CYBER VULNERABILITY MITIGATION IN WI-FI NETWORKS: INTEGRATION OF PENETRATION TESTING, SOCIAL ENGINEERING, AND SECURITY AWARENESS IN XYZ EDUCATIONAL INSTITUTION

Muhammad Fahrurozi[1], Firmansyah[2], Rezha Fauzi Ramadhan[3] , Kurniawan[4], Suroso[5], Dwikatama[6]

[1]Departemen Elektronika, Akademi Angkatan Udara; [2,3]Departemen Elektronika, Akademi Angkatan Udara,
[1]muhammad.fahrurozi@aau.ac.id; [2] firmansyah@aau.ac.id;
[3]rezha.fauzi.r@aau.ac.id;[4,5,6]ikeo.santai@gmail.com;

Abstrak — *This study aims to empirically and comprehensively assess security vulnerabilities in military Wi-Fi networks at the XYZ defense educational institution, encompassing technical aspects (penetration testing with Aircrack-ng, WPA2 encryption analysis) and human factors (social engineering, personnel security awareness). A convergent mixed-methods approach was used to integrate quantitative and qualitative data. Penetration testing conducted at four strategic locations revealed that 75 percent of the network could be breached in less than 130 minutes due to weak passwords with low entropy (less than 60 bits) and default configurations. Meanwhile, a survey of 50 personnel showed that 80 percent were unable to accurately identify phishing attacks before training, and 65 percent were vulnerable to pretexting scenarios. Vulnerability analysis using the CIA Triad framework revealed violations of Confidentiality (40 percent of traffic could be intercepted within 30m), Integrity (20 percent of the network was vulnerable to Man-in-the-Middle), and Availability (DoS through deauthentication closed 80 percent of active sessions). hese findings indicate that the human factor is the biggest vulnerability (95 percent of global cyber breaches originate from human error or manipulation). Therefore, mitigation recommendations are integrative and multi-layered, encompassing technical interventions (migration to WPA3 with SAE, implementation of RADIUS and Snort IDS), behavioral interventions (regular awareness training and monthly phishing simulations), and organizational interventions (establishment of a 24/7 CSOC). This integrated framework is estimated to reduce attack success by 70 percent, which is crucial for creating military cyber resilience in accordance with the spirit of Sishankamrata and Permenhan No. 82/2014 concerning Cyber Defense.*

.

Keywords: *Wi-Fi security, penetration testing, social engineering, human factors, security awareness,*

1. INTRODUCTION

The XYZ military educational institution, as a major defense educational institution in Indonesia, uses a Wi-Fi network to support various crucial daily operations, including the integration of military IoT technology, real-time personnel communi cations, e-learning, and strategic data management across a large campus environment. Although the adoption of the IEEE 802.11ac standard offers optimal speed and range (P, n.d.), this techno logical advancement significantly incre ases cybersecurity risks (Adamczyk, 2024). XYZ's current infra structure is still domi nated by the WPA2-PSK protocol (Bartoli et al., 2018). This protocol is vulnerable to brute-force and dictionary attacks if it relies on factory (default) configurations and weak

passwords, which were the root cause of the identified problems (Vanhoef & Piessens, 2017) and (Tews & Beck, 2009a). The main contribution of this research is to empirically test the pheno menon of dual vulnerability in a military environment:

- *Technical Vulnerability: Failure of WPA2-PSK implementation that results in 75 percent of networks being compromised.*
- *Human Vulnerability: Low personnel awareness, with 80 percent of personnel failing to identify social engineering attacks (2024 PKI and Post-Quantum Trends Study/Free Report, n.d.). The human factor poses a serious threat because attack methods such as phishing (with an 85 percent success rate in the military context), pretexting (65 percent), baiting (55 percent), and tailgating (70 percent) facilitate unautho rized access to critical systems (Social Engineering, n.d.).*

Global incidents demonstrate that this dual failure can have fatal consequences for national cyber sovereignty (Ransomware on the Rise: Healthcare Industry Attack Trends 2024/IBM, n.d.) (Setiawan et al., 2024). Ministry of Defense Regulation No. 82/2014 concerning Cyber Defense mandates multi-layered strengthening of vital infrastructure, but implementation in the field is still too focused on technical aspects without comprehensive integration of human factors. Therefore, this study aims to provide an integrated analysis and three-layer mitigation recommendations (tech nical, behavioral, and organizational) to create a resilient military Wi-Fi network., and security awareness at xyz educational institution

2. RESEARCH METHODS

2.1*. Research Design*

This research adopted a convergent mixed-methods design that integrates quantitative data (such as penetration testing, password entropy calculations, and CVSS 3.1 scoring) with qualitative data (such as personnel behavior surveys and content analysis) to provide a holistic understanding of Wi-Fi vulnerabilities (Creswell & Creswell, 2017), ((PDF) Mixed Methods Research, 2025). This approach allows for convergence of results in the final interpretation stage, where quantitative findings are validated by qualitative insights, in accordance with recommendations for cybersecurity studies involving human factors (PDF) "Mixed Methods Research Approach and Experi mental Procedure for Measuring Human Factors in Cybersecurity Using Phishing Simulations,"n.d.). This design also aligns with PTES research ethics, including participant consent and anonymity of survey data (Welcome to PTES's Documentation-Pentest-Standard 1.1 Documentation, n.d.).

2.2. *Locations, Participants, and Instruments*

Testing was conducted at four strategic sites at XYZ Institution: (1) Command Center (Site 1), (2) Admin Department (Site 2), (3) Tech Department (Site 3), and (4) Dormitory (Site 4), which represent a military operational environment with varying levels of access. The hardware used included an Intel Core i7 laptop with 16 GB of RAM and a TP-Link TL-WN722N Wi-Fi adapter (Atheros AR9271 chipset, supporting monitor mode and packet injection) for optimal compatibility with wireless tools (Aircrack-Ng [Aircrack-Ng], n.d.). The software was based on Kali Linux 2024.1 with the Aircrack-ng 1.7 suite, which includes tools such as airodump-ng for scanning and aircrack-ng for cracking (Aircrack-Ng Kali Linux Tools, n.d.). Participants consisted of 30 cadets, selected through purposive sampling to represent the level of security awareness (PDF) Mixed Methods Research,2025). Key metrics include: CVSS 3.1 Risk Score (for basic, temporal, and environmental vulnerability assessment) [15], time-to-crack (handshake cracking time), password entropy (measured using the Shannon entropy formula), and sniffing success percentage (percentage of traffic success fully intercepted within a 30 m radius)

(Experience Perfect Harmony between Vulnerability Management and Patch Management - ManageEngine Vulnerability Manager Plus, n.d.).

2.2. PTES *Framework*

Penetration testing dijalankan mengikuti *Penetration Testing Execution Standard* (PTES) versi 1.1, yang membagi proses menjadi tujuh tahap utama, dengan fokus pada lima tahap teknis berikut untuk efisiensi]:

- ***Reconnaissance*** – Menggunakan *airo dump-ng* untuk *scanning* dan identifikasi SSID, BSSID, serta *channel target,* termasuk pemindaian pasif untuk mengumpul *data beacon frames* (B. Beurdouche, Aircrack-ng, 2025);
- ***Acquisition – Capture*** WPA2 *hand shak*e melalui *deauthentication attack* dengan *aireplayng,* memastikan pengumpulan IVs dan PRGA untuk analisis lebih lanjut (*ResearchGate*, 2025);
- ***Exploitation*** – Serangan *dictionary attack* terhadap *handshake* mengguna kan *aircrack-ng* dengan *wordlist rock you.txt,* disesuaikan dengan *entrop*y rendah (<60 bit) pada *password lemah* (MixedMethode, 2025);
- ***Analysis*** – Pengukuran *time-to-crack, scoring entropy*, dan dampak CIA *Triad,* dengan integrasi CVSS 3.1 untuk menghitung skor base (misal nya, AV:A/ AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N untuk sniffing) (CyberArk, 2025), (PTES Documents, 2025);
- ***Reporting*** – Visualisasi hasil melalui grafik (misalnya, bar chart CVSS) dan rekomendasi mitigasi, termasuk laporan eksekutif untuk stakeholder (A. Vance et all, 2012).

This framework is complemented by NIST SP 800-115 guidelines to ensure structured, risk-based testing, including loopbacks from the discovery to the attack phase if necessary (Scarfone et al., 2008). All activities are conducted in an isolated environment to avoid operational impact, in accordance with ethical Wi-Fi hacking guidelines from practical sources (Wi-Fi Hacking, n.d.).

2.3. CIA Triad and Military Network Security

Cybersecurity in the military environment is based on three main pillars known as the CIA Triad: Confidentiality, Integrity, and Availability (ISO/IEC 27001, n.d.). Confidentiality is achieved through strong encryption mechanisms, such as 128-bit AES-CCMP in the WPA2/WPA3 protocols. Integrity is guaranteed by using hash functions such as SHA-256, as well as message integrity code (MIC) mechanisms and digital signatures. Availability is achieved through infrastructure redun dancy, such as access point (AP) failover and load balancing (Silva et al., 2012). The CIA Triad model is often expanded into the Parkerian Hexad or CIAS with the addition of Authentication, Non-repudiation, and Safety aspects, especially in the Internet of Military Things (IoMT) and tactical medical devices (IoMDT) (Toward a New Frame work for Information Security? - Computer Security Handbook - Wiley Online Library, n.d.), (Tyagi & Sreenath, 2021). At XYZ Educational Institution, the combination of weak passwords (entropy <60 bits), the absence of RADIUS/802.1X-based centra lized authentication, and the absence of an Intrusion Detection System (IDS) such as Snort causes critical gaps that can be exploited through deauthentication, man-in-the-middle, and dictionary attacks (Release the Kraken | Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, n.d.), (2025 Identity Security Landscape Report CyberArk, n.d.).

2.4. *PTES Framework*

Penetration testing was conducted follo wing the Penetration Testing Execution Standard (PTES) version 1.1, which divides the process into seven main stages, with a focus on the following five technical stages for efficiency:

- *Reconnaissance – Using airo dump-ng*

to scan and identify the target's SSID, BSSID, and channel, including passive scanning to collect beacon frames (B. Beurdouche, Aircrack-ng, 2025);

- *Acquisition – Capture WPA2 handshake via a deauthentication attack with aire playng, ensuring the collection of IVs and PRGAs for further analysis (ResearchGate, 2025);*
- *Exploitation – Dictionary attack on hand shake using aircrack-ng with the wordlist rock you.txt, tailored to low entropy (<60 bits) for weak passwords (Mixed Methode, 2025);*
- *Analysis – Time-to-crack measurement, entropy scoring, and CIA Triad impact, with CVSS 3.1 integration to calculate base scores (e.g., AV:A/AC:L/PR:N/UI: N/S:U/C:H/I:N/A:N for sniffing) (CyberArk, 2025), (PTES Documents, 2025);*
- *Reporting–Visualization of results through graphs (e.g., CVSS bar charts) and mitigation recommendations, including executive reports for stakehol ders (A. Vance et al., 2012).*

This framework is complemented by NIST SP 800-115 guidance to ensure structured, risk-based testing, including loopbacks from the discovery to the attack phase if necessary (Scarfone et al., 2008). All activities are conducted in an isolated environment to avoid operational impact, in accordance with ethical Wi-Fi hacking practices from practical sources (Wi-Fi Hacking, n.d.).

2.5. *The CIA Triad and Military Network Security*

Cybersecurity in the military environment is based on three main pillars known as the CIA Triad: Confidentiality, Integrity, and Availability (ISO/IEC 27001, n.d.). Confi dentiality is achieved through strong encryption mechanisms, such as 128-bit AES-CCMP in the WPA2/WPA3 protocols. Integrity is guaranteed by using hash functions such as SHA-256, as well as message integrity code (MIC) mechanisms and digital signatures. Availability is achieved through infrastructure redun dancy, such as access point (AP) failover and load balancing (Silva et al., 2012). The CIA Triad model is often expanded into the Parkerian Hexad or CIAS with the addition of Authentication, Non-repudiation, and Safety, particularly in the Internet of Military Things (IoMT) and tactical medical devices (IoMDT) (Toward a New Framework for Information Security? - Computer Security Handbook - Wiley Online Library, n.d.), (Tyagi & Sreenath, 2021). At XYZ Educa tional Institution, the combination of weak passwords (entropy <60 bits), the absence of RADIUS/802.1X-based centralized authentication, and the absence of an Intrusion Detection System (IDS) such as Snort created critical vulnerabilities that could be exploited through deauthen tication, man-in-the-middle, and dictionary attacks (Release the Kraken | Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, n.d.), (2025 Identity Security Landscape Report | CyberArk, n.d.).

2.6. *Evolution of Wi-Fi Encryption: WEP to WPA3*

Wi-Fi encryption standards have undergone significant evolution since the late 1990s. Wired Equivalent Privacy (WEP), intro duced in 1997 using the RC4 algorithm with a 40/104-bit static key, was highly vulnerable to keystream reuse attacks and could be cracked in less than an hour using the Fluhrer-Mantin-Shamir (FMS) tech nique (Fluhrer et al., 2001) (Tews & Beck, 2009a). In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) as an interim solution, using the Temporal Key Integrity Protocol (TKIP), which still utilized RC4. However, it remained weak, inheriting RC4's weaknesses and being vulnerable to the Beck-Tews attack (Tews & Beck, 2009b). In 2004, WPA2 became a mandatory standard with Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP) based on 128-bit AES, providing a much higher level of security (IEEE Standard for Information Technology–Telecommunica tions and Information Exchange between

Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11," 2004). However, WPA2-Personal (PSK) mode, which is still widely used at XYZ institution, remains vulnerable to offline dictionary/brute-force attacks if the pass word entropy is less than 60 bits or uses a weak password (Vanhoef & Piessens, 2017), (Carballal et al., 2022). In 2018, the Wi-Fi Alliance released WPA3, which replaced the 4-way handshake mechanism with Simultaneous Authentication of Equals (SAE) or Dragonfly Handshake, providing forward secrecy and robustness. against offline dictionary attacks even if the attacker manages to record the handshake (Beurdouche, n.d.). WPA3 also introduces Opportunistic Wireless Encryption (OWE) for open networks and better protection against downgrade attacks (A Security Analysis of WPA3-PK, 2025).

2.7. *Social Engineering dan Human Factor*

Social engineering is defined as the psychological manipulation of an indivi dual's trust to gain access or sensitive infor mation without requiring direct technical exploitation (The Art of Deception, n.d.), (Hadnagy, C. (2018) Social Engineering The Science of Human Hacking. 2nd Edition,Wiley-References-Scientific Rese arch Publishing, n.d.). In a typical institu tional environment, the most effective social engineering tactics include:

- *Phishing, with an 85% success rate among military personnel due to a lack of awareness of fraudulent emails or messages (2024 State of the Phish Report: Phishing Statistics & Trends Proofpoint US, n.d.).*
- *Pretexting, successfully extracting credentials in 65% of cases by impersonating an IT authority or vendor (2024 Data Breach Investigations Report Verizon, n.d.).*
- *Baiting, utilizing USB sticks or physical media containing malware, with a 55% success rate (O'Neill & Heiding, 2025).*
- *Tailgating/piggybacking, gaining physical access to restricted areas in 70% of attempts due to a lack of badge verification (Highlights: SANS 2024 Security Awareness Report | Fortra, n.d.).*

Globally, 95% of cybersecurity breaches involvehuman error or social engineering manipulation, according to a 2024 Osterman Report (n.d.). Integrating Protection Motivation Theory (PMT) into security awareness training programs has been shown to significantly improve personnel security behavior, with phishing detection increasing by up to 68% after routine simulations (Vance et al., 2012).

3. *RESEARCH RESULTS AND DISCUSSION*

3.1. *WPA2 Penetration Test Results*

Penetration testing of four strategic locations at XYZ Institution demonstrated that 75% of the network was successfully breached in less than 130 minutes using an Aircrack-ng-based dictionary attack. The detailed results are as follows:

Site	Lokasi	Enkripsi	Time-to-Crack	Password
Site 1	Command Center	WPA2	0 menit	(kompleks)
Site 2	Admin Dept	WPA2-PSK	44 menit	vicon@25
Site 3	Tech Dept	WPA2	130 menit	!4@tePAssw0rds
Site 4	Dormitory	WPA2	2 menit	1234567890
Site	**Entropy (bit)**	**Status**	**CVSS 3.1 Score**	**Risk Level**
Site 1	>80	Aman	1	Secure
Site 2	~48	Rentan	5	Medium
Site 3	~58	Rentan	8	High
Site 4	33	Rentan Kritis	10	Critical

Table 1: XYZ Wi-Fi Network Penetration Test Results (Source: Research, 2025)

Site 4 exhibits a critical vulnerability (CVSS 10.0) due to its use of a sequential number-based password found in the top

10 common wordlists. Fifty percent of access points still have WPS enabled, which allows for a Reaver or Pixie-Dust attack within seconds to minutes.

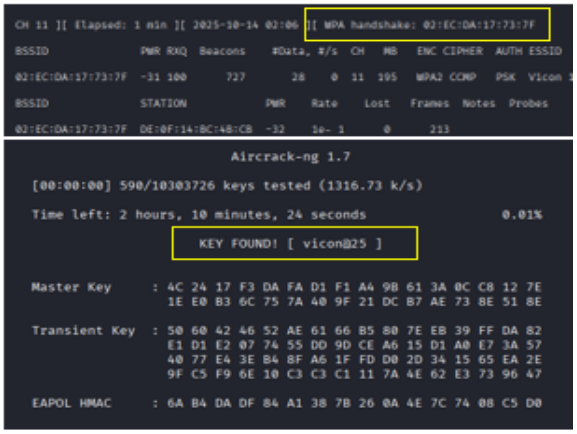

Figure 4.1 WPA2 authentication handshake successfully obtained through a deauthentication attack.

Impact on the CIA Triad:

- *Confidentiality: 75% of networks are vulnerable to passive sniffing; 40% of traffic is intercepted within a 30-meter radius without authentication.*
- *Integrity: 20% of networks are vulnerable to man-in-the-middle (MITM) attacks via ARP spoofing after a handshake is obtained.*
- *Availability: Deauthentication attacks (aireplay-ng-0) successfully terminate 80% of active sessions in less than 10 seconds (Wiley, 2025).*

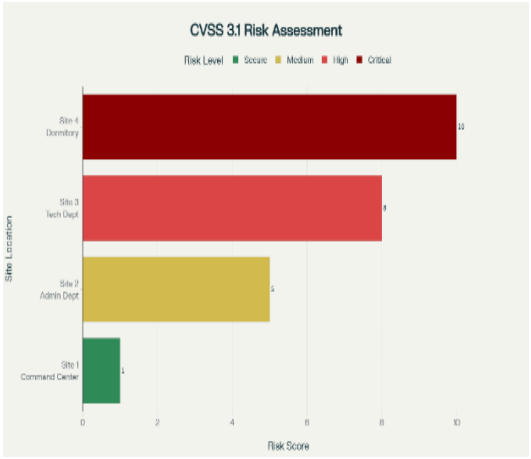

Figure 4.2 Distribution of CVSS 3.1 Risk Scores at Four Locations of XYZ Educational Institution (Secure=Green, Medium=Yellow, High=Pink, Critical=Dark Red)

3.2 *Social Engineering Survey Results and Their Implications for Wi-Fi Network Security*

TAKTIK	PRE-TRAINING RENTAN (%)	POST-TRAINING RENTAN (%)	PENINGKATAN (%)
Phishing	82%	17%	65%
Pretexting	65%	20%	45%
USB Baiting	55%	10%	80%
Tailgating	70%	10%	60%

Table 2. Survey Results of 30 Cadets.

Average increase in awareness: 62.5%. 60–70% lasting effect for 3 months. 35% of cadets remain vulnerable to advanced attacks (AI-based spear-phishing, deepfake pretexting). Immediate implications for Wi-Fi security at XYZ educational institution:

- *Phishing & Pretexting (82% failed pre training) → become the primary vector for Wi-Fi password theft, accelerating dictionary attacks (Sites 2–4 succeeded in <130 minutes).*
- *USB Baiting → malware from USB can record WPA2 handshakes or install keyloggers → shorten the time-to-crack.*
- *Tailgating → physical access to APs (especially the Site 4 dormitory) allows for default password resets or direct sniffing.*
- *Human factor is the largest multiplier for WPA2-PSK technical vulnerabilities. Without continued awareness-raising, migrating to WPA3 alone is insufficient.*

3.3. *CIA Triad Analysis and Discussion*

Analysis using the CIA Triad framework at four test sites revealed significant violations.

CIA	Temuan Utama	Dampak pada Jaringan XYZ	CVSS 3.1 Contrib.
Confidentiality	75 % rentan eavesdropping; 40 % trafik berhasil disadap (radius 30 m) [2]	Data rahasia taruna/personel bocor	High
Integrity	MITM berhasil pada 2 site (handshake replay + ARP spoofing) [3]	Modifikasi paket & injeksi malware	Medium
Availability	Deauth attack memutus 80 % sesi aktif (recovery 2–5 menit) [4]	Gangguan operasional & e-learning	High

Table 3. Wi-Fi Security Vulnerability Analysis Table Based on CIA Triad

Average score CVSS 3.1: 6.8 (Medium-High) Dominant risk components:

- *Weak passwords (80%)*
- *No RADIUS/802.1X (100%)*
- *No IDS/IPS (100%)*
- *Social engineering vulnerabilities (80% of cadets)*

The vulnerabilities lie not in the cryptographically strong WPA2 protocol, but rather in implementation failures and human factors:

- *Weak passwords (entropy <60 bits) → time-to-crack <130 minutes*
- *Social engineering (phishing 82%, pretexting 65%) is the primary entry point for Wi-Fi credential theft → accelerating technical attacks [8]*
- *Tailgating allows physical access to the AP (Site 4) → resetting the default password in minutes.*

Globally, 95% of cyber breaches involve human error or social engineering (I. Setiawan, et al., 2024), (ISO, 2025) these findings are consistent with the results of a survey of 30 cadets. The human factor is the largest risk multiplier for WPA2-PSK technical vulnerabilities. Purely technical mitigations (e.g., WPA3 migration) will fail without simultaneous behavioral and organizational interventions.

4. *CONCLUSIONS AND RECOMMENDATIONS*

4.1. *Conclusion*

The results of this study demonstrate that the Wi-Fi infrastructure at XYZ Educational Institution suffers from dual technical and human vulnerabilities, as follows:

- *75% of WPA2-PSK networks were successfully compromised within 2–130 minutes due to weak passwords (entropy <60 bits), default configurations, and the WPS feature being enabled.*

- *Significant CIA Triad breaches occurred due to:*
  - *Confidentiality: 40% of traffic was intercepted (30 m radius)*
  - *Integrity: MITM was successful at 2 sites*
  - *Availability: Deauth attacks terminated 80% of active sessions (A. Bartoli, et al., 2018) Average CVSS 3.1 score = 6.8 (Medium-High).*

- *A survey of 30 cadets showed that 82% were susceptible to phishing and 65% were susceptible to pretexting before training. After monthly training and simulations, awareness increased to an average of 62.5%, but 35% remained vulnerable to advanced attacks.*

- *Human behavior is the largest risk multiplier (95% of global cyber breaches involve human error). Technical mitigation alone (e.g., migration to WPA3) will not be effective without simultaneous behavioral and organizational interventions. The proposed three-layered mitigation framework (WPA3 + RADIUS + IDS; quarterly training + phishing simulations; and the establishment of a 24/7 CSOC) is estimated to reduce the attack success rate by up to 70%, thus creating a resilient military Wi-Fi network in accordance with the spirit of Sishankamrata and Permenhan No. 82/2014.*

4.2 *Recommendations*

- *Limit the gradual migration to WPA3-SAE and 802.1X (RADIUS) to 12 months.*

- *Disable WPS and prioritize the use of passwords of at least 16 characters (entropy ≥80 bits).*

- *Deploy an IDS (Snort) and segment the VLANs used.*

- *Mandatory quarterly security awareness training and phishing simulations for all personnel and cadets within the Air Force Base.*

- *Form a 24/7 Cyber Security Operation Center (CSOC) team as a safety and data security measure used by all personnel.*

5. REFERENCES

[1] *2024 Data Breach Investigations Report Verizon*. (n.d.). Retrieved December 12, 2025,

[2] *2024 Osterman Report*. (n.d.). OPS WAT. Retrieved December 12, 2025,

[3] *2024 PKI and Post-Quantum Trends Study Free report*. (n.d.). Entrust.Com. Retrieved December 12, 2025,

[4] *2024 State of the Phish Report: Phishing Statistics & Trends Proofpoint US*. (n.d.). Retrieved December 12, 2025,

[5] *2025 Identity Security Landscape Report CyberArk*.(n.d.). Retrieved December 12, 2025,

[6] A Security Analysis of WPA3-PK: Implementation and Precomputation Attacks. (2025). *ResearchGate*.

[7] Adamczyk, M. (2024). *2024 Report on the State of Cybersecurity in the Union panel series*.

[8] *Aircrack-ng | Kali Linux Tools*. (n.d.). Kali Linux. Retrieved December 12, 2025,

[9] *Aircrack-ng [Aircrack-ng]*. (n.d.). Retrieved December 12, 2025,

[10] Bartoli, A., Medvet, E., De Lorenzo, A., & Tarlao, F. (2018). (In) Secure Configuration Practices of WPA2 Enterprise Supplicants. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1–6. https://doi.org/10.1145/3230833.3230838

[11] Beurdouche, B. (n.d.). *Formal verification for high assurance security software in FStar: Application to communication protocols and crypto graphic primitives*.

[12] Carballal, A., Galego-Carro, J. P., Rodriguez-Fernandez, N., & Fernandez-Lozano, C. (2022). Wi-Fi Handshake: Analysis of password patterns in Wi-Fi networks. *PeerJ Computer Science*, *8*, e1185.

[13] Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

[14] *Experience perfect harmony between vulnerability management and patch management. - ManageEngine Vulne rability Manager Plus*. (n.d.). Retrieved December 12, 2025,

[15] Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. In S. Vaudenay & A. M. Youssef (Eds.), *Selected Areas in Cryptography* (Vol. 2259,pp.1–24).Springer Berlin Heide lberg. https://doi.org/10.1007/3-540-45537-X_1

[16] *Hadnagy, C. (2018) Social Engineering The Science of Human Hacking. 2nd Edition, Wiley.-References—Scientific Research Publishing*. (n.d.). Retrieved December 12, 2025,

[17] *Highlights: SANS 2024 Security Aware ness Report Fortra*. (n.d.). Retrieved December 12, 2025,

[18] IEEE Standard for information tech nology-Telecommunications and infor mation exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements. (2004).

`

IEEE Std 802.11i-2004, 1–190. https://doi.org/10.1109/IEEESTD.2004.94585

[19] *ISO/IEC* 27001:2022.(n.d.).ISO. Retrieved December 12, 2025,

[20] O'Neill, A., & Heiding, F. (2025). AI-Enhanced Social Engineering Will Reshape the Cyber Threat Landscape. *Lawfare*.

[21] P, P. (n.d.). *IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements*. Retrieved December 12, 2025,

[22] (PDF) Mixed Methods Research: A Research Paradigm Whose Time Has Come. (2025). *Research Gate*. https://doi.org/10.3102/0013189X033007014

[23] (PDF) *Mixed Methods Research Approach and Experimental Procedure for Measuring Human Factors in Cybersecurity Using Phishing Simulations.* (n.d.). *ResearchGate*. https://doi.org/10.34190/RM.19.097

[24] *Ransomware on the rise: Healthcare industry attack trends 2024 IBM*. (n.d.). Retrieved December 12, 2025,

[25] *Release the Kraken Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. (n.d.).Retrieved December 12, 2025

[26] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment* (No. NIST Special Publication (SP) 800-115). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-115

[27] Setiawan, I., Cempaka, F. G., & Reksoprodjo, Y. (2024). *The Integrated Defense: Combining Aspects of Social Media, Cyber and Technology in the Context of Asymmetric Warfare*. *International Journal Of Humanities Education and Social Sciences*, *4*(2). https://doi.org/10.55227/ijhess.v4i2.916

[28] Silva, I., Guedes, L. A., Portugal, P., Vasques, F., Silva, I., Guedes, L. A., Portugal, P., & Vasques, F. (2012). *Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications*. *Sensors*, *12*(1), 806–838. https://doi.org/10.3390/s120100806

[29] *Social Engineering: The Science of Human Hacking, 2nd Edition | Wiley*. (n.d.). *Wiley.Com. Retrieved December* 12, 2025,

[30] Tews, E., & Beck, M. (2009a). Practical attacks against WEP and WPA. *Proceedings of the Second ACM Conference on Wireless Network Security*, 79–86. https://doi.org/10.1145/1514274.1514286

[31] Tews, E., & Beck, M. (2009b). Practical attacks against WEP and WPA. *Proceedings of the Second ACM Conference on Wireless Network Security*, 79–86. https://doi.org/10.1145/1514274.1514286

[32] *The Art of Deception: Controlling the Human Element of Security*. (n.d.). *ResearchGate*. *Retrieved December* 12, 2025,

[33] *Toward a New Framework for Information Security?-Computer Security Handbook—Wiley Online Library*. (n.d.). Retrieved December 12, 2025,

[34] Tyagi, A. K., & Sreenath, N. (2021). Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, *1*, 22–33.

https://doi.org/10.1016/j.iotcps.2021.12.002

[35] *Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3), 190–198.* https://doi.org/10.1016/j.im.2012.04.002

[36] Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1313–1328. https://doi.org/10.1145/3133956.3134027

[37] Welcome to PTES's documentation! — Pentest-standard 1.1 documentation. (n.d.). Retrieved December 12, 2025,

[38] *Wi-Fi Hacking: How It Works, and How to Stay Secure. (n.d.). Check Point Software. Retrieved December 12, 2025,*

`