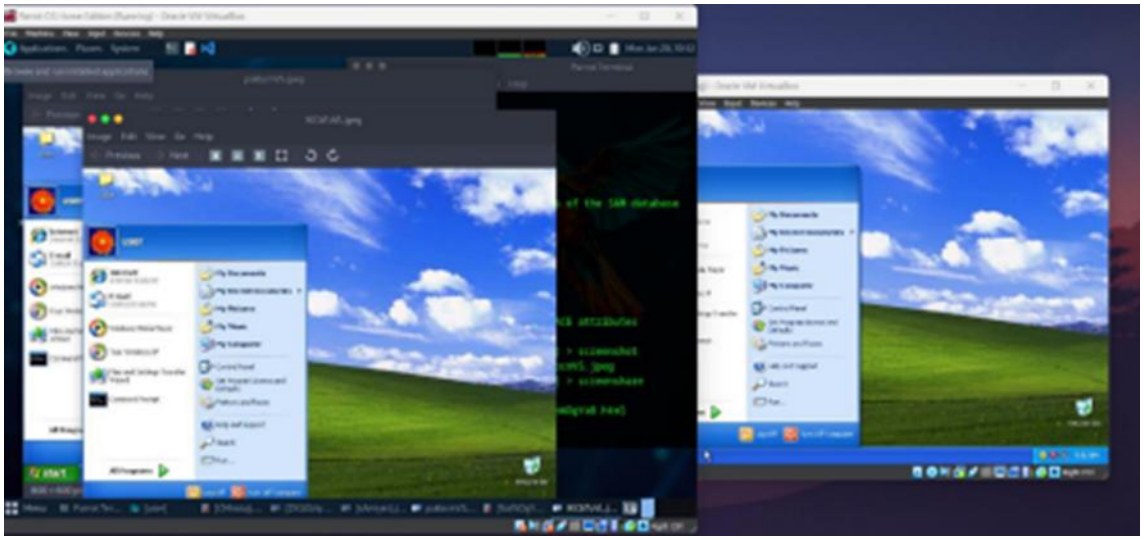
Meterpreter, yang merupakan bagian dari Metasploit Framework, memberikan kemampuan lanjutan seperti pengambilan file, manipulasi proses, dan eksekusi perintah. Dalam konteks eksploitasi ini, langkah mempertahankan akses sangat penting untuk memungkinkan penyerang melakukan tindakan lebih lanjut, seperti mengakses data sensitif atau menyebarkan malware tambahan. Namun, tahap ini juga menunjukkan kerentanan besar pada sistem target, terutama jika tidak ada mekanisme keamanan tambahan, seperti firewall atau sistem deteksi intrusi (IDS).

3.5 Covering Tracks (Menghapus Jejak)

Langkah terakhir dalam eksploitasi ini adalah menghapus jejak aktivitas penyerang di sistem target. Hal ini dilakukan dengan menggunakan perintah clearev di sesi Meterpreter, yang membersihkan log sistem, aplikasi, dan keamanan pada Windows XP. Dengan membersihkan log, penyerang berusaha untuk mencegah deteksi aktivitas yang mencurigakan oleh administrator sistem.

3.6 Hasil Hacking

Pada tahap hasil eksploitasi, peneliti berhasil mendapatkan akses penuh ke sistem Windows XP melalui sesi Meterpreter. Dengan akses ini, peneliti dapat melakukan berbagai tindakan terhadap sistem target, termasuk mengambil tangkapan layar (screenshot) dari tampilan desktop target untuk memantau aktivitas pengguna. Selain itu, peneliti dapat melihat layar secara langsung (live screenshare) untuk mendapatkan informasi real-time tentang apa yang sedang dilakukan pada sistem.

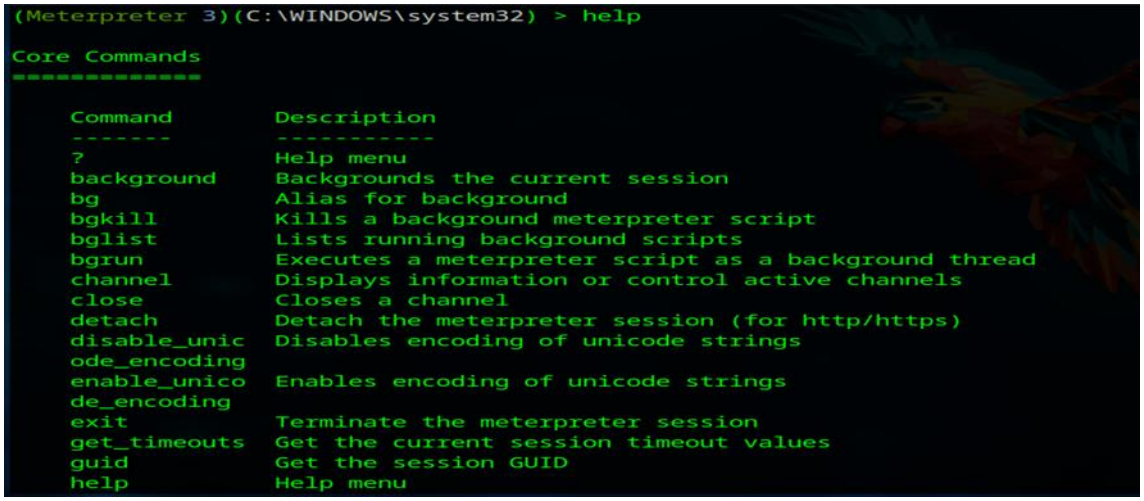


Gambar 2. Melakukan Screenshot dan ScreenShare

Peneliti juga berhasil mengunggah file virus dari Parrot OS ke Windows XP, yang memungkinkan pengujian terhadap penyebaran file atau program tertentu pada sistem target ini. Dalam upaya ini, mereka menggunakan berbagai metode untuk memastikan bahwa file tersebut dapat beroperasi dan menyebar tanpa deteksi oleh perangkat lunak keamanan yang ada di sistem Windows XP. Pengujian ini memberikan wawasan penting tentang kerentanan yang ada pada sistem operasi lama dan bagaimana virus dapat mengeksploitasi kelemahan tersebut untuk menyebar lebih luas. Melalui eksperimen ini, para peneliti dapat menganalisis pola penyebaran, kecepatan infeksi, dan efektivitas strategi pertahanan yang digunakan untuk memerangi ancaman tersebut. Hasilnya

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

menunjukkan bahwa meskipun Windows XP sudah usang, masih banyak celah yang dapat dimanfaatkan oleh virus modern, yang menegaskan pentingnya menjaga keamanan dan memperbarui sistem operasi. Selain itu, peneliti dapat menambah folder baru pada direktori di Windows XP sesuai kebutuhan, sehingga memungkinkan pengorganisasian file yang lebih sistematis. Selain itu, peneliti juga dapat menghapus folder yang tidak lagi diperlukan, menunjukkan bahwa mereka memiliki kontrol penuh terhadap struktur file dalam sistem operasi tersebut. Jejak log sistem berhasil dihapus menggunakan perintah clearev, yang membuat aktivitas lebih sulit untuk dideteksi, selaian itu juga dapat mematikan komputer target dari jarak jauh, menunjukkan tingkat kendali tinggi yang dapat dicapai dengan eksploitasi ini. Meterpreter menyediakan berbagai perintah tambahan yang dapat diakses dengan mengetikkan help. Ini mencakup kemampuan lain seperti manipulasi proses, pencurian informasi kredensial, atau eksekusi perintah sistem. Lihat Gambar 3



Gambar 3. Perintah Yang Dapat Diakses

Hasil ini menegaskan bahwa setelah eksploitasi berhasil, penyerang memiliki fleksibilitas luas untuk melakukan tindakan lanjutan yang dapat membahayakan keamanan dan integritas sistem target. Pengabdian kepada masyarakat ini adalah usaha untuk menyebarluaskan ilmu pengetahuan, teknologi, dan seni kepada masyarakat tentang kesadaran keamanan Sistem Informasi dan data pada lingkungan kerja. Setelah mengikuti Worksop ini Peserta dapat lebih peduli mengenai pentingkan menjaga keamanan data dan informasi karena sebagai suatu asset organisasi yang sangat berharga. Berikut Gambar 4 poto Kegiatan Workshop.

Gambar 4. Dokumentasi Peserta Workshop

DOI: https://doi.org/xx.xxxxx/ilung.v3i2

4. KESIMPULAN

Hasil dari kegiatan pengabdian pada masyarakat ini diharapkan dapat menciptakan lingkungan kerja yang aman dan mencegah potensi kerugian akibat serangan siber. Beberapa kesimpulan yang dapat diambil dari pentingnya dilaksanakan workshop ini adalah:

- Pengabdian Masyarakat adalah Inisiatif Positif: Melalui pengabdian masyarakat dalam bentuk workshop edukasi kesadaran Keamanan Data Pegawai pada PT. Persona Optima Indonesia dengan contoh Exploit Windows XP Menggunakan Parrot OS, para ahli keamanan siber berkontribusi secara aktif untuk memberikan manfaat bagi masyarakat. Dengan berbagi pengetahuan dan keterampilan, mereka membantu pemilik organisasi dan masyarakat secara umum untuk menghadapi tantangan keamanan siber.

- Kegiatan Pkm ini mengungkapkan bahwa sistem operasi Windows XP, yang sudah tidak lagi didukung oleh Microsoft, memiliki kerentanan serius terhadap serangan eksploitasi, khususnya kerentanan MS17-010 pada protokol SMBv1.

- Pada contoh Kesadaran Keamanan ini memanfaatkan Parrot OS sebagai contoh, sistem operasi berbasis Linux yang dirancang untuk keamanan siber, peneliti berhasil mengeksploitasi kelemahan ini menggunakan Metasploit Framework. Eksploitasi dilakukan secara sistematis, mulai dari pengintaian jaringan, pemindaian kerentanan, hingga pelaksanaan eksploitasi yang menghasilkan akses penuh ke sistem target.

- Peningkatan Kesadaran Masyarakat: Melalui partisipasi aktif dalam workshop ini, masyarakat dapat memahami risiko keamanan yang ada dan pentingnya tindakan proaktif untuk melindungi data mereka. Kesadaran yang lebih tinggi tentang keamanan cyber akan membantu mengurangi risiko serangan siber.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Pontianak yang telah memberikan dukungan terhadap Kegiatan pkm ini. Terima kasih kepada PT. Persona Optima Indonesia dan rekan-rekan dosen yang telah memberikan masukan dan dukungan dalam menyelesaikan tulisan ini. Kepada para reviewer saya juga mengucapkan banyak terima kasih atas bimbingan dan arahannya sehingga tulisan ini dapat sesuai seperti apa yang diharapkan. Semoga tulisan ini dapat memberikan manfaat bagi banyak orang, saat ini maupun yang akan datang.

DAFTAR PUSTAKA

Ananda Khairunnisa, P., Annisa, N., Parhusip, J., Kampus, A., Yos Sudarso, J., Jekan Raya, K., … Penulis, K. (2024). Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia. *Jurnal Ilmu Teknik dan Informatika*, 4, 9–16. Retrieved from https://doi.org/10.51903/teknik

Fitrisia, Y., & Saragih, J. P. (2024). ANALISA FORENSIK CYBER ATTACK TERHADAP WEB SECURITY. *Jurnal Komputer Terapan*, 10(2), 111–122. Retrieved from https://doi.org/10.35143/jkt.v10i2.6402

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, 22(2), 143–158. Retrieved from https://doi.org/10.33164/iptekkom.22.2.2020.143-158

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38–52. Retrieved from https://doi.org/10.35870/jpni.v6i1.1097

Raúl Ortiz-Serrano, L., & Cruz-Triana, A. (2024). *Securing Your Home Network: A Guide to Parrot OS Tools*.