Neptunus : Jurnal Ilmu Komputer Dan Teknologi Informasi
Volume. 3, No. 2, Mei 2025
e-ISSN : 3031-898X; dan p-ISSN : 3031-8998; Hal. 13-25
DOI: https://doi.org/10.61132/neptunus.v3i1.753
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Eksploitasi Kerentanan dan Remote Access pada Windows 10

Albert Christofen[1*], Isram Rasal[2]
[1,2] Universitas Gunadarma, Indonesia
E-mail : albertchristofen29@gmail.com[1], isramrasal@staff.gunadarma.ac.id[2]

Alamat: Jalan Margonda Raya Nomor 100, Pondok Cina, Depok, Jawa Barat 16424
**Korespondensi penulis: albertchristofen29@gmail.com*

Abstract. *Exploitation is an activity carried out to gain benefits by harming others arbitrarily without responsibility. Exploitation is a threat in the field of Cyber Security that not only poses risks but also jeopardizes an individual's security and privacy. According to data from the Institute of Internal Auditors, financial losses due to cybercrime exploitation worldwide reached 8 trillion US dollars in 2023. In Cyber Security, one exploitation technique involves using Remote Access methods to take over access rights and enable remote system control. Based on this issue, the author conducts research on Remote Access using three different target models based on the Windows operating system. These three targets will demonstrate how vulnerabilities in an operating system can be exploited to gain Remote Access. The method for testing Remote Access involves identifying the vulnerabilities available in the target system. The study employs three techniques: exploiting the ms17-010 vulnerability, utilizing the SmbGhost vulnerability, and using a backdoor. The results show that all three approaches successfully penetrated the target system and made modifications.*

Keywords: *Exploits, Remote Access, Vulnerabilities*

Abstrak. Eksploitasi atau exploitation merupakan aktifitas yang dilakukan untuk mengambil keuntungan dengan merugikan orang lain secara sewenang-wenang tanpa adanya tanggung jawab. eksploitasi merupakan ancaman di dalam dunia Cyber Security yang tidak hanya mengancam namun dapat merugikan keamanan dan privasi seseorang. Berdasarkan data Institut Auditor Internal kerugian akibat eksploitasi akibat kejahatan siber di seluruh dunia pada tahun 2023 mencapai 8 triliun dolar AS. Dalam dunia Cyber Security, salah satu teknik eksploitasi adalah menggunakan metode Remote Access untuk mengambil alih hak akses dan memungkinkan untuk mengontrol sistem dari jarak jauh. Dari permasalahan tersebut maka penulis akan melakukan penelitian Remote Access menggunakan tiga model target yang berbeda berbasis sistem operasi Windows. Tiga target tersebut akan menunjukkan bagaimana kerentanan dalam sebuah sistem operasi dapat dieksploitasi hingga mendapatkan akses Remote Access. Metode mengenai pengujian Remote Access dapat diakses dengan mengetahui kerentanan yang tersedia terhadap target eksploitasi. Teknik yang digunakan sebanyak 3 cara yaitu menggunakan kerentanan ms17-010, menggunakan kerentanan SmbGhost dan menggunakan backdoor. Dari ketiga target tersebut, hasil yang didapat berhasil masuk ke dalam sebuah sistem dan membuat perubahan.

Kata kunci: Eksploitasi, Kerentanan, Remote Access

1. LATAR BELAKANG

Keamanan sistem operasi merupakan aspek krusial dalam dunia teknologi informasi, terutama dengan meningkatnya jumlah serangan siber yang menargetkan kerentanan perangkat lunak. Sistem operasi Windows 10, sebagai salah satu sistem operasi yang paling banyak digunakan secara global, menjadi sasaran utama eksploitasi oleh peretas. Salah satu metode serangan yang sering digunakan adalah eksploitasi kerentanan untuk memperoleh akses jarak jauh tanpa otorisasi, yang dapat digunakan untuk mencuri data, menyebarkan malware, atau bahkan mengendalikan sistem target (Arifin, 2020).

Eksploitasi kerentanan sistem operasi umumnya dilakukan dengan memanfaatkan kelemahan dalam protokol komunikasi dan sistem autentikasi. Salah satu vektor serangan

yang banyak dimanfaatkan adalah Server Message Block (SMB), yang memiliki riwayat panjang dalam berbagai insiden keamanan (Kumar & Kumar, 2019). Serangan terkenal seperti WannaCry dan EternalBlue telah menunjukkan bagaimana kerentanan SMB dapat memberikan akses penuh kepada penyerang terhadap sistem yang tidak diperbarui (Wang & Zhang, 2021). Selain itu, serangan berbasis backdoor juga kerap digunakan untuk mempertahankan akses jarak jauh terhadap sistem yang telah berhasil disusupi (Mursalim, 2023).

Berdasarkan penelitian terdahulu, serangan eksploitasi sering kali dilakukan dengan menggunakan alat seperti Metasploit dan Nmap, yang memungkinkan penyerang untuk mengidentifikasi dan mengeksploitasi kerentanan yang ditemukan (Kennedy et al., 2011). Metasploit berperan sebagai framework eksploitasi yang menyediakan berbagai modul untuk menyerang sistem target, sedangkan Nmap digunakan sebagai pemindai jaringan guna mengidentifikasi layanan yang terbuka dan rentan terhadap serangan (Widharma, 2020).

Penelitian ini bertujuan untuk mengeksplorasi tingkat kerentanan sistem operasi Windows 10 versi 2016, 2019, dan 22H2 terhadap eksploitasi berbasis remote access. Pengujian dilakukan menggunakan metode Penetration Testing Execution Standard (PTES), yang mencakup tahapan mulai dari pengumpulan informasi, analisis kerentanan, eksploitasi, hingga pasca-eksploitasi (Andhika, 2021). Hasil dari penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan sistem keamanan yang lebih tangguh, baik bagi individu maupun organisasi yang menggunakan Windows 10. Selain itu, penelitian ini juga dapat menjadi referensi bagi praktisi keamanan siber dalam menyusun strategi pertahanan yang lebih efektif terhadap serangan berbasis remote access.

2. KAJIAN TEORITIS

Keamanan Sistem Komputer

Keamanan sistem komputer adalah bidang yang sangat penting dalam teknologi informasi, yang bertujuan untuk melindungi sistem komputer dari berbagai ancaman dan serangan. Menurut Stallings (2018), keamanan sistem komputer adalah upaya untuk melindungi sistem komputer dan data dari akses yang tidak sah, penggunaan yang tidak sah, pengungkapan, gangguan, modifikasi, atau perusakan (Stallings, 2018). Tanenbaum dan Bos (2015) menambahkan bahwa keamanan sistem komputer juga melibatkan perlindungan terhadap hardware, software, dan data dari ancaman internal dan eksternal (Tanembaum & Bos, 2015).

Ancaman terhadap keamanan sistem komputer dapat berasal dari berbagai sumber, termasuk serangan dari luar, kesalahan manusia, dan kerentanan perangkat lunak. Menurut Bustami dan Bahri (2020), beberapa ancaman umum terhadap keamanan sistem komputer meliputi serangan virus, serangan denial of service (DoS), serangan man-in-the-middle, dan serangan insider (Bustami & Bahri, 2020). Serangan virus adalah salah satu ancaman paling umum yang dapat merusak data dan perangkat lunak. Serangan DoS bertujuan untuk membuat sistem tidak dapat diakses oleh pengguna yang sah dengan membanjiri sistem dengan lalu lintas yang berlebihan. Serangan man-in-the-middle melibatkan penyadapan komunikasi antara dua pihak untuk mencuri atau memodifikasi data. Serangan insider dilakukan oleh orang dalam organisasi yang memiliki akses ke sistem dan data (Bustami & Bahri, 2020).

Eksploitasi Sistem Komputer

Eksploitasi sistem komputer adalah tindakan yang memanfaatkan ke rentanan dalam sistem komputer untuk mendapatkan akses yang tidak sah atau menyebabkan kerusakan. Eksploitasi ini dapat dilakukan oleh individu atau kelompok dengan berbagai motif, termasuk pencurian data, sabotase, atau keuntungan finansial. Menurut Bishop (2018), eksploitasi sistem komputer adalah tindakan yang memanfaatkan kelemahan atau kerentanan dalam hardware, software, atau jaringan untuk mendapatkan akses yang tidak sah atau menyebabkan kerusakan (Bishop, 2018).

Eksploitasi ini dapat dilakukan melalui berbagai metode, termasuk serangan buffer overflow, injeksi SQL, dan serangan cross site scripting (XSS). Eksploitasi sistem komputer dapat dibagi menjadi beberapa jenis berdasarkan metode yang digunakan. Menurut Bishop (2018), beberapa jenis eksploitasi yang umum meliputi serangan buffer overflow, injeksi SQL, dan serangan cross-site scripting (XSS) (Bishop, 2018).

Penetration Testing

Penetration Testing, atau pengujian penetrasi, merupakan metode evaluasi keamanan pada sistem komputer, jaringan, atau aplikasi dengan cara mensimulasikan serangan yang berasal dari pihak internal maupun eksternal (Hafizh & Rasal, 2025). Metodologi ini bertujuan untuk mengidentifikasi dan mengeksploitasi kerentanan yang mungkin ada dalam sistem, yang dapat digunakan oleh penyerang untuk mendapatkan akses tidak sah atau merusak data (Perrin, 2020). Proses penetration testing biasanya melibatkan beberapa tahap,

termasuk perencanaan, pengumpulan informasi, pemindaian kerentanan, eksploitasi, dan pelaporan hasil (Kumar & Kumar, 2019).

Remote Access

Remote access adalah teknologi yang memungkinkan pengguna untuk mengakses dan mengelola komputer atau jaringan dari lokasi yang berbeda. Menurut Bishop (2018), remote access adalah kemampuan untuk mengakses komputer atau jaringan dari lokasi yang berbeda melalui jaringan komunikasi, seperti internet (Bishop, 2018). Stallings (2018) menambahkan bahwa remote access dapat dilakukan melalui berbagai metode, termasuk Virtual Private Network (VPN), Remote Desktop Protocol (RDP), dan Secure Shell (SSH) (Stallings, 2018).

Server Message Block

Server Message Block (SMB) adalah protokol jaringan yang digunakan untuk menyediakan akses bersama ke file, printer, dan komunikasi serial antara node pada jaringan. Kerentanan pada protokol SMB dapat dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah ke sistem dan data. Menurut penelitian yang dilakukan oleh Arifin (2020), kerentanan SMB telah menjadi target utama bagi berbagai serangan siber, termasuk serangan ransomware seperti WannaCry dan eksploitasi EternalBlue (Arifin, 2020).

Windows Defender

Windows Defender adalah aplikasi antivirus yang dikembangkan oleh Microsoft dan secara otomatis terpasang pada komputer atau laptop berbasis Windows. Aplikasi ini berfungsi sebagai sistem keamanan yang melindungi perangkat dari berbagai ancaman malware dan serangan siber. Menurut Widharma (2020), Windows Defender adalah aplikasi antivirus yang dirancang untuk melindungi sistem operasi Windows dari ancaman malware, termasuk virus, spyware, dan perangkat lunak berbahaya lainnya. Windows Defender bekerja dengan memindai file dan program yang masuk ke sistem, serta memonitor aktivitas sistem untuk mendeteksi dan menghapus ancaman yang ditemukan (Widharma, 2020).

Backdoor

Backdoor adalah metode yang digunakan oleh penyerang untuk mendapatkan akses tidak sah ke sistem komputer atau jaringan tanpa terdeteksi oleh mekanisme keamanan yang ada. Backdoor sering kali dipasang oleh malware atau oleh penyerang yang telah mendapatkan akses awal ke sistem. Menurut penelitian yang dilakukan oleh Mursalim

(2023), backdoor dapat digunakan untuk berbagai tujuan, termasuk pencurian data, pengawasan, dan peluncuran serangan lebih lanjut (Mursalim, 2023).

NMAP

Nmap (Network Mapper) adalah alat open-source yang digunakan untuk eksplorasi jaringan dan audit keamanan. Menurut Widharma (2020), Nmap adalah alat yang digunakan untuk memetakan jaringan dan mengidentifikasi layanan yang berjalan pada host dalam jaringan tersebut. Nmap bekerja dengan mengirimkan paket-paket khusus ke host target dan menganalisis respons yang diterima untuk menentukan status dan karakteristik host tersebut (Widharma, 2020).

Metasploit

Metasploit adalah kerangka kerja untuk pengujian penetrasi yang digunakan untuk mengembangkan dan mengeksekusi exploit terhadap sistem target (Kennedy, 2011). Pertama kali dikembangkan oleh H.D. Moore pada tahun 2003 dan sekarang dikelola oleh Rapid7, Metasploit telah berkembang menjadi salah satu alat yang paling penting dalam dunia keamanan siber (Hafizh & Rasal, 2025).

3. METODE PENELITIAN

Penelitian ini menggunakan metode Penetration Testing Execution Standard (PTES) untuk menguji eksploitasi kerentanan pada sistem operasi Windows 10 versi 2016, 2019, dan 22H2. PTES merupakan standar yang terdiri dari tujuh tahap utama yang dirancang untuk mengidentifikasi, mengeksploitasi, dan mengevaluasi kerentanan suatu sistem.

Sumber: (Fikri, et al., 2023).

Gambar 1. Kerangka Kerja PTES

Tahapan-tahapan dalam metode ini meliputi:

1) Pre-Engagement Interactions

   Tahap ini merupakan langkah awal dalam proses pengujian penetrasi, yang mencakup perencanaan dan pengaturan skenario penelitian. Lingkup pengujian ditetapkan menggunakan virtual machine, di mana Windows 10 digunakan sebagai sistem target dan Kali Linux sebagai sistem penyerang. Konfigurasi lingkungan uji mencakup aktivasi atau deaktivasi fitur keamanan seperti Windows Defender dan Firewall untuk mengevaluasi dampaknya terhadap keberhasilan eksploitasi.

2) Intelligence Gathering

   Pada tahap ini, dilakukan pengumpulan informasi terkait sistem target, termasuk alamat IP, versi sistem operasi, dan layanan yang berjalan. Informasi ini diperoleh menggunakan alat pemindaian jaringan seperti Nmap, yang membantu dalam mengidentifikasi port terbuka dan layanan rentan.

3) Threat Modeling

   Berdasarkan data yang diperoleh pada tahap sebelumnya, dilakukan pemetaan ancaman yang mungkin terjadi pada sistem target. Ancaman dikategorikan berdasarkan tingkat risiko dan kemungkinan eksploitasi yang dapat dilakukan terhadap sistem target.

4) Vulnerability Analysis

   Tahap ini mencakup analisis dan validasi kerentanan yang ditemukan dalam sistem target. Tiga jenis eksploitasi utama yang diuji dalam penelitian ini adalah:

   a. MS17-010 (EternalBlue): Kerentanan pada protokol SMB yang memungkinkan serangan remote code execution.
   b. SMBGhost (CVE-2020-0796): Eksploitasi yang memanfaatkan kelemahan dalam Windows SMBv3, yang dapat menyebabkan akses tidak sah ke sistem.
   c. Backdoor dengan payload reverse_https: Teknik eksploitasi yang memungkinkan penyerang mempertahankan akses jarak jauh secara tersembunyi.

5) Exploitation

   Pada tahap ini dilakukan untuk menguji sejauh mana eksploitasi dapat berjalan dengan Metasploit Framework. Eksploitasi yang berhasil akan memungkinkan akses remote shell, eksekusi perintah, serta kontrol penuh terhadap sistem target.

6) Post-Exploitation

Pada tahap ini, dilakukan evaluasi dampak eksploitasi setelah akses berhasil diperoleh. Pengujian mencakup analisis potensi pengambilan data sensitif, eskalasi hak akses, serta persistensi akses dalam sistem.

7) Reporting

Tahap akhir dari metode penelitian ini adalah penyusunan laporan, yang mendokumentasikan seluruh proses pengujian penetrasi, temuan eksploitasi, serta rekomendasi mitigasi. Hasil ini bertujuan untuk memberikan wawasan yang lebih mendalam mengenai risiko keamanan Windows 10 serta langkah-langkah yang dapat diterapkan untuk memperkuat sistem dari serangan serupa.

4. HASIL DAN PEMBAHASAN

Penelitian ini mengevaluasi kerentanan pada Windows 10 versi 2016, 2019, dan 22H2 menggunakan metode Penetration Testing Execution Standard (PTES). Pengujian dilakukan dengan mengidentifikasi dan mengeksploitasi kerentanan MS17-010, SMBGhost, dan backdoor berbasis payload reverse_https. Proses dimulai dengan intelligence gathering, yang mencakup pemindaian jaringan menggunakan Nmap untuk mengidentifikasi layanan terbuka pada sistem target. Setelah itu, dilakukan analisis kerentanan terhadap sistem target, di mana ditemukan bahwa MS17-010 dan SMBGhost dapat dieksploitasi jika Windows Defender dan Firewall dalam keadaan nonaktif. Dengan menggunakan Metasploit Framework, eksploitasi terhadap sistem berhasil dilakukan pada konfigurasi dengan keamanan rendah, memungkinkan penyerang memperoleh remote access dan eskalasi hak istimewa.

Tabel 1. Skenario Penyerangan

Versi Windows Target	Skenario	Konfigurasi Keamanan	Tools yang digunakan	Hasil Pengujian
Windows 10 versi 2016	A	Firewall aktif, Password Sharing aktif	Nmap, Metasploit	Eksploitasi gagal karena sistem keamanan aktif
	B	Firewall nonaktif, Password Sharing nonaktif	Nmap, Metasploit	Eksploitasi berhasil, sistem rentan terhadap serangan SMBGhost
Windows 10 versi 2019	A	Firewall aktif	Nmap, Metasploit	Eksploitasi gagal, konfigurasi keamanan mencegah akses tidak sah
	B	Firewall nonaktif	Nmap, Metasploit	Eksploitasi berhasil, penyerang mendapatkan akses remote.

Windows 10 versi 22H2	A	Windows Security - Real Time Protection aktif	Nmap, Metasploit, msfvenom	Eksploitasi gagal, backdoor terdeteksi sebagai ancaman
	B	Windows Security - Real Time Protection nonaktif	Nmap, Metasploit, msfvenom	Eksploitasi berhasil, penyerang memperoleh sesi meterpreter dan dapat mengakses sistem target

Perbandingan Hasil Pengujian pada Windows 10 Versi 2016

1. Pre-Engagement Interactions

Pada skenario pertama, interaksi pra-engagement dilakukan dengan mengidentifikasi informasi dasar mengenai sistem target. Sistem Windows 10 versi 2016 dengan firewall aktif menunjukkan resistensi terhadap pemindaian awal, membatasi data yang dapat dikumpulkan. Sebaliknya, pada skenario kedua, dengan firewall dinonaktifkan, lebih banyak informasi tentang layanan yang berjalan dapat diperoleh, memungkinkan tahap selanjutnya berjalan lebih efektif.

2. Intelligence Gathering

Pada skenario pertama, firewall yang aktif membatasi hasil pemindaian Nmap, sehingga hanya beberapa port yang terdeteksi terbuka. Ini mengurangi kemungkinan eksploitasi lebih lanjut. Sebaliknya, skenario kedua memperlihatkan lebih banyak port terbuka, termasuk SMB (Server Message Block), yang merupakan target utama eksploitasi menggunakan kerentanan SMBGhost.

3. Threat Modeling

Dengan data yang diperoleh dari tahap sebelumnya, ancaman potensial dievaluasi. Pada skenario pertama, risiko serangan lebih rendah karena minimnya informasi yang dapat dikumpulkan. Sementara itu, pada skenario kedua, dengan lebih banyak port yang terbuka dan layanan yang dapat diakses, risiko eksploitasi meningkat karena adanya potensi kerentanan pada SMB.

4. Vulnerability Analysis

Pada skenario pertama, sistem tampak lebih aman karena firewall aktif menghalangi eksploitasi langsung. Pemindaian terhadap kerentanan SMBGhost (CVE-2020-0796) tidak memberikan hasil yang signifikan. Namun, dalam skenario kedua, analisis menunjukkan bahwa SMBGhost dapat dieksploitasi karena firewall dan mekanisme keamanan lainnya dinonaktifkan, menjadikan sistem lebih rentan.

5. Exploitation

Eksploitasi dalam skenario pertama mengalami hambatan signifikan akibat firewall yang aktif, sehingga serangan tidak dapat dijalankan. Sementara itu, dalam skenario kedua, eksploitasi dengan Metasploit berhasil, memungkinkan akses tidak sah ke sistem. Payload yang digunakan dapat mengeksekusi kode berbahaya, menunjukkan bahwa sistem dalam konfigurasi ini sangat rentan terhadap serangan.

6. Post-Exploitation

Setelah eksploitasi berhasil pada skenario kedua, sesi meterpreter diperoleh, memungkinkan penyerang untuk melakukan berbagai tindakan seperti pencurian data dan eskalasi hak akses. Pada skenario pertama, eksploitasi gagal sehingga tidak ada akses pasca-eksploitasi yang dapat dilakukan.

7. Reporting

Pada tahap pelaporan, skenario pertama menunjukkan sistem yang relatif aman dengan firewall sebagai garis pertahanan utama. Namun, skenario kedua menyoroti kelemahan signifikan dalam sistem ketika firewall dinonaktifkan, memungkinkan eksploitasi penuh melalui SMBGhost.

Perbandingan Hasil Pengujian pada Windows 10 Versi 2019

1. Pre-Engagement Interactions

Pada tahap ini, dilakukan perencanaan awal terhadap kedua skenario dengan menentukan target sistem, yaitu Windows 10 versi 2019. Dalam skenario pertama, target memiliki firewall aktif, sedangkan dalam skenario kedua, firewall dinonaktifkan. Langkah ini penting untuk mengetahui konfigurasi awal sistem sebelum dilakukan pengujian keamanan.

2. Intelligence Gathering

Tahap ini melibatkan pengumpulan informasi terkait sistem target, seperti alamat IP, port yang terbuka, serta layanan yang berjalan. Pada skenario pertama, firewall yang aktif membatasi informasi yang dapat diperoleh menggunakan Nmap, sehingga hanya sedikit port yang terdeteksi. Sebaliknya, pada skenario kedua, firewall yang dinonaktifkan memungkinkan lebih banyak informasi diambil, termasuk port SMB yang terbuka dan potensi eksploitasi layanan yang rentan.

3. Threat Modeling

Setelah mendapatkan informasi sistem target, dilakukan analisis untuk menentukan ancaman potensial. Pada skenario pertama, ancaman lebih sulit diidentifikasi karena firewall membatasi visibilitas terhadap layanan yang berjalan. Sementara itu, pada skenario kedua,

ancaman lebih jelas terlihat, dengan identifikasi kerentanan SMBGhost yang dapat dimanfaatkan untuk eskalasi hak akses.

4. Vulnerability Analysis

Analisis kerentanan dilakukan dengan menggunakan berbagai alat seperti Metasploit dan Nmap untuk memvalidasi apakah sistem target rentan terhadap eksploitasi. Dalam skenario pertama, firewall yang aktif mencegah eksploitasi langsung terhadap SMB, sehingga serangan gagal dilakukan. Namun, dalam skenario kedua, firewall yang nonaktif memungkinkan eksploitasi SMBGhost berjalan dengan sukses, membuka potensi bagi penyerang untuk mendapatkan akses lebih dalam ke sistem target.

5. Exploitation

Tahap eksploitasi dilakukan dengan mencoba menyusup ke dalam sistem menggunakan kerentanan yang telah ditemukan. Pada skenario pertama, eksploitasi gagal karena firewall memblokir komunikasi dengan server penyerang. Sebaliknya, dalam skenario kedua, eksploitasi berhasil dengan memanfaatkan payload pada Metasploit, sehingga penyerang dapat memperoleh akses awal ke sistem target.

6. Post-Exploitation

Tahap ini berfokus pada pemanfaatan akses yang telah diperoleh. Pada skenario pertama, akses tidak dapat diperoleh karena perlindungan keamanan sistem masih aktif. Namun, dalam skenario kedua, setelah eksploitasi berhasil, penyerang dapat menjalankan perintah dari jarak jauh dan mengendalikan sistem target menggunakan sesi meterpreter, memungkinkan pencurian data atau pemasangan backdoor untuk akses lebih lanjut.

7. Reporting

Dalam skenario pertama, serangan tidak berhasil karena firewall yang aktif melindungi sistem dari eksploitasi. Sementara itu, dalam skenario kedua, eksploitasi berhasil dilakukan akibat tidak adanya proteksi yang memadai, menunjukkan bahwa firewall memainkan peran penting dalam mencegah akses tidak sah ke dalam sistem.

Perbandingan Hasil Pengujian pada Windows 10 Versi 22H2

1. Pre-Engagement Interactions

Pada tahap awal ini, dilakukan kesepakatan target eksploitasi serta identifikasi batasan dan tujuan pengujian. Kedua skenario memiliki pendekatan yang sama dalam tahap ini, yaitu menentukan Windows 10 versi 22H2 sebagai target eksploitasi dan memastikan bahwa lingkungan pengujian dikonfigurasi untuk mensimulasikan serangan dalam kondisi nyata.

Namun, pada skenario pertama, faktor keamanan lebih diperhatikan karena Windows Security dalam kondisi aktif, yang memungkinkan mitigasi dini terhadap ancaman.

2. Intelligence Gathering

Pada tahap ini, dilakukan pemindaian jaringan menggunakan Nmap untuk mengidentifikasi layanan dan port yang terbuka pada sistem target. Dalam kedua skenario, informasi mengenai sistem operasi dan layanan jaringan berhasil dikumpulkan. Namun, pada skenario pertama, firewall dan proteksi real-time Windows Security memblokir sebagian besar deteksi yang dilakukan oleh Nmap, sedangkan pada skenario kedua, dengan Windows Security nonaktif, informasi lebih mudah diperoleh karena tidak ada proteksi yang membatasi pemindaian.

3. Threat Modeling

Setelah informasi sistem diperoleh, dilakukan analisis terhadap potensi ancaman berdasarkan kerentanan yang terdeteksi. Pada skenario pertama, meskipun beberapa port terbuka, fitur keamanan yang aktif mengurangi kemungkinan eksploitasi. Sementara itu, pada skenario kedua, sistem lebih rentan karena tidak ada perlindungan tambahan, sehingga ancaman terhadap layanan yang berjalan dapat langsung dikonfirmasi dan ditargetkan untuk eksploitasi.

4. Vulnerability Analysis

Tahap ini melibatkan identifikasi dan validasi kerentanan yang ada dalam sistem. Pada skenario pertama, meskipun SMBGhost terdeteksi sebagai kerentanan potensial, eksploitasi tidak dapat dilakukan karena Windows Security dan fitur keamanan lainnya berhasil memblokir payload. Sebaliknya, pada skenario kedua, tidak ada sistem pertahanan yang aktif, sehingga Metasploit berhasil memverifikasi bahwa eksploitasi dapat dilakukan terhadap layanan SMB yang berjalan tanpa perlindungan.

5. Exploitation

Pada tahap ini, serangan dilakukan dengan mencoba menyusup ke dalam sistem target menggunakan payload yang telah disiapkan. Dalam skenario pertama, upaya eksploitasi gagal karena Windows Security secara otomatis mendeteksi aktivitas mencurigakan dan memblokir payload sebelum dieksekusi. Sebaliknya, dalam skenario kedua, dengan proteksi dinonaktifkan, eksploitasi berhasil dan sesi meterpreter diperoleh, memungkinkan penyerang untuk mengakses sistem secara penuh.

6. Post Exploitation

Setelah akses diperoleh, penyerang mengeksplorasi sistem lebih lanjut untuk melihat potensi dampak serangan. Pada skenario pertama, karena eksploitasi gagal, tidak ada tindakan

lanjutan yang dapat dilakukan. Sebaliknya, dalam skenario kedua, penyerang dapat mengeksekusi perintah meterpreter, membaca file sistem, mengunggah dan mengunduh data, serta melakukan eskalasi hak akses jika diperlukan.

7. Reporting

Tahap akhir dari pengujian ini adalah mendokumentasikan hasil eksploitasi. Pada skenario pertama, laporan menyatakan bahwa sistem Windows Security efektif dalam mencegah eksploitasi SMBGhost, sementara pada skenario kedua, laporan mencatat bahwa sistem tanpa perlindungan rentan terhadap eksploitasi dan memungkinkan akses penuh bagi penyerang.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, eksploitasi kerentanan dalam sistem operasi Windows 10 dapat berhasil dilakukan menggunakan teknik pentesting dengan memanfaatkan kerentanan MS17-010, SMBGhost, dan backdoor dengan payload reverse_https. Eksploitasi ini memungkinkan penyerang untuk memperoleh remote access jika kondisi keamanan sistem, seperti Firewall dan antivirus, dalam keadaan nonaktif. Hasil penelitian menunjukkan bahwa kelemahan dalam konfigurasi keamanan sistem dapat dimanfaatkan untuk mendapatkan akses tidak sah, sehingga penting bagi pengguna untuk memastikan sistem mereka selalu diperbarui dan dilindungi dengan kebijakan keamanan yang ketat.

Sebagai saran untuk penelitian selanjutnya, disarankan untuk mengeksplorasi beragam tools dan metode eksploitasi lainnya guna memperoleh hasil yang lebih luas dan mendalam dalam aspek keamanan sistem operasi. Selain itu, pengujian terhadap berbagai konfigurasi keamanan Windows 10 juga dapat dilakukan untuk memahami bagaimana perubahan dalam pengaturan sistem mempengaruhi tingkat kerentanannya. Dengan demikian, penelitian mendatang diharapkan dapat memberikan solusi lebih efektif dalam mencegah eksploitasi dan meningkatkan ketahanan sistem terhadap serangan siber.

DAFTAR REFERENSI

Andhika, D. A. (2021). TA: Pengujian penetrasi pada Windows 10 menggunakan model Penetration Testing Execution Standard (PTES) (PhD thesis). Universitas Dinamika.

Arifin, A. K. (2020). Analisis aktivitas dan pola serangan EternalBlue dan WannaCry ransomware yang beraksi pada jaringan. Jurnal Teknik Informatika dan Desain Komunikasi Visual Universitas Telkom, 2(2), 1–10.

Bishop, M. (2018). Computer security: Art and science. Addison-Wesley Professional.

Bustami, A., & Bahri, S. (2020). Ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi: Systematic review. Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), 7(2), 12–25.

Fikri, M. N., Zen, B. P., Adhitama, R., & Firdaus, E. A. (2023). Analisis keamanan sistem informasi website SMA Negeri 1 Sokaraja menggunakan metode Penetration Testing Execution Standard (PTES). Jurnal Informatika, 2(2), 19–27.

Hafizh, M. N., & Rasal, I. (2025). Implementasi pengujian kerentanan Windows 10 menggunakan EternalBlue dan phishing. Jurnal Penelitian Teknologi Informasi dan Sains, 3(1), 82–91. https://jurnal.tibsemarang.ac.id/index.php/JPTIS

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The penetration tester's guide. No Starch Press.

Kumar, K. S., & Kumar, S. S. (2019). Impact of SMB MS17-010 vulnerability on enterprise network infrastructure. International Journal of Network Security, 21(3), 456–465.

Kumar, R., & Kumar, S. (2019). The stages of penetration testing: An overview. Journal of Cyber Security Technology, 3(2), 91–104.

Mursalim. (2023). Analisis ancaman phishing backdoor remote access trojan (BRAT). Jurnal Teknik Informatika dan Desain Komunikasi Visual Universitas Selamat Sri, 2(2), 1–10.

Perrin, G. (2020). Penetration testing: A hands-on introduction to hacking. No Starch Press.

Rapid7. (2024). 2024 attack intelligence report: Insights from four years of vulnerability and exploit data (Technical Report). Rapid7 Labs.

Stallings, W. (2018). Computer organization and architecture. Pearson.

Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems. Pearson.

Wang, L., & Zhang, Y. (2021). Forensic analysis of WannaCry ransomware exploiting SMB MS17-010 vulnerability. Digital Investigation, 28, S45–S53.

Widharma, I. G. S. (2020). Pengamanan sistem jaringan komputer dengan teknologi firewall. ResearchGate. https://www.researchgate.net/