Jurnal Rekursif, Volume 14 Nomor 1, Maret 2026, ISSN 2303-0755, e-ISSN 2777-0427
https://ejournal.unib.ac.id/index.php/rekursif/

UJI *PRIVILEGE ESCALATION* PADA LAB *VULNHUB LIN.SECURITY* MENGGUNAKAN *TACTIC FRAMEWORK PRIVILEGE ESCALATION MITRE ATT&CK* DENGAN METODE *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK* (ISSAF)

Muhammad Willdhan Arya Putra[1], Funny Farady Coastera[2], Tiara Eka Putri[3]

[1,2] Program Studi Informatika, FakultasTeknik, Universitas Bengkulu
[3]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Bengkulu
Jl. WR. Supratman, Kandang Limun, Bengkulu (38271A) INDONESIA

[1]aryaputrascorpio@gmail.com
[2]ffaradyc@unib.ac.id
[3]tiaraekaputri@unib.ac.id

Abstrak: Penelitian ini bertujuan mengidentifikasi dan mengevaluasi teknik privilege escalation pada sistem operasi Linux menggunakan metode Information System Security Assessment Framework (ISSAF) dan taktik dari MITRE ATT&CK. Pengujian dilakukan pada lab VulnHub Lin.Security yang rentan. Tahapan meliputi perencanaan (konfigurasi VirtualBox), assessment (enumerasi sistem dan pengujian 7 taktik MITRE ATT&CK: Abuse Elevation Control Mechanism, Account Manipulation, Create or Modify System Process, Escape to Host, Event Triggered Execution, Exploitation for Privilege Escalation, Hijack Execution Flow), dan pelaporan. Hasil menunjukkan ketujuh taktik berhasil dieksploitasi pada lingkungan lab, mengungkap kerentanan seperti miskonfigurasi SetUID/SetGID, sudo, SSH keys, systemd, docker SUID, file konfigurasi shell, kerentanan kernel (PwnKit), dan LD_PRELOAD. Kesimpulan utama adalah kerentanan privilege escalation pada sistem Linux dapat dieksploitasi menggunakan taktik MITRE ATT&CK, menekankan pentingnya audit keamanan dan pembaruan berkala untuk mitigasi risiko.
Kata Kunci: Privilege Escalation, ISSAF, MITRE ATT&CK, Linux, Keamanan Sistem Operasi, VulnHub.

Abstract: This study aims to identify and evaluate privilege escalation techniques on Linux kernel-based operating systems using the Information System Security Assessment Framework (ISSAF) methodology and MITRE ATT&CK tactics. The research was conducted in the vulnerable VulnHub Lin.Security lab. Phases included planning (VirtualBox configuration), assessment (system enumeration and testing of 7 MITRE ATT&CK tactics: Abuse Elevation Control Mechanism, Account Manipulation, Create or Modify System Process, Escape to Host, Event Triggered Execution, Exploitation for Privilege Escalation, Hijack Execution Flow), and reporting. Results showed all seven tactics were successfully exploited in the lab environment, revealing vulnerabilities such as SetUID/SetGID misconfiguration, sudo issues, SSH key manipulation, systemd misuse, docker SUID exploitation, shell configuration file vulnerabilities, kernel exploits (PwnKit), and LD_PRELOAD hijacking. The main conclusion is that privilege escalation vulnerabilities in Linux systems can be exploited using MITRE ATT&CK tactics, emphasizing the importance of regular security audits and updates for risk mitigation.
Keywords: Privilege Escalation, ISSAF, MITRE ATT&CK, Linux, Operating System Security, VulnHub.

I. PENDAHULUAN

Keamanan siber merupakan isu krusial di era digital, dengan insiden seperti kebocoran data dan serangan ransomware yang terus meningkat,

termasuk di Indonesia [10]. Salah satu vektor serangan kritis setelah penyerang mendapatkan akses awal ke sistem adalah privilege escalation. Teknik ini memungkinkan penyerang dengan hak akses terbatas untuk mendapatkan hak akses yang lebih tinggi (seringkali root atau administrator), memberikan kontrol penuh atas sistem [14]. Dampaknya bisa sangat merusak, mulai dari defacement, pencurian data sensitif, hingga penanaman malware persisten.

Meskipun banyak metode pengujian penetrasi fokus pada lapisan aplikasi atau jaringan [1], [18], [21], evaluasi keamanan pada lapisan sistem operasi seringkali kurang mendapat perhatian komprehensif. Padahal, kerentanan pada level ini dapat memfasilitasi pengambilalihan sistem secara total. Framework seperti MITRE ATT&CK menyediakan basis pengetahuan taktik dan teknik penyerangan berdasarkan insiden nyata, termasuk 14 teknik untuk privilege escalation (Tactic TA0004) pada sistem Linux dan Windows [16].

Untuk memfasilitasi pembelajaran dan pengujian teknik keamanan secara etis, platform seperti VulnHub menyediakan lingkungan laboratorium virtual yang sengaja dibuat rentan [23], [24]. Penelitian ini menggunakan lab Lin.Security dari VulnHub, sebuah lingkungan berbasis kernel Linux, yang relevan mengingat dominasi Linux di infrastruktur server [22].

Penelitian sebelumnya yang menggunakan metode Information System Security Assessment Framework (ISSAF) [11] seringkali fokus pada aplikasi web [10], [21] atau jaringan nirkabel [19], dan terkadang melewatkan tahap privilege escalation secara mendalam [12]. ISSAF sendiri merupakan metodologi terstruktur untuk asesmen keamanan sistem, jaringan, atau aplikasi, terdiri dari fase Planning and Preparation, Assessment, dan Reporting, Clean-up and Destroy Artefacts [11].

Oleh karena itu, penelitian ini bertujuan untuk: (1) Menganalisis penerapan taktik privilege escalation dari framework MITRE ATT&CK pada sistem operasi berbasis kernel Linux di lab VulnHub Lin.Security. (2) Menerapkan metode ISSAF untuk mengidentifikasi, mengevaluasi, dan merekomendasikan mitigasi kerentanan privilege escalation pada lab tersebut. Penelitian ini berfokus pada 7 taktik privilege escalation dari MITRE ATT&CK yang relevan dengan lingkungan Linux.

II. LANDASAN TEORI

A. Penetration Testing dan ISSAF

Penetration Testing adalah proses simulasi serangan siber untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan dalam sistem atau jaringan [15], [20]. Tujuannya adalah untuk mengevaluasi postur keamanan dan memberikan rekomendasi perbaikan. Salah satu metodologi yang dapat digunakan adalah ISSAF, yang menyediakan pendekatan sistematis melalui tiga fase utama: Planning, Assessment, dan Reporting [11]. Fase Assessment mencakup langkah-langkah seperti pengumpulan informasi (information gathering), identifikasi kerentanan (vulnerability identification), penetrasi, perolehan akses dan privilege escalation, enumerasi lebih lanjut, dan pemeliharaan akses [11].

B. Privilege Escalation dan MITRE ATT&CK

Privilege Escalation (TA0004) adalah proses mendapatkan hak akses yang lebih tinggi dari yang dimiliki saat ini [14], [16]. Framework MITRE ATT&CK mendokumentasikan berbagai taktik dan teknik yang digunakan penyerang. Untuk privilege escalation di Linux, beberapa teknik relevan yang diuji dalam penelitian ini meliputi [16]:

1. Abuse Elevation Control Mechanism (T1548): Mengeksploitasi mekanisme kontrol akses seperti SetUID/SetGID bits (T1548.001) atau konfigurasi Sudo (T1548.003). File dengan bit SetUID/SetGID berjalan dengan hak akses pemilik/grup file tersebut, bukan pengguna yang menjalankan [8]. Sudo memungkinkan pengguna biasa menjalankan perintah sebagai root jika dikonfigurasi secara tidak aman [8].
2. Account Manipulation (T1098): Memodifikasi akun pengguna, contohnya menambahkan kunci SSH penyerang ke authorized_keys (T1098.004) untuk akses persisten tanpa password [8].
3. Create or Modify System Process (T1543): Membuat atau mengubah proses sistem seperti Systemd Service (T1543.002) untuk menjalankan kode berbahaya dengan hak akses tinggi saat service dimulai [8].
4. Escape to Host (T1611): Keluar dari lingkungan terbatas seperti kontainer (misalnya Docker) ke sistem host utama, seringkali dengan mengeksploitasi konfigurasi SUID pada binary Docker atau mounting filesystem host [8].
5. Event Triggered Execution (T1546): Mengeksekusi kode berdasarkan pemicu sistem, contohnya memodifikasi file konfigurasi shell seperti .bashrc atau .bash_profile (T1546.004) yang dieksekusi saat pengguna login [8].
6. Exploitation for Privilege Escalation (T1068): Mengeksploitasi bug atau kerentanan perangkat lunak pada kernel atau aplikasi (seperti PwnKit/CVE-2021-403) untuk mendapatkan hak akses root [8].
7. Hijack Execution Flow (T1574): Membajak alur eksekusi program, misalnya melalui Dynamic Linker Hijacking (T1574.006) dengan variabel lingkungan LD_PRELOAD untuk memuat library berbahaya, atau Path Interception (T1574.007) dengan memanipulasi variabel PATH pada script yang dijalankan Crontab [8], [9].

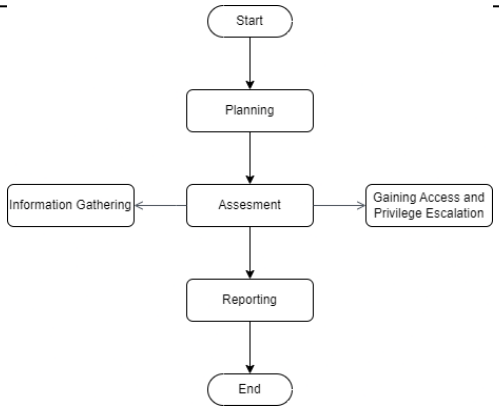
C. VulnHub

VulnHub adalah platform yang menyediakan Virtual Machine (VM) yang sengaja dibuat rentan untuk tujuan pelatihan dan pengujian keamanan siber secara legal dan etis [23], [24]. Lab Lin.Security yang digunakan dalam penelitian ini adalah salah satu VM yang tersedia di VulnHub.

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan penelitian terapan dengan metode observasi teknis dan studi kasus. Objek penelitian adalah lab virtual VulnHub Lin.Security, sebuah sistem operasi berbasis kernel Linux yang dirancang memiliki kerentanan. Tujuan utama adalah mengidentifikasi dan mengevaluasi kerentanan privilege escalation menggunakan kerangka kerja ISSAF [11] sebagai panduan metodologi dan framework MITRE ATT&CK [16] sebagai basis pengetahuan taktik dan teknik penyerangan.

Alur penelitian mengikuti tiga fase utama dari metodologi ISSAF, sebagaimana digambarkan secara ringkas pada Gambar 1:



Gambar 1. Diagram Alir Metode Penelitian

A. Planning and Preparation

Tahap ini melibatkan persiapan lingkungan pengujian. Virtual Machine (VM) Lin.Security dijalankan menggunakan VirtualBox versi 7.0. Konfigurasi sumber daya VM diatur sesuai kebutuhan minimum untuk menjalankan lab dan alat pengujian, meliputi:

- Prosesor: 2 CPU Core
- Memori Dasar: 2048 MB
- Memori Video: 16 MB
- Adapter Jaringan: 1 (mode Bridged)

Spesifikasi ini dianggap cukup untuk menjalankan command-line interface (CLI) dan proses pengujian yang tidak terlalu intensif sumber daya.

B. Assessment

Fase ini merupakan inti dari pengujian, terdiri dari dua sub-tahap:

1. Enumeration: Pengumpulan informasi awal mengenai sistem target dilakukan untuk mengidentifikasi potensi vektor serangan privilege escalation. Informasi yang dikumpulkan meliputi:
   - Konfigurasi Sudo (sudo -l) untuk melihat binary yang dapat dijalankan user target dengan hak akses root.
   - Versi Kernel (uname -a) untuk mencari exploit kernel yang relevan.
   - File dengan bit SetUID dan SetGID (find / -perm -u=s atau -g=s) yang berpotensi disalahgunakan.
   - Informasi Pengguna Sistem (cat /etc/passwd, grep home /etc/passwd) untuk mengidentifikasi pengguna aktif dan direktori home mereka.
2. Privilege Escalation Testing: Berdasarkan hasil enumerasi, dilakukan pengujian terhadap 7 taktik privilege escalation dari framework MITRE ATT&CK yang relevan dengan sistem Linux:
   - Abuse Elevation Control Mechanism: Menguji eksploitasi file SetUID/SetGID dan konfigurasi Sudo, seringkali merujuk pada database GTFOBins untuk payload.
   - Account Manipulation: Menguji penambahan kunci SSH ke ~/.ssh/authorized_keys milik user root.
   - Create or Modify System Process: Menguji pembuatan malicious Systemd Service yang memberikan reverse shell.
   - Escape to Host: Menguji eksploitasi binary Docker dengan SUID untuk mount filesystem host dan mendapatkan shell host.
   - Event Triggered Execution: Menguji modifikasi file .bashrc atau .bash_profile untuk mengeksekusi reverse shell saat user login.
   - Exploitation for Privilege Escalation: Menguji exploit kernel yang diketahui (seperti PwnKit CVE-2021-403) berdasarkan versi kernel yang ditemukan saat enumerasi.
   - Hijack Execution Flow: Menguji pembajakan LD_PRELOAD pada binary yang dijalankan via Sudo dan

Path Interception pada script yang dijalankan oleh Crontab.

C. Reporting, Clean-up and Destroy Artefacts

Tahap akhir meliputi analisis hasil pengujian dari fase assessment. Semua temuan kerentanan yang berhasil dieksploitasi didokumentasikan. Berdasarkan temuan tersebut, disusun rekomendasi mitigasi untuk setiap teknik privilege escalation yang berhasil. Artefak atau perubahan yang dibuat selama pengujian (misalnya, file script, service baru) idealnya dibersihkan dari sistem target setelah pengujian selesai, meskipun dalam konteks lab VulnHub ini tidak wajib.

IV. HASIL DAN PEMBAHASAN

Tahap ini memaparkan temuan dari penerapan metodologi ISSAF pada lab VulnHub Lin.Security, fokus pada fase assessment yang meliputi enumerasi dan pengujian teknik privilege escalation MITRE ATT&CK.

A. Hasil Enumerasi

Pengumpulan informasi awal mengungkapkan beberapa konfigurasi dan atribut sistem yang krusial untuk tahap pengujian:

I. Konfigurasi Sudo: Perintah sudo -l untuk user target (bob) menunjukkan daftar binary yang luas yang dapat dijalankan dengan hak akses root, termasuk binary seperti find, pkexec, docker, systemctl, dan lainnya. Konfigurasi ini sangat permisif.

II. Informasi Kernel: Perintah uname -a menunjukkan sistem menjalankan kernel Linux versi 4.15.0-213-generic pada Ubuntu 18.04 LTS, yang diketahui rentan terhadap exploit PwnKit (CVE-2021-403).

III. File SetUID/SetGID: Pencarian menggunakan find mengidentifikasi sejumlah binary dengan bit SetUID atau SetGID aktif, salah satunya seperti /usr/bin/find, /usr/bin/pkexec, ataupun /usr/bin/docker.

IV. User Sistem: Analisis /etc/passwd mengidentifikasi beberapa user dengan direktori home, termasuk bob, peter, susan, dan root.

B. Pengujian Taktik Privilege Escalation MITRE ATT&CK

Berdasarkan hasil enumerasi, 7 taktik MITRE ATT&CK diuji. Semua taktik berhasil dieksploitasi pada lingkungan lab ini, seperti dijelaskan di bawah ini:

1. Abuse Elevation Control Mechanism (T1548)

- SetUID/SetGID (T1548.001): Binary /usr/bin/find yang memiliki bit SetUID berhasil dieksploitasi. Merujuk pada GTFOBins, perintah find . -exec /bin/sh -p \; -quit digunakan untuk memperoleh shell dengan hak akses root (uid=0).
- Sudo (T1548.003): User bob memiliki hak untuk menjalankan /usr/bin/pkexec via sudo. Menggunakan payload dari GTFOBins, sudo pkexec /bin/sh, berhasil memberikan shell root.

2. Account Manipulation (T1098)

- SSH Authorized Keys (T1098.004): Dengan asumsi akses awal telah diperoleh, kunci publik SSH penyerang berhasil ditambahkan ke file /root/.ssh/authorized_keys melalui listener netcat pada port 31337 (nc -l -p 31337 | tee ~/.ssh/authorized_keys). Hal ini memungkinkan penyerang melakukan login SSH ke akun root tanpa memerlukan password.

3. Create or Modify System Process (T1543)

- Systemd Service (T1543.002): Hak sudo user bob untuk systemctl dieksploitasi. Sebuah bash script (malicious_script.sh) yang menjalankan listener reverse shell socat dibuat. Selanjutnya, file unit Systemd (malicious.service) dibuat untuk mengeksekusi script ini sebagai root dengan restart otomatis. Setelah service ditempatkan di /etc/systemd/system/ dan dijalankan (sudo systemctl start malicious.service), koneksi netcat dari mesin penyerang ke port listener (31337) berhasil mendapatkan shell root.

4. Escape to Host (T1611)

- Docker SUID: Binary /usr/bin/docker yang memiliki bit SetUID dieksploitasi. Dengan perintah docker run -v /:/mnt --rm -it alpine chroot /mnt bash, penyerang menjalankan kontainer Alpine Linux, melakukan mount filesystem root dari host ke /mnt di dalam kontainer, dan kemudian menggunakan chroot /mnt untuk memperoleh shell dengan akses penuh ke filesystem host sebagai root.

5. Event Triggered Execution (T1546)

- Unix Shell Configuration Modification (T1546.004): Perintah reverse shell socat ditambahkan ke file /root/.bash_profile. Ketika user root login (misalnya melalui SSH yang kuncinya telah ditanam), file .bash_profile dieksekusi, mengirimkan koneksi shell root ke listener netcat penyerang pada port 13337.

6. Exploitation for Privilege Escalation (T1068)

- Kernel Exploit (PwnKit): Berdasarkan identifikasi versi kernel yang rentan (Ubuntu 18.04), exploit PwnKit (CVE-2021-403) yang menargetkan pkexec diunduh dan dijalankan. Eksekusi exploit ini secara langsung berhasil memberikan shell root.

7. Hijack Execution Flow (T1574)

- Dynamic Linker Hijacking (LD_PRELOAD) (T1574.006): Konfigurasi /etc/sudoers yang mempertahankan variabel LD_PRELOAD (Defaults env_keep+=LD_PRELOAD) dieksploitasi. Sebuah shared object (exploit.so) dibuat dari kode C sederhana yang menjalankan shell dengan UID 0. Dengan menjalankan binary yang diizinkan Sudo (misal: /usr/bin/more) sambil memuat shared object berbahaya (sudo LD_PRELOAD=./exploit.so /usr/bin/more), shell root berhasil diperoleh.

- Path Interception by Crontab (T1574.007): File /etc/crontab ditemukan menjalankan script /etc/startup.sh sebagai root tanpa PATH eksplisit. Penyerang memodifikasi /etc/startup.sh untuk menyalin /bin/bash ke /tmp/rootbash dan memberikannya bit SetUID (chmod +xs /tmp/rootbash). Setelah cron job berjalan, penyerang menjalankan /tmp/rootbash -p untuk mendapatkan shell root.

C. Ringkasan Hasil Pengujian

Tabel 1 merangkum keberhasilan pengujian untuk setiap taktik MITRE ATT&CK yang dievaluasi pada lab Lin.Security.

Tabel 1. Ringkasan Hasil Pengujian Privilege Escalation

No.	Teknik Uji MITRE ATT&CK	Hasil
1.	Abuse Elevation Control Mechanism	Berhasil
2.	Account Manipulation	Berhasil
3.	Create or Modify System Process	Berhasil
4.	Escape to Host	Berhasil
5.	Event Triggered Execution	Berhasil
6.	Exploitation for Privilege Escalation	Berhasil
7.	Hijack Execution Flow	Berhasil

Hasil pengujian ini mengkonfirmasi bahwa lingkungan lab VulnHub Lin.Security secara efektif mensimulasikan berbagai vektor serangan privilege escalation yang umum. Keberhasilan eksploitasi pada semua taktik yang diuji menyoroti pentingnya konfigurasi sistem yang aman dan praktik pemeliharaan yang cermat untuk mencegah perolehan hak akses yang tidak sah.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Penelitian ini telah berhasil mengidentifikasi dan mengevaluasi teknik-teknik privilege escalation pada sistem operasi berbasis kernel Linux menggunakan lab VulnHub Lin.Security sebagai studi kasus. Dengan menerapkan metodologi ISSAF dan menguji 7 taktik spesifik dari framework MITRE ATT&CK, ditemukan bahwa semua taktik yang diuji—Abuse Elevation Control Mechanism, Account Manipulation, Create or Modify System Process, Escape to Host, Event Triggered Execution, Exploitation for Privilege Escalation, dan Hijack Execution Flow—berhasil dieksploitasi dalam lingkungan lab yang terkontrol ini.

Keberhasilan eksploitasi (100% dari taktik yang diuji) menunjukkan bahwa kerentanan yang terkait dengan miskonfigurasi SetUID/SetGID, Sudo, manajemen kunci SSH, Systemd services, Docker SUID, file konfigurasi shell, kerentanan kernel (PwnKit), dan mekanisme runtime linking (LD_PRELOAD, PATH interception) merupakan vektor serangan privilege escalation yang valid dan signifikan pada sistem Linux. Hal ini menegaskan efektivitas framework MITRE ATT&CK sebagai panduan untuk mengaudit potensi jalur serangan privilege escalation dan menyoroti pentingnya penerapan praktik keamanan yang baik untuk melindungi sistem operasi. Meskipun pengujian dilakukan pada lingkungan lab yang sengaja dibuat rentan, temuan ini memberikan wawasan berharga mengenai mekanisme serangan yang mungkin terjadi di lingkungan produksi.

B. Saran

Berdasarkan temuan kerentanan dan keberhasilan eksploitasi teknik privilege escalation, berikut adalah beberapa saran mitigasi yang dapat diterapkan untuk meningkatkan keamanan sistem operasi Linux:

1. Pembaruan Sistem Berkala: Lakukan pembaruan kernel dan perangkat lunak secara rutin untuk menambal kerentanan yang diketahui, seperti yang dieksploitasi oleh PwnKit (T1068). Gunakan perintah seperti sudo apt update && sudo apt upgrade pada sistem berbasis Debian/Ubuntu.
2. Prinsip Least Privilege:
    - Batasi penggunaan Sudo hanya untuk pengguna dan perintah yang benar-benar diperlukan. Hindari konfigurasi NOPASSWD: ALL. Konfigurasikan /etc/sudoers secara spesifik (misal: user ALL=(ALL) NOPASSWD: /usr/bin/specific_command).
    - Nonaktifkan bit SetUID dan SetGID (chmod u-s, g-s) pada binary yang tidak memerlukannya. Lakukan audit berkala menggunakan find untuk mendeteksi file dengan bit ini. Pertimbangkan penggunaan Linux Capabilities sebagai alternatif yang lebih granular.
3. Pengerasan Konfigurasi:
    - Batasi izin tulis pada file konfigurasi shell (.bashrc, .bash_profile) dan

direktori sensitif seperti ~/.ssh/. Gunakan chmod 600 ~/.ssh/authorized_keys dan chmod 700 ~/.ssh.

- Nonaktifkan atau batasi penggunaan LD_PRELOAD dalam konfigurasi Sudoers (hapus baris env_keep+=LD_PRELOAD).
- Definisikan PATH secara eksplisit dan aman dalam script yang dijalankan oleh Crontab untuk mencegah Path Interception. Gunakan absolute path untuk perintah dalam cron jobs.
- Batasi hak pengguna untuk membuat atau memodifikasi Systemd services. Terapkan Mandatory Access Control (MAC) seperti SELinux/AppArmor.

4. Keamanan Kontainer:
    - Nonaktifkan bit SUID pada binary Docker (chmod u-s /usr/bin/docker) jika tidak digunakan dengan SUID.
    - Gunakan rootless Docker atau jalankan kontainer dengan pengguna non-root.
    - Terapkan kebijakan keamanan Docker yang ketat: batasi volume mounting, nonaktifkan mode privileged, gunakan read-only volumes jika memungkinkan.
5. Pemantauan dan Audit:
    - Pantau log sistem (/var/log/auth.log untuk Sudo, log Systemd journal) untuk aktivitas mencurigakan.
    - Gunakan alat audit seperti auditd untuk memantau perubahan pada file kritis (misal: authorized_keys, konfigurasi shell, /etc/sudoers, /etc/crontab) dan eksekusi binary SetUID/SetGID.
    - Audit konfigurasi Sudo (visudo --check) dan Crontab secara berkala.
    - Monitor proses yang berjalan dan koneksi jaringan (netstat, ss) untuk mendeteksi listener atau service yang tidak dikenal.

REFERENSI

[1] Fatihah, A., & Dinarto, P. (2024). Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ. Innovative: Journal Of Social Science Research, 4(2), 4536–4549. https://doi.org/10.31004/INNOVATIVE.V4I2.9741

[2] Gede, I., Sanjaya, A. S., Made, G., Sasmita, A., Made, D., & Arsa, S. (2020). Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City). Computer Network and Information Security, 4, 30–40. https://doi.org/10.5815/ijcnis.2020.04.03

[3] Sandika, P., Muhyidin, Y., & Singasatia, D. (2024). ANALISIS KEAMANAN JARINGAN PADA WEB SERVER MENGGUNAKAN METASPLOIT FRAMEWORK DENGAN METODE INFORMATION SYSTEM SECURITY ASSESMENT FRAMEWORK (ISSAF) PADA SMKN XYZ. Scientica: Jurnal Ilmiah Sains Dan Teknologi, 2(11), 136-150–136–150. https://jurnal.kolibi.org/index.php/scientica/article/view/2757

[4] Rusdan, M., Manurung, D. T. H., & Genta, F. K. (2020). Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia). Jurnal Test Engineering And Management.

[5] Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web Application Penetration Testing on Udayana University's OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). International Journal of Information Technology and Computer Science, 16(2), 45–56. https://doi.org/10.5815/IJITCS.2024.02.04

[6] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379–398. https://doi.org/10.3390/FORENSICSCI2020028

[7] Mitraberdaya. (2024, July 23). Pelajaran Dari Kasus Kebocoran Data PDN. https://www.mitraberdaya.id/id/news-information/pelajaran-dari-kebocoran-data-pdn

[8] MITRE ATT&CK® | Privilege Escalation, Tactic TA0004. (2021, January 6). https://attack.mitre.org/tactics/TA0004/

[9] Rapid7. (2024). What is the MITRE ATT&CK Framework? Rapid7.

[10] Ardiyanti, H. (2016). Cyber Security dan Tantangan Pengembangannya di Indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5(1). https://doi.org/10.22212/JP.V5I1.336

[11] OISSG Team. (2006). Information Systems Security Assessment Framework (ISSAF) draft 0.2. OISSG.

[12] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. Nist Special Publication, 800-115. https://doi.org/10.6028/NIST.SP.800-115

[13] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. The MITRE Corporation.

[14] Jaafar, F., Nicolescu, G., & Richard, C. (2016). A Systematic Approach for Privilege Escalation Prevention. Proceedings - 2016 IEEE International Conference on Software Quality, Reliability and Security-Companion, QRS-C 2016, 101–108. https://doi.org/10.1109/QRS-C.2016.17

[15] Kumar, R., & Tlhagadikgora, K. (2019). Internal Network Penetration Testing Using Free/Open Source Tools: Network and System Administration Approach. Communications in Computer and Information Science, 956, 257–269. https://doi.org/10.1007/978-981-13-3143-5_22

[16] PTES. (2012). PTES Technical Guidelines - The Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[17] Yadu, P., & Sharma, V. (2021). A Review on Software Testing Tools and Techniques. International Journal of Advance Research in Computer Science and Management Studies, 9(7).

[18] Ariffin, N., Zainal, A., Maarof, M. A., & Nizam Kassim, M. (2018). A Conceptual Scheme for Ransomware Background Knowledge Construction. Proceedings of the 2018 Cyber Resilience Conference, CRC 2018. https://doi.org/10.1109/CR.2018.8626868

[19] Yasuhara, K., Walnycky, D., Baggili, I., Alhishwan, A., & Ahmed, A. (2022). Computer Law Commons, Defense and Security Studies Commons, Forensic Science and Technology Commons, Information Security Commons, National Security Law Commons. Annual ADFSL Conference on Digital Forensics, Security and Law. https://commons.erau.edu/adfsl/2022/presentations/1

[20] Potukuchi, R. V., & Ravindran, U. (2022). A Review on Web Application Vulnerability Assessment and Penetration Testing. Review of Computer Engineering Studies, 9, 1–22. https://doi.org/10.18280/rces.090101

[21] Oriyano, & Philip, S. (2014). CEH v8: Certified Ethical Hacker version 8 study guide (Study Guide, Vol. 8). Sybex Inc.

[22] W3Techs. (2025, April). Usage Statistics and Market Share of Operating Systems for Websites. https://w3techs.com/technologies/overview/operating_system

[23] Boekweg, K. I. (2024). Developing a SQL Injection Exploitation Tool with Natural Language Generation. https://scholarsarchive.byu.edu/etd

[24] Wilson, B. (2024). About ~ VulnHub. https://www.vulnhub.com/about/