Journal of Technology and Informatics (JoTI)
Vol. 3, No. 2, Bulan April Tahun 2022
P-ISSN 2721-4842
E-ISSN 2686-6102 DOI: 10.37802/joti.v3i2.222

Pengujian Penetrasi pada Windows 10 menggunakan Model *Penetration Testing Execution Standard* (PTES)

Delfan Azhar Andhika[1], Slamet[2] , Norma Ningsih[3]
[1,2] Universitas Dinamika, [3] Politeknik Elektronika Negeri Surabaya
Email: 14410100117@dinamika.ac.id, slamet@dinamika.ac.id, norma@pens.ac.id

Abstract: *Windows 10 is an operating system that is used by many people, organizations and companies. Windows 10 itself has a bug (vulnerability) when first installed by the user. This bug (vulnerability) can interfere with existing processes, some settings do not work as it should then if the bug (vulnerability) is used for something that is not legal, can also lead to inaccessible data (ransomware), delete user data to damage the system Windows 10 itself. The solution is to do penetration testing on the Windows 10 operating system and find bugs (vulnerabilities) in accordance with the method used, namely the Penetration Testing Execution Standard (PTES) model, using tools that fit the stages in the Penetration model Testing Execution Standard (PTES). The results of penetration testing using the Penetration Testing Execution Standard (PTES) model show that with the right tools, researchers can look for bugs (vulnerabilities) that exist on Windows 10 systems and patch them. This research consists of 4 stages, namely testing the Lack of OS Hardening attack, testing the Easily Guessable Credentials attack, testing the Missing Patch attack, and testing the Lack of Application Hardening attack. To test the attacks carried out, 3 tools were used, namely Nmap, Hydra and Metasploit Framework.*

Keywords: *Bug, Vulnerability, Penetration Testing Execution Standard, Windows 10*.

PENDAHULUAN

Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi saat ini. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang komprehensif dan terstruktur untuk memberikan perlindungan dari risiko organisasi yang munkgin dihadapi. Dalam upaya memecahkan masalah keamanan, dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi dan komunikasi [1]. Keamanan informasi digunakan untuk menggambarkan perlindungan aset informasi, termasuk komputer dan non-komputer peralatan, fasilitas dan data untuk menjamin kerahasiaan, integritas dan ketersediaan informasi melalui kebijakan aplikasi, Pendidikan dan teknologi [2].

Serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Beberapa kemungkinan serangan, di antaranya interruption, interception, modification dan fabrication [3]. Jaringan komputer merupakan sekumpulan perangkat keras maupun perangkat lunak dari beberapa komputer yang saling terhubung dan berbagi data antara satu dengan lainnya [4].

Dari celah-celah yang ditemukan ini, kemudian dapat berakibat fatal jika ada pihak yang menggunakan celah ini untuk kepentingan individu yang bisa merusak sistem tersebut sehingga merugikan instansi/perusahaan. Kemudian individu ini bisa membuat *ransom* terhadap sistem pada instansi/perusahaan yang membuat pihak instansi/perusahaan tidak bisa mengakses data-data penting mereka dan harus membayar sejumlah uang kepada individu ini untuk bisa mengakses data-data penting mereka kembali.

Pengerasan sistem atau biasa disebut *system hardening* mengacu pada teknik yang meminimalkan kerentanan dan ancaman keamanan dengan menetapkan berbagai fungsi dalam Sistem Target. Sistem ini terutama terhubung ke jaringan, dan terutama digunakan sebagai metode untuk melindungi server dengan akses yang sering kepada eksternal [5].

Objek dari penelitian ini adalah Windows 10, dikarenakan Windows 10 telah mempunyai bug dari pertama kali diinstal oleh pengguna. Menurut penelitian yang dilakukan oleh [6], ditemukan bahwa Windows memiliki kerentanan yang lebih serius, karena beberapa layanan dan daemonnya tidak aman dan terbuka untuk diakses. Ini memberikan kemungkinan eksploitasi. Windows 10 adalah serangkaian sistem operasi komputer pribadi yang diproduksi oleh Microsoft sebagai bagian dari keluarga sistem operasi Windows NT. Ini adalah penerus Windows 8.1, dan dirilis ke manufaktur pada 15 Juli 2015 [7].

Selain itu, berdasar website yang dirilis oleh [8], Windows 10 dari versi 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903 sampai 1909 memiliki kelemahan (vulnerability) yang sudah ada pada saat pertama kali diinstal.

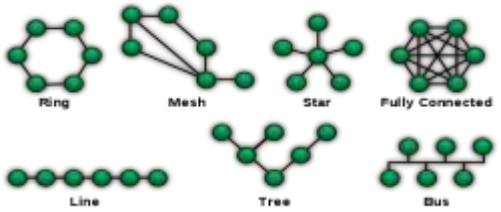
Oleh karena itu, dibutuhkan Penetration Testing yang bertujuan untuk mencari dan menemukan celah-celah yang ada pada sistem atau host tersebut.

Penetration testing adalah sebuah serangan cyber simulasi resmi pada komputer, dilakukan untuk mengevaluasi keamanan sistem [9]. Penetration Testing Execution Standard (PTES) terdiri dari 7 bagian utama. Bagian tersebut membahas semua yang terkait dengan penetration testing. Dari Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation sampai Reporting [10].

METODE PENELITIAN

Topologi Jaringan

Topologi jaringan adalah susunan atau pemetaan interkoneksi antara node, dari suatu jaringan, baik secara fisik (riil) dan logis (virtual). Topologi digunakan untuk melakukan pengabelan secara fisik dari suatu jaringan. Topologi fisik jaringan adalah cara yang digunakan untuk menghubungkan workstation-workstation di dalam LAN tersebut [11]. Beberapa contoh topologi jaringan adalah sebagai berikut:

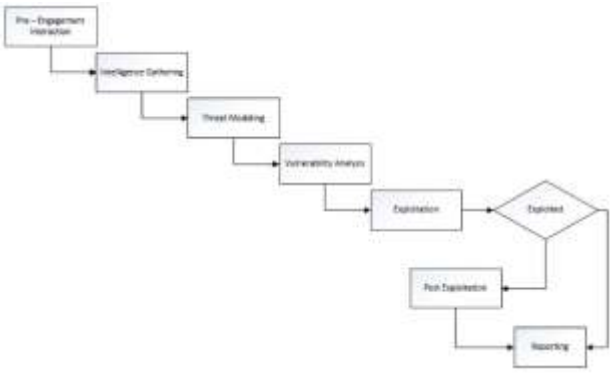


Gambar 1. Topologi Jaringan

Penetration Testing Execution Standard

Dalam menyelesaikan penelitian penetration testing dalam hal persiapan, mencari intel, pemodelan ancaman, analisis kelemahan, explotasi, pasca exploitasi dan reporting. Tahapan-tahapan tersebut mengacu pada metode penelitian yang digunakan pada penetration testing ini yaitu menggunakan metode Penetration Testing Execution Standard (PTES) yang dimulai dari tahap Pre-engagements sampai Reporting seperti pada Gambar 2.

Penetration Testing Execution Standard (PTES) adalah standar baru yang dirancang untuk menyediakan bahasa dan ruang lingkup yang sama bagi bisnis dan penyedia layanan keamanan untuk melakukan pengujian penetrasi, terdiri dari tujuh bagian utama. mencakup tentang pengujian penetrasi dari awal dan alasan melakukan penetration testing, melalui pengumpulan informasi dan model ancaman di mana penguji melakukan pengujian untuk mendapatkan informasi yang lebih banyak dan melalui penelitian kerentanan, eksploitasi dan pasca eksploitasi, di mana dari semua tahap itu dilakukan dan akhirnya dilanjutkan dengan membuat laporan yang menangkap seluruh proses [10].



Gambar 2. Tahapan Penelitian

PENGUJIAN PENETRASI

Observasi

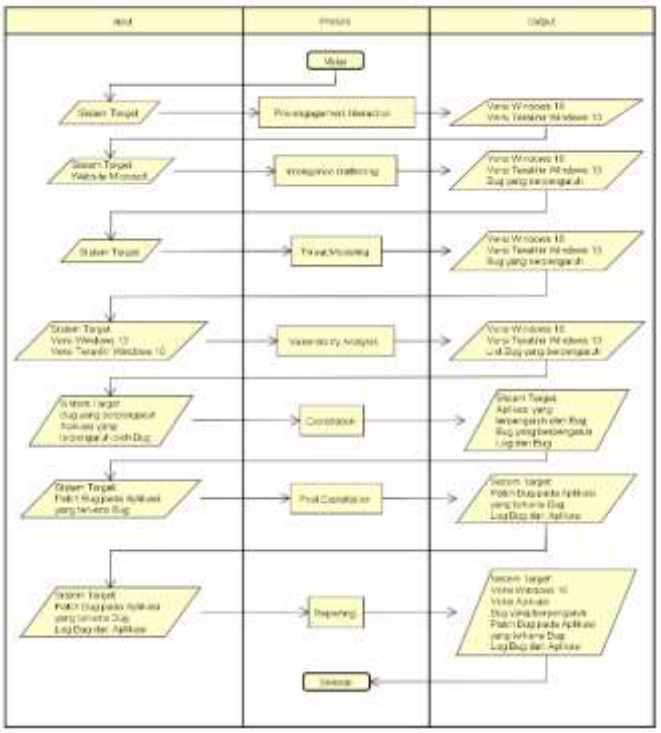
Observasi yang didapatkan dari penelitian ini yaitu menggunakan Lab sendiri, percobaan pengujian yang dilakukan terisolasi, berarti tidak mengganggu atau dapat mengubah Host/Device lain pada jaringan yang digunakan. penelitian ini terdiri dari 4 hal yaitu pengujian serangan *Lack of OS Hardening*, pengujian serangan *Easily Guessable Credentials*, pengujian serangan *Missing Patch*, pengujian serangan *Lack of Application Hardening*. Untuk melakukan tes terhadap serangan yang dilakukan, digunakan 3 *tools*, yaitu *Nmap, Hydra* dan *Metasploit Framework*. Ketiga tools tersebut digunakan untuk melakukan *scanning*, *brute-force* dan eksploitasi pada Sistem *Target*.

Studi Literatur

Data-data dan informasi yang digunakan sebagai studi literatur yang dilakukan dengan mempelajari materi tentang Penetration Testing, Penetration Testing Execution Standard, penggunaan tools Metasploit Framework, Nmap, Wireshark dan Hydra.

Kerangka Penelitian

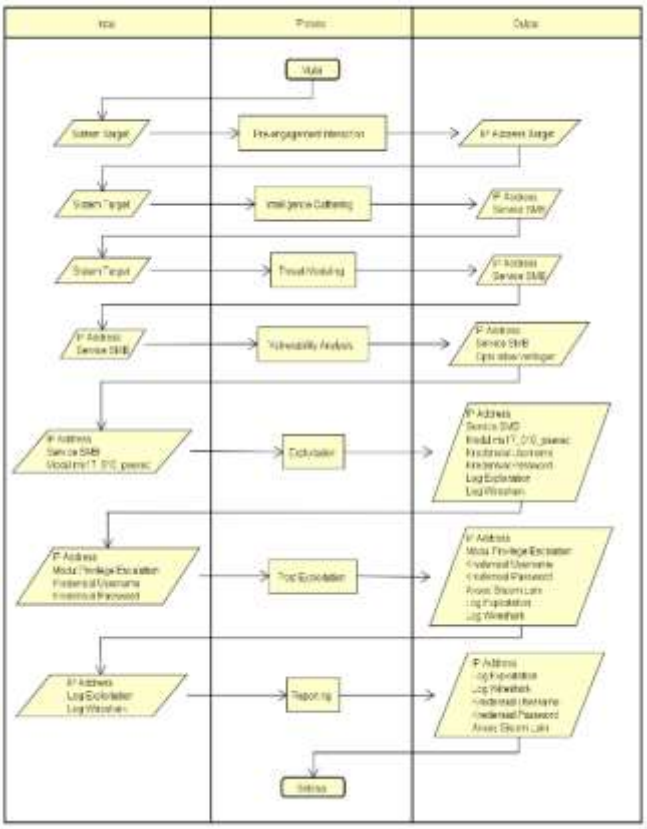
Dalam melakukan penelitian ini, peneliti melakukan tahapan kegiatan dengan mengikuti model Penetration Testing Execution Standard yang dapat dilihat pada Gambar 3 sampai dengan Gambar 6. Kerangka Penelitian Missing Patch menjelaskan proses data yang diproses pada Diagram IPO di atas melalui 7 tahap sesuai dengan tahap pada metode Penetration Testing Execution Standard. Patch adalah sekumpulan perubahan pada program komputer atau data pendukungnya yang dirancang untuk memperbarui, memperbaiki, atau meningkatkannya. Ini termasuk memperbaiki kerentanan keamanan dan bug lainnya, dengan tambalan seperti itu biasanya disebut bugfixes atau bug fixes.



Gambar 3. Kerangka Penelitian Missing Patch

Kerangka Penelitian Lack of OS Hardening menjelaskan proses data yang diproses pada Diagram IPO di atas melalui 7 tahap sesuai dengan tahap pada metode Penetration Testing Execution Standard. Pengerasan

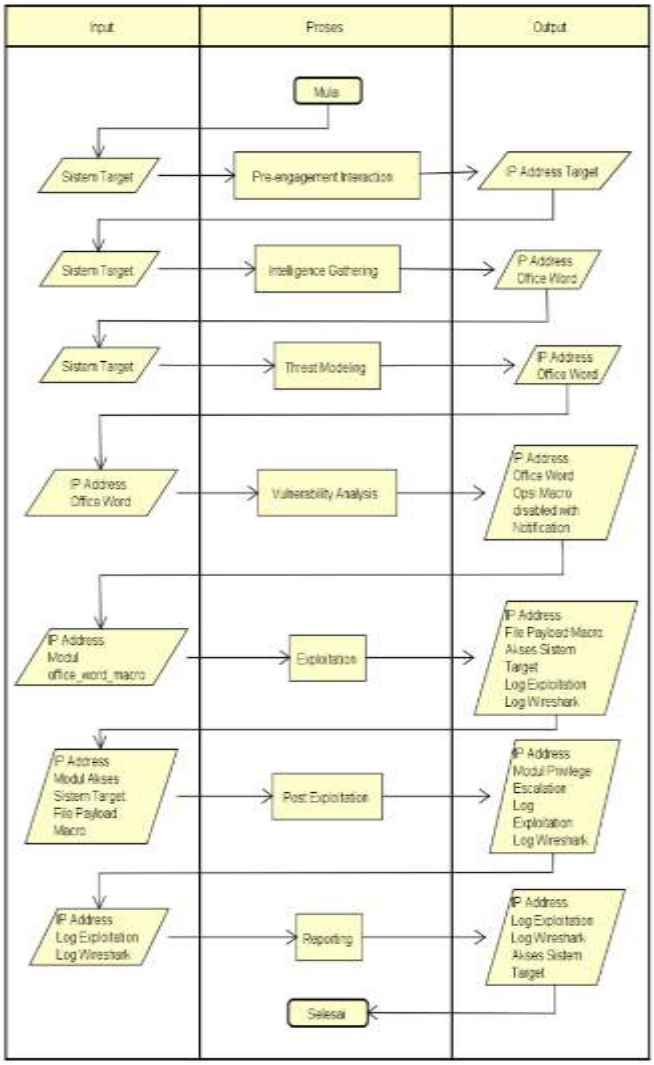
Operating System adalah tindakan untuk mengkonfigurasi Operating System dengan aman, memperbaruinya, membuat aturan dan kebijakan untuk membantu mengatur sistem dengan cara yang aman, dan menghapus aplikasi dan layanan yang tidak perlu. Ini dilakukan untuk meminimalkan paparan Operating System komputer terhadap ancaman dan untuk mengurangi kemungkinan risiko [13].



Gambar 4. Kerangka Penelitian Lack of OS Hardening

Kerangka Penelitian Lack of Application Hardening menjelaskan proses data yang diproses pada Diagram IPO di atas melalui 7 tahap sesuai dengan tahap pada metode Penetration Testing Execution Standard. Pengerasan aplikasi, juga dikenal sebagai pelindung bagi aplikasi, adalah sebuah tindakan yang menerapkan tingkat keamanan untuk melindungi aplikasi dari pencurian IP, penyalahgunaan, eksploitasi kerentanan, gangguan atau bahkan repacking oleh orang-orang yang mempunyai tujuan buruk [14]

Kerangka Penelitian Easily Guessable Credentials menjelaskan proses data yang diproses pada Diagram IPO di atas melalui 7 tahap sesuai dengan tahap pada metode Penetration Testing Execution Standard. Memindai kredensial yang lemah menghasilkan tingkat pengembalian yang tinggi untuk mengidentifikasi risiko. Kondisi yang ditemukan pada masing-masing host berpotensi memungkinkan siapa pun yang memiliki akses ke perangkat, kemampuan untuk mengkonfigurasinya sesuka mereka [15].



Gambar 5. Kerangka Penelitian Lack of Application Hardening

PTES

Pada tahapan ini, peneliti mengimplementasikan metode PTES yang mempunyai 7 tahapan, yaitu:

Pre-engagements Interaction

Pada tahap ini, peneliti meminta izin kepada pihak yang ditesting untuk melakukan penetration testing pada Sistem Target.

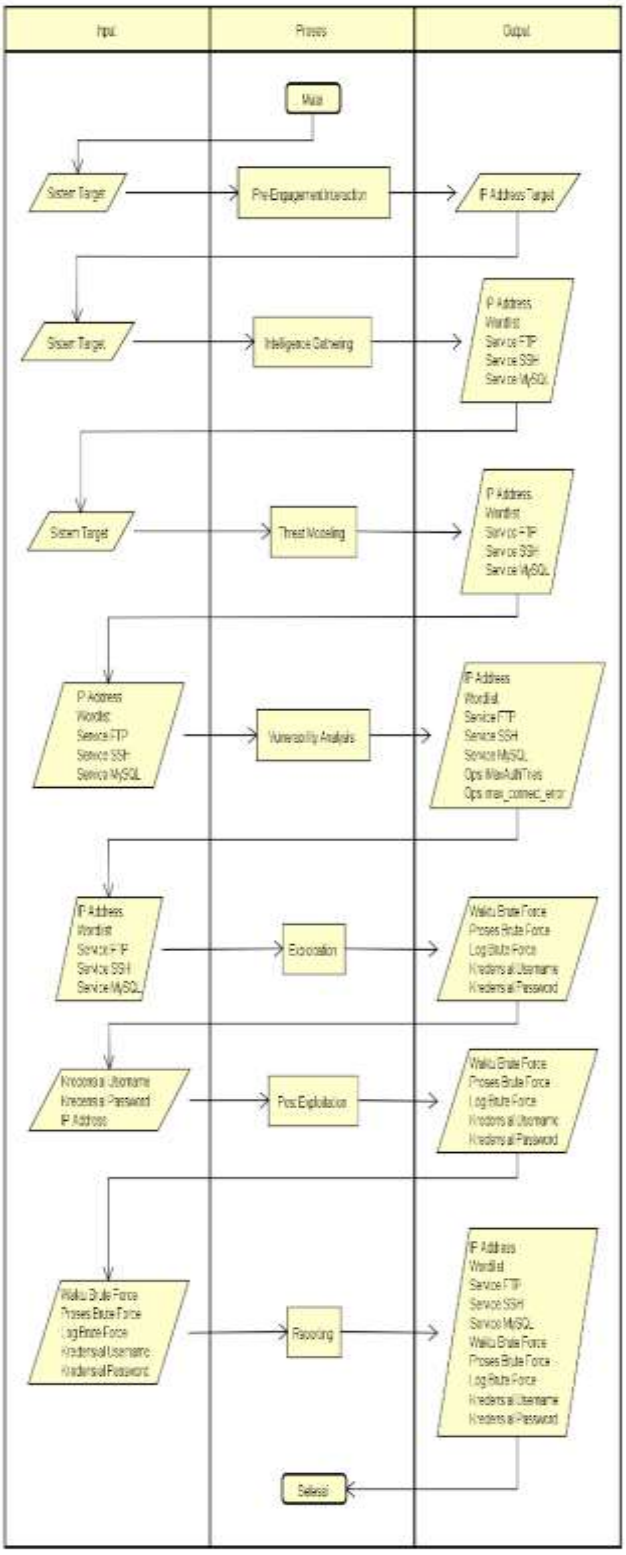
Intelligence Gathering

Pada tahap ini, peneliti dapat mengumpulkan informasi terhadap Sistem Target untuk menghasilkan representasi yang dapat dimengerti.

Threat Modeling

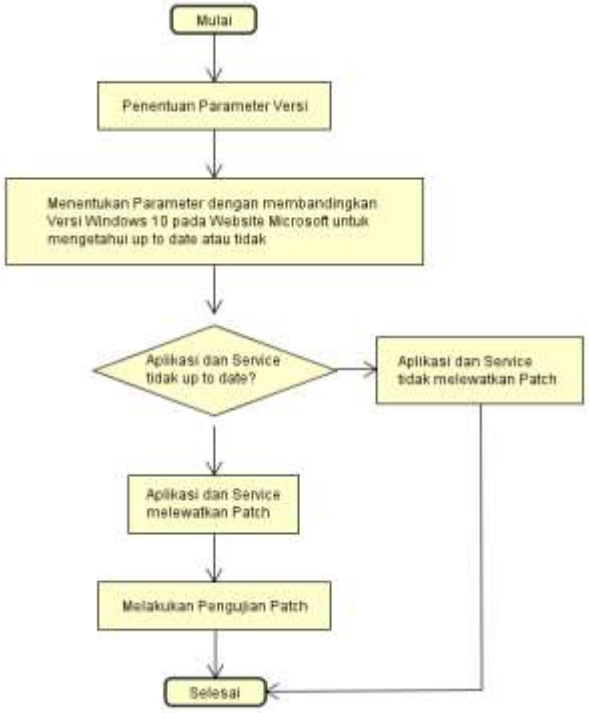
Pada tahap ini, peneliti dapat menentukan model atau jenis ancaman yang memungkinkan setelah memperoleh informasi berdasarkan tahapan sebelumnya, seperti dijelaskan di bawah ini:

Scenario pengujian penetrasi yang dilakukan dalam penelitian ini yaitu menguji suatu sistem keamanan aplikasi dan service Windows menggunakan tools uji penetrasi nmap, metasploit framework.



Gambar 6. Kerangka Penelitian Easily Guessable Credentials

1. Scenario Serangan: Missing Patch.

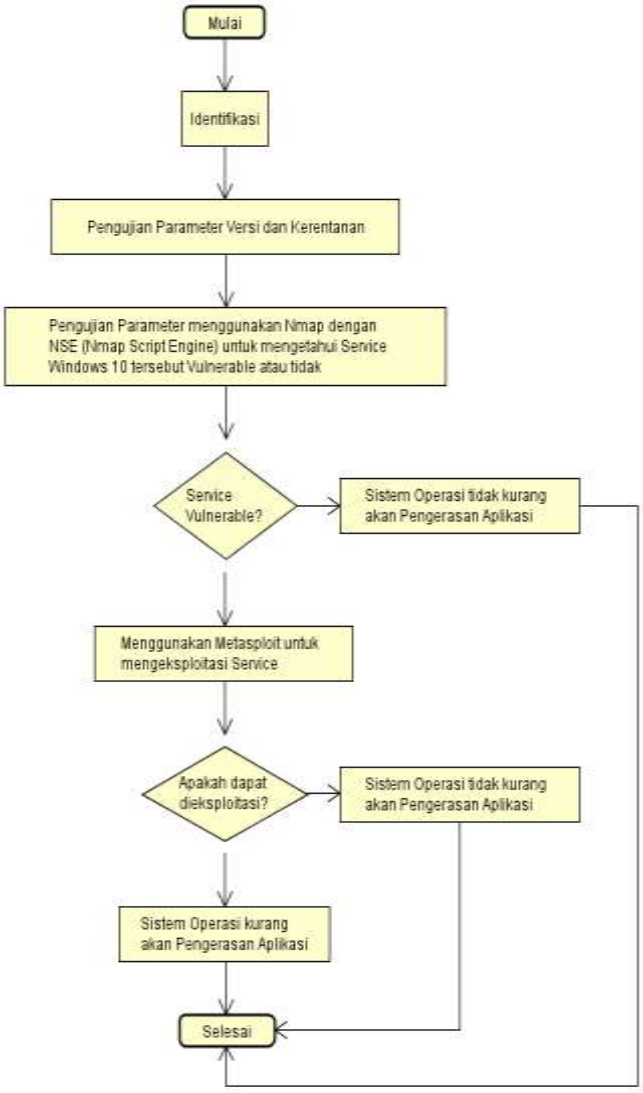


Gambar 7. Scenario Serangan Missing Patch

Scenario Serangan: *Missing Patch* dilakukan dengan tahapan seperti gambar 7 dan langkah-langkahnya dijelaskan sebagai berikut:

1. Mengidentifikasi parameter *Missing Patch*, yaitu Versi.
2. Pengujian manual dilakukan dengan cara melihat versi *Windows 10*, setelah ditemukan versi berapa aplikasi/*service Windows* tersebut, maka dapat dicek dengan https://docs.microsoft.com/en-us/windows/release-information/resolved-issues-windows-10-1903. Apakah versi pada aplikasi bawaan atau *service* pada *Windows 10* tersebut sudah *up to date* atau tidak.
3. Setelah ditemukan bahwa versi yang ada pada aplikasi bawaan atau *service Windows* tersebut di bawah dibandingkan dengan versi yang ada pada website resmi *Microsoft* pada url https://docs.microsoft.com/en-us/windows/release-information/resolved-issues-windows-10-1903, maka aplikasi bawaan atau *service* pada *Windows 10* tersebut melewatkan *patch* (*Missing Patch*).
4. Lalu dilakukan pengujian terhadap *bug* (kerentanan) yang dilewatkan tersebut dengan mendownload *patch* terkait dan memproduksi kembali *bug* (kerentanan) yang dialami sebelumnya dan membuktikan bahwa *bug* (kerentanan) sudah tidak dialami setelah men-*download* dan menginstal *patch* untuk *bug* (kerentanan) tersebut.

2. Scenario Serangan: Lack of OS Hardening.

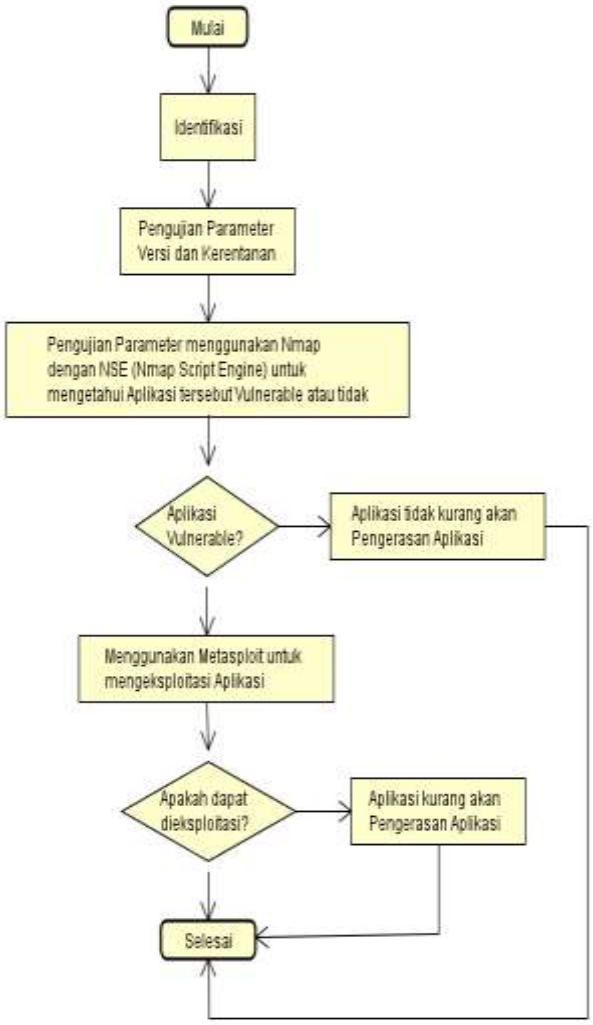


Gambar 8. Scenario Serangan Lack of OS Hardening

Scenario Serangan: *Lack of OS Hardening* dilakukan dengan tahapan seperti gambar 8 dan langkah-langkahnya dijelaskan sebagai berikut:

1. Mengidentifikasi parameter *Lack of OS Hardening*, yaitu Versi dan Kerentanan.
2. Pengujian Otomatis dilakukan menggunakan *Tools nmap* dan *Metasploit Framework*. *Nmap* digunakan untuk mendeteksi versi *Service Windows 10* dan mengetahui apakah *service* yang dilakukan *scanning* itu rentan atau tidak.
3. *Nmap* mempunyai *script* khusus untuk mengetahui apakah sebuah *service* itu rentan atau tidak dengan menjalankan *NSE* (*Nmap Script Engine*). Setelah diketahui bahwa *service* tersebut rentan, maka dapat dilanjutkan ke tahap Analisa pengujian.
4. Pada tahap Analisa pengujian, peneliti menggunakan *Metasploit Framework* untuk mengeksploitasi kerentanan yang sebelumnya diketahui menggunakan *Nmap*. *Service* yang tereksploitasi ini masuk ke dalam kategori *Lack of OS Hardening*.

3. Scenario Serangan: Lack of Application Hardening

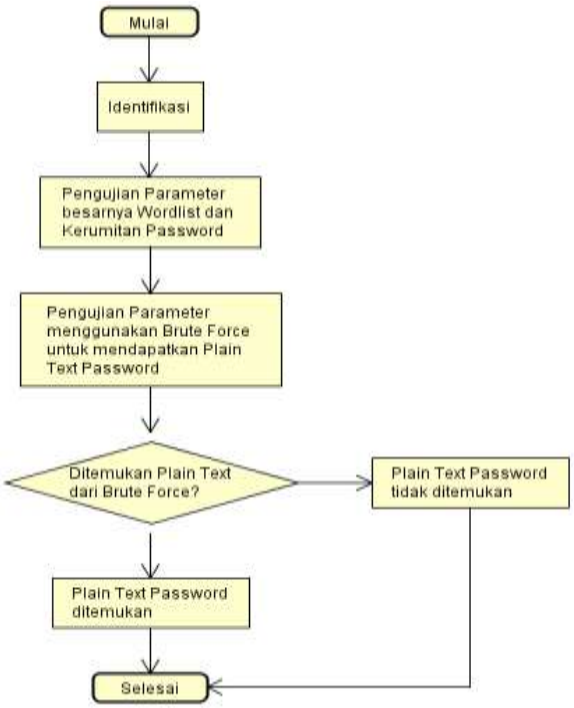


Gambar 9. Scenario Serangan Lack of Application Hardening

Scenario Serangan: *Lack of Application Hardening* dilakukan dengan tahapan seperti gambar 9 dan langkah-langkahnya dijelaskan sebagai berikut:

1. Mengidentifikasi parameter *Lack of Application Hardening*, yaitu Versi dan Kerentanan.
2. Pengujian Otomatis dilakukan menggunakan *Tools Nmap* dan *Metasploit Framework*. *Nmap* digunakan untuk mendeteksi versi Aplikasi bawaan yang ada pada *Windows 10* dan mengetahui apakah aplikasi yang dilakukan *scanning* itu rentan atau tidak.
3. Penggunaan *NSE* (*Nmap Script Engine*) untuk mengetahui Aplikasi yang dilakukan *scanning*, *vulnerable* atau tidak.
4. Setelah diketahui bahwa Aplikasi bawaan tersebut *vulnerable*, maka dapat dieksploitasi menggunakan *Metasploit Framework* dan jika berhasil dieksploitasi, maka Aplikasi bawaan *Windows 10* tersebut masuk ke dalam kategori *Lack of Application Hardening*.

4. Scenario Serangan: Easily Guessable Credentials



Gambar 10. Scenario Serangan Easily Guessable Credentials

Scenario Serangan: *Easily Guessable Credentials* dilakukan dengan tahapan seperti gambar 10 dan langkah-langkahnya dijelaskan sebagai berikut:

1. Mengidentifikasi parameter *Easily Guessable Credentials*, yaitu besarnya *wordlist* dan kerumitan *password*.
2. Pengujian penetrasi dilakukan dengan cara menggunakan tools bernama Hydra, dengan cara memasukkan user yang digunakan pada service FTP/SSH/MySQL, kemudian memasukkan wordlist yang digunakan dan dijalankan proses brute force tersebut.
3. Setelah proses brute force selesai pada hydra, maka dapat dilihat pada akhir log bahwa hydra menemukan atau tidak menemukan password yang digunakan pada service FTP/SSH/MySQL tersebut.
4. *Vulnerability analysis*, pada tahap ini, peneliti dapat menggabungkan tahapan *intelligence gathering* dan *threat modeling* untuk dapat melanjutkan ke tahap *exploitation* supaya pada tahap *exploitation*, dapat langsung menguji kerentanan yang didapat pada hasil di tahap *vulnerability analysis*.
5. *Exploitation*, pada tahap ini, peneliti melakukan exploitasi kepada sistem *Target*, exploitasi ini dilakukan berdasarkan pada tahapan sebelumnya, yaitu tahap *vulnerability analysis*.
6. *Post exploitation*, pada tahap ini, peneliti sudah harus bisa melakukan *penetration testing* terhadap sistem *Target* dan berusaha untuk mempertahankan akses pada sistem *Target* atau bahkan dapat memiliki hak akses paling tinggi pada sistem *Target*.

Vulnerability Analysis

Pada tahap ini, peneliti dapat menggabungkan tahapan intelligence gathering dan threat modeling untuk dapat melanjutkan ke tahap exploitation supaya pada tahap exploitation, dapat langsung menguji kerentanan yang didapat pada hasil di tahap vulnerability analysis.

Exploitation

Pada tahap ini, peneliti melakukan exploitasi kepada sistem Target, exploitasi ini dilakukan berdasarkan pada tahapan sebelumnya, yaitu tahap vulnerability analysis.

Post Exploitation

Pada tahap ini, peneliti sudah harus bisa melakukan penetration testing terhadap sistem Target dan berusaha untuk mempertahankan akses pada sistem Target atau bahkan dapat memiliki hak akses paling tinggi pada sistem Target.

Reporting

Pada tahap ini, peneliti dapat memberikan laporan terhadap Target tentang kerentanan yang ada pada sistem Target.

HASIL DAN PEMBAHASAN

Hasil dan Pembahasan untuk Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES).

Missing Patch

Bahwa bug (kerentanan) masalah kompabilitas software Avast terjadi dikarenakan masalah update Windows 10 Anniversary Update dengan CPU Intel Skylake yang menggunakan Virtualilzation Technology (Intel VT) pada BIOS yang membuat sistem Target menyebabkan blue screen of death. Masalah ini dapat diselesaikan dengan cara download aplikasi Avast versi terakhir pada website resmi Avast.

Lack of Operating System Hardening

Vulnerability dari port SMB pada Sistem Target yaitu ada fungsi bernama srv!SrvOS2FeaListSizeToNt, yang digunakan untuk menghitung ukuran yang diperlukan untuk mengubah struktur Daftar OS/2 Full Extended Attributes (FEA) menjadi struktur NT FEA yang sesuai. Struktur ini digunakan untuk menggambarkan karakteristik file. Fungsi penghitungan ini tidak ada di Microsoft Windows 10, seperti yang telah diatur oleh kompiler. Kerentanan demikian muncul di srv!SrvOs2FeaListToNt. Kemudian modul ms17_010_psexec mengotomasi proses exploitasi dari pengecekan versi dari Sistem Target sampai melanjutkan memilih Target dan proses pengiriman dan eksekusi payload yang dikirim ke Sistem Target.

Lack of Application Hardening

Vulnerability pada Office Word khususnya pada fitur Macro, dapat membuka peluang bagi Penyerang untuk mengambil alih Sistem Target dikarenakan Macro sendiri

dapat mengeksekusi kode pada Sistem Windows 10 dan dapat dimanfaatkan untuk mengeksekusi kode berbahaya.

Easily Guessable Credentials

Dari 6 kategori wordlist yang digunakan terhadap service FTP dan SSH, lalu 5 kategori wordlist yang digunakan terhadap service MySQL, hanya wordlist custom saja yang dapat masuk ke dalam sistem Target. Bahwa password yang berupa gabungan dari 2 kata masih belum aman, karena masih dapat ditebak dengan cepat dan password hanya dalam lowercase.

KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil dari Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES) yang terdiri dari 4 hal yaitu ditemukan kerentanan (vulnerability) pada sistem operasi Windows 10, pertama kategori Lack of Operating System Hardening yaitu sistem target mempunyai kelemahan yang dapat dieksploitasi dan peneliti dapat menguasai sistem target setelah ditemukan kerentanan melalui 7 proses Pre-engagements Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation hingga Reporting dengan menggunakan Model Penetration Testing Execution Standard (PTES). Kedua yaitu kategori Easily Guessable Credentials, bahwa Sistem Target menggunakan password yang kurang kuat dan masih mudah ditebak. Ketiga yaitu kategori Missing Patch, Sistem Target mempunyai aplikasi yang sudah out of date dan menyebabkan Windows 10 untuk crash dikarenakan masalah kompabilitas antara aplikasi dan sistem operasi. Dan keempat yaitu kategori Lack of Application Hardening, bahwa Sistem Target mempunyai aplikasi office di mana fitur Macro aktif dengan opsi “Disable all macros with notification” dan dapat dimanfaatkan oleh Peneliti untuk menguasai Sistem Target.

Untuk penelitian selanjutnya dapat dilakukan pengujian yang dapat mencakup lebih banyak kategori dan dilakukan analisis pengujian dengan lebih detil, tidak hanya dilihat dari sisi network packet yang mengalir pada saat dilakukan pengujian penetrasi.

Daftar Pustaka

[1] W, Y., Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing. *Annual Research Seminar*, 300.

[2] Astuti, E. F., & Sari, P. K. (2019). Analisis Budaya Keamanan Informasi di Klinik Pratama Kota Bandung. Jurnal Mitra Manajemen (JMM Online), 3, 316-317.

[3] Ariyani, F., Krisnawati, M., T, Y. K., & Nurhidayah, I. (2014). *Makalah Keamanan Sistem.* Retrieved Desember 16, 2019, from Makalah Keamanan Sistem: https://www.academia.edu/25732897/Makalah_Keamanan_Sistem

[4] Asy'ari, M. F., Budiyono, A., & Widjajarto, A. (2019). Analisa Parameter Ethereum Pada Jaringan Peer To Peer Blockchain Di Aplikasi Transfer Koin Terhadap Aspek Processor. e-Proceeding of Engineering, 7648.

[5] Choi, S.-K., Yang, C.-H., & Kwak, J. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. KSII Transactions On Internet And Information Systems, 906-918.

[6] Stiawan, D., Idris, M. Y., Abdullah, A. H., AlQurashi, M., & Budiarto, R. (2016). Penetration Testing and Mitigation of Vulnerabilities Windows Server. International Journal of Network Security, Vol 18, No.3, 501-513.

[7] Myerson, T. (2015). *Hello World: Windows 10 Available on July 29 | Windows Experience Blog*. Retrieved from Hello World: Windows 10 Available on July 29: https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/

[8] Microsoft. (2019). *Resolved issues in Windows 10, version 1903 and Windows Server, version 1903*. Retrieved from Resolved issues in Windows 10, version 1903 and Windows Server, version 1903: https://docs.microsoft.com/en-us/windows/release-information/resolved-issues-windows-10-1903

[9] Interior, U. D. (2018). *What is Penetration Testing?* Retrieved from Penetration Testing | U.S. Department of the Interior: https://www.doi.gov/ocio/customers/penetration-testing

[10] PCI Security Standards Council. (2015). Penetration Testing Guidance. Retrieved from Penetration Testing Guidance: https://www.pcisecuritystandards.org

[11] Wulandari, R. (2016). Analisis QoS (Quality of Service) pada Jaringan Internet (Studi Kasus: UPT Loka Uji Teknik Penambangan Jampang Kulon - LIPI). Jurnal Teknik Informatika dan Sistem Informasi, 2, 164-165.

[12] Smith, H. (2019, May 24). *6 Important OS Hardening Steps to Protect Your Clients*. Retrieved from ConnectWise: https://www.continuum.net/blog/6-important-steps-to-harden-your-clients-operating-systems

[13] Butterworth, P. (2019, October 24). *Application Hardening Methods and Benefits - Intertrust Technologies*. Retrieved from Intertrust: https://www.intertrust.com/blog/application-hardening-and-its-importance/

[14] Asadoorian, P. (2010, November 23). *Scanning For Default & Common Credentials Using Nessus*. Retrieved from Tenable: https://www.tenable.com/blog/scanning-for-default-common-credentials-using-nessus