Vol. 4, No. 3, Desember 2023, hal. 645-650

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Pengujian sistem keamanan wireless router pada ekosistem rumah cerdas berbasis NIST sp800-115

Mandahadi Kusuma[1], Dedy Hariyadi[2], Hendarto Kurniawan[3], , Filda Fikri Faizal Muttaqin[4]
Email: [1] mandahadi.kusuma@uin-suka.ac.id, [2]milisdad@gmail.com , [3]hendartokurniawan@gmail.com, [4]19106050038@student.uin-suka.ac.id

[1,4]Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga Yogyakarta
[2]Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta
[3]Pemerintah Kota Yogyakarta

Diterima 30 November 2023 | Direvisi: - | Disetujui: 26 Desember 2023

Abstrak

Informasi pribadi yang terekam melalui perangkat yang digunakan perlu dijaga agar tidak dicuri atau disalahgunakan orang lain, sehingga sangat diperlukan sebuah konfigurasi jaringan yang lebih aman dari upaya peretasan. Termasuk diantaranya informasi pribadi yang terdapat di ekosistem rumah cerdas. Sebuah rumah yang seharusnya menjadi tempat paling nyaman jangan sampai terganggu karena salah mengkonfigurasi ekosistem rumah cerdas. Pada beberapa penelitian sebelumnya telah dibahas tentang celah konfigurasi keamanan pada infrastruktur jaringan, namun belum fokus pada ekosistem rumah cerdas dari sisi internal pengguna. Oleh karena itu dalam penelitian ini diusulkan model pengujian konfigurasi jaringan nirkabel 2.4 GHz pada ekosistem rumah cerdas menggunakan aplikasi yang dikembangkan khusus untuk pemeriksaan celah keamanan *misconfiguration*, yang diharapkan dapat memperluas penelitian celah keamanan infrastruktur jaringan berdasarkan kerangka NIST 800-115. Model pengujian pada aplikasi yang digunakan dapat memberikan informasi status aman dan tidak aman pada sebuah ekosistem jaringan nirkabel. Hasil temuan tersebut akan memberikan rekomendasi kepada pemilik jaringan nirkabel untuk melakukan sebuah tindakan konfigurasi ulang jaringan nirkabel-nya menjadi lebih aman.

Kata kunci: *rumah cerdas, misconfiguration, keamanan informasi, jaringan nirkabel.*

Testing the wireless router security system in a smart home ecosystem based on NIST sp800-115

Abstract

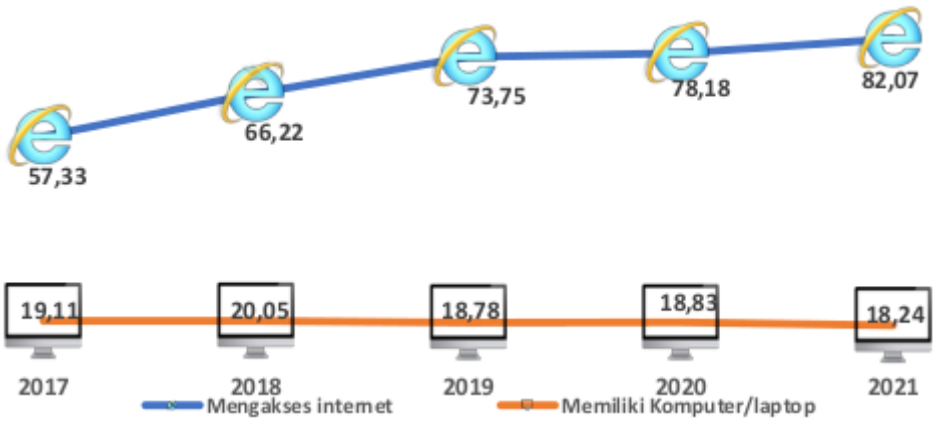
It is important to safeguard personal information captured by the device being used against theft or unauthorized use, which makes network design that is more resistant from hacking attempts. This includes personal information within the ecosystem of smart homes. A house that should be the most comfortable place should not be disturbed because of the wrong configuration of the smart home ecosystem. Several previous studies have discussed security configuration gaps in network infrastructure, but have not focused on the smart home ecosystem from the user's internal side. Therefore, in this research, a 2.4 GHz wireless network configuration testing model is proposed in a smart home ecosystem using an application developed specifically for checking misconfiguration security gaps, which is expected which is expected to expand research on network infrastructure security gaps based on the NIST 800-115 framework. The application's testing technique can reveal details about a wireless network ecosystem's safe and risky conditions. The results of these findings will provide recommendations to wireless network owners to take action to reconfigure their wireless networks to make them more secure.

Tempatkan abstrak berbahasa Inggris pada bagian ini. Gunakan font Times New Roman 10pt, italic.

Keywords: *smarthome, misconfiguration, information security, wireless network.*

1. PENDAHULUAN

Pertumbuhan pengguna internet di Indonesia dari tahun ke tahun menunjukan perkembangan. Berdasarkan survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) penetrasi pengguna internet di Indonesia pada tahun 2018 64.8%, 2019 – 2020 73.7%, dan 2021 – 2022 77.02% [1]. Pertumbuhan pengguna internet pada lingkungan rumah juga mengalami peningkatan dari tahun ke tahun, seperti pada Gambar 1 [2].



Gambar 1. Pertumbuhan internet di Indonesia

Dengan pertumbuhan internet yang selalu meningkat dari tahun ke tahun secara nasional maupun secara khusus di lingkungan rumah tangga. Maka tidak menutup kemungkinan implementasi rumah cerdas semakin terbuka. Prediksi yang dikeluarkan oleh Gartner bahwa pertumbuhan rumah cerdas akan meningkat 20 kali lipat pada tahun 2023 [3]. Ekosistem rumah cerdas tidak terlepas dengan teknologi Internet of Things atau biasa disingkat IoT. Pada teknologi IoT dapat diartikan sebuah perangkat yang saling terhubung, berkomunikasi dan berbagi menggunakan jaringan internet. Hal ini terwujud dalam bentuk aristektur IoT yang terbagi menjadi empat layer, yaitu: *smart device/sensor layer*, *network layer*, *support layer*, dan *application layer*. Rumah cerdas yang merupakan implementasi dari IoT terletak pada *application layer* [4].

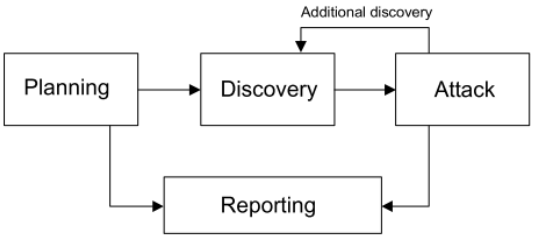
Dalam implementasi rumah cerdas perlu mempertimbangkan keamanan pada setiap layer. Menurut Garfinkel, dkk menyatakan tidak ada sebuah sistem yang aman saat saling terhubung dalam hal ini melalui jaringan internet [5]. Arsitektur jaringan pada ekosistem rumah cerdas berbeda dengan arsitektur pada perkantoran yang relatif rumit dan memerlukan tenaga dengan kemampuan jaringan komputer. Sedangkan pada ekosistem rumah cerdas peralatan dipasang secara otomatis berfungsi. Oleh sebab itu keamanan pada gateway rumah cerdas telah terkonfigurasi dengan otomatis dan berbasis web. Hal ini merupakan tantangan dalam mengamankan dan menjaga privasi data pada ekosistem rumah cerdas. Kesalahan dalam mengkonfigurasi sistem pada ekosistem rumah cerdas dapat menyebabkan beberapa gangguan seperti mendapat akses ke media penyimpan, mengganggu operasional sistem rumah cerdas, atau mengambil alih sistem secara keseluruhan [6].

NIST adalah singkatan dari National Institute of Standards and Technology (NIST). NIST adalah lembaga pemerintah Amerika Serikat yang berfokus pada pengembangan dan pengembangan standar dan teknologi. Kegiatan utama NIST mencakup penelitian ilmiah, penyediaan referensi dan alat pengukuran yang akurat, pengembangan dan pemeliharaan standar teknis, dan dukungan inovasi dan peningkatan daya saing industri di Amerika Serikat. Pada akhirnya standar keamanan yang dikeluarkan oleh NIST sering dijadikan referensi dan rujukan oleh pada pelaku industri dan peneliti diseluruh dunia. Standar NIST dapat dibandingkan dengan standard keamanan dari lembaga lain seperti ISO dan COBIT. Penggunaan standar NIST pada manajemen pengelolaan sistem informasi dapat memudahkan proses audit keamanan [7].

Pengembangan aplikasi pengujian keamanan memanfaatkan aplikasi android seperti yang telah dilakukan pada penelitian tentang pengembangan perangkat monitoring dan keamanan iot juga memanfaatkan aplikasi *mobile* android, yang digunakan untuk mengamankan kendaraan bermotor dnegan memanfaatkan sinyal wifi[8]. penelitian sebelumnya telah dilakukan pengujian sistem keamanan pada infrastruktur yang memanfaatkan celah kesalahan konfigurasi dengan memanfaatkan data dari Open Source Intelligent (OSINT). Namun, pemodelannya belum fokus ke ekosistem rumah cerdas dari sisi internal pengguna [9]. Maka pada penelitian ini dilakukan pemodelan pengujian infrastruktur ekosistem cerdas dengan tujuan untuk melindungi dari upaya serangan siber yang disebabkan kesalahan konfigurasi dari sisi pengguna.

2. METODE PENELITIAN

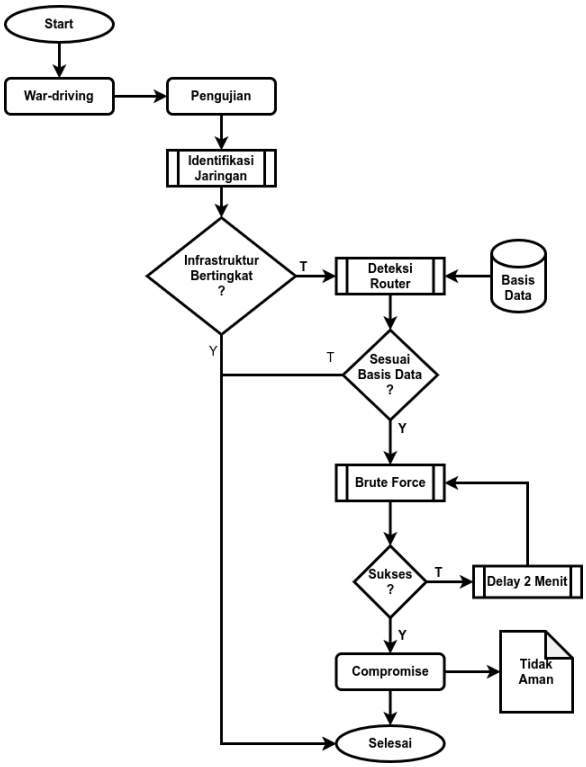
Petunjuk yang dikeluarkan oleh National Institude of Standards and Technology (NIST) tentang petunjuk teknis pengujian dan assessmen keamanan informasi memberikan rekomendasi tahapan pengujian dan assesmen keamanan informasi yang terdiri dari empat tahapan, yaitu *Planning, Discovery, Attack, dan Reporting*. NIST sendiri merupaan Adapun petunjuk tersebut tertuang pada NIST SP 800-115 dengan empat tahapan, seperti pada gambar 2. Pada tahapan *Attack* akan berulang melakukan *Discovery* dengan tujuan untuk memastikan celah keamanan baru yang ditemukan saat melakukan pengujian [10].



Gambar 2. 4 tahapan assesmen keamanan

Tahapan *Attack* dalam bentuk *proof of concept* (PoC) serangan jaringan nirkabel menggunakan komputer. Hasil PoC dikembangkan menjadi sebuah aplikasi pengujian khusus untuk melakukan pengujian misconfiguration pada infrastruktur jaringan nirkabel yang disediakan oleh penyedia internet. Selanjutnya aplikasi tersebut diuji kembali pada ekosistem rumah cerdas untuk memastikan konfigurasi jaringan nirkabel. Tahapan *Attack* tidak melakukan serangan atau melakukan perusakan, tetapi hanya memastikan misconfiguration pada jaringan nirkabel ekosistem rumah cerdas. Seperti penelitian yang dilakukan oleh Fernandes, dkk menemukan permasalahan keamanan pada perangkat cerdas pada ekosistem rumah cerdas. Celah keamanan yang ditemukan diantaranya alarm palsu, menonaktifkan mode liburan, dan pencurian kode PIN [11]. Sedangkan menurut Kang, dkk bahwa perangkat cerdas pada ekosistem rumah cerdas sebagian gagal mengimplementasikan sistem keamanan. Oleh sebab itu banyak data-data perangkat cerdas terekspos pada platform *information gathering* berbasis internet seperti shodan dan censys [12].

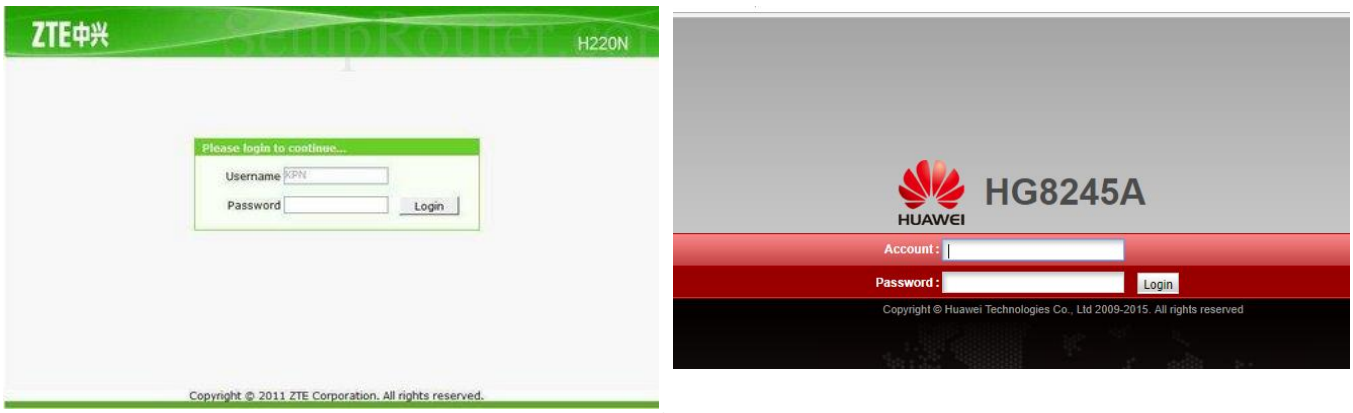
Pada penelitian ini tahapan pengujian keamanan pada ekosistem rumah cerdas mengadopsi NIST SP 800-115 yang diawali dengan melakukan identifikasi jaringan nirkabel menggunakan teknik war-driving, yaitu sebuah teknik untuk mencatat pancaran sinyal *access point* dengan melakukan pergerakan dari satu titik ke titik lainnya [13]. Rumah yang teridentifikasi memiliki *access point* dilakukan pengujian menggunakan metode *Double Gray Box*, sebuah metode pengujian yang dilakukan peneliti dengan melibatkan pemilik rumah berdasarkan ruang lingkup yang telah disepakati bersama, seperti mengetahui potensi celah keamanan yang disebabkan misconfiguration [14]. Tahapan pengujian dilakukan dengan 3 tahapan, yaitu identifikasi topologi jaringan, identifikasi merk *access point* atau *wireless router*, dan *bruteforce* sistem *access point*. Maka rancangan pengembangan aplikasi dengan tujuan pengujian keamanan jaringan nirkabel pada ekosistem rumah cerdas seperti pada gambar 3.



Gambar 3. tahapan pengujian

3. HASIL DAN PEMBAHASAN

Pada penelitian yang telah dilakukan di Pakistan, teknik wardriving digunakan untuk memerangi tindak kejahatan terorisme yang memanfaatkan sinyal wi-fi dalam komunikasi internal mereka. Dengan menggunakan teknik wardriving para penegak hukum di Pakistan dapat melakukan observasi dan pengamatan dari pancaran sinyal wi-fi [15]. Tahap selanjutnya menggunakan metode *Double Gray Box* untuk mendapatkan informasi lebih lanjut ekosistem rumah cerdas dari pemilik rumah. Berdasarkan obeservasi pada rumah cerdas, perangkat Optic Network Terminal (ONT) yang disediakan penyedia jasa internet skala rumahan didominasi produk dari Huawei dan ZTE dengan halaman login seperti pada **Error! Reference source not found.**.



Gambar 4. Halaman login wifi router ONT ZTE dan Huawei

Setelah mendapatkan izin oleh pemilik rumah tahapan selanjutnya melakukan identifikasi lapisan jaringan komputer yang diterapkan pada rumah cerdas. Topologi jaringan komputer yang memiliki potensi celah keamanan adalah topologi jaringan yang tidak bertingkat, artinya dari ONT yang memiliki fitur wireless *access point* langsung terhubung dengan perangkat-perangkat cerdas pada rumah cerdas. Selain itu jaringan yang tidak menerapkan segmentasi juga memiliki potensi celah keamanan, misal tidak membagi jaringan utama antara perangkat cerdas dengan pengguna tamu.

Dengan topologi jaringan yang tidak bertingkat memudahkan pengguna lain atau tamu dapat mengakses jaringan utama pada perangkat cerdas. Hal ini berpotensi pelaku tindak kejahatan dapat menerobos jaringan utama rumah cerdas dengan melakukan deteksi tipe router atau ONT yang digunakan seperti ZTE atau Huawei. Jika ONT telah teridentifikasi maka tahapan selanjutnya melakukan teknik bruteforce, yaitu suatu teknik menerobos sebuah sistem dengan menebak atau mencoba satu per satu *username* dan *password* yang bersumber dari basis data atau kamus [16]. Adapun basis data atau kamus yang digunakan pada teknik *bruteforce* seperti pada Tabel 1.

Table 1. Kombinasi *username* dan *password* wifi router ONT

Daftar kamus user	Admin, root, user, admin, support, telecomadmin, superuser
Daftar kamus password	user, telkomjatineg4r4, Mn@lh4!nk9#m, Dj9@t!n03g4r6#f, zep2kjzol, Telkomdso123, admin, Qc!80ebor3#to#b, Yu9j#4qa!rth#y, Pq@54r!e8ow&q#u, theworldinyourhand, admintelecom, superuser, user1234, %0|F?H@f!berhO3e

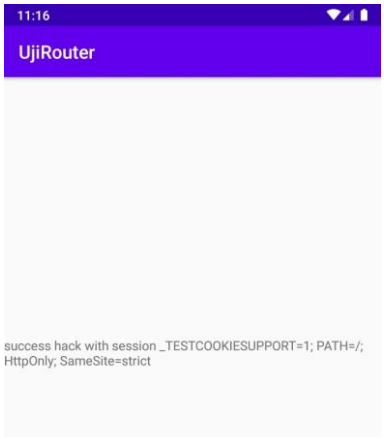
Teknik *bruteforce* yang diterapkan melakukan jeda waktu 2 menit jika *username* dan *password* yang dimasukan tidak sesuai. Hal ini menyesuaikan dengan algoritma dari sistem ONT yang telah mengantisipasi serangan *bruteforce* dengan interval 1 menit. Oleh sebab itu untuk mengantisipasi pemblokiran pasca kegagalan pada teknik *bruteforce* maka aplikasi yang dibangun untuk menguji keamanan ONT diberikan interval 2 menit seperti pada pseudocode dibawah ini.

Pseudocode *Bruteforce* attack

```
// define the set of possible passwords
List<String> passwords = Arrays.asList("password1", "password2", "password3", ...);

// define the target account
String targetAccount = "username";

// try each password in the set
for (String password : passwords) {
   // attempt to login to the target account using the current password
   boolean loginSuccessful = attemptLogin(targetAccount, password);

   // if the login is successful, stop the bruteforce attack
   if (loginSuccessful) {
      Log.d("BruteForce", "Login successful using password: " + password);
      break;
   }
```

```
   // if the login was not successful, wait 2 minutes before trying the next password
   else {
      try {
         Thread.sleep(120000);
      } catch (InterruptedException e) {
         Log.e("BruteForce", "Error while sleeping", e);
      }
   }
}
```

Untuk mempermudah pengujian pada ekosistem rumah cerdas diperlukan aplikasi berbasis *mobile*, sebagai contoh aplikasi yang berjalan pada ponsel cerdas Android. Pengembangan aplikasi berbasis *mobile* sesuai penelitian yang dilakukan di India bahwa pengembangan aplikasi pada ponsel cerdas Android disesuaikan dengan tingkat popularitas pengguna ponsel cerdas Android yang terjangkau dari sisi harga dan kemudahan penggunaannya [17]. Maka pada penelitian ini juga melakukan pengembangan aplikasi untuk pengujian wifi router ONT yang selaras dengan ponsel cerdas Android. Dalam penelitian ini bahasa pemrograman yang digunakan menggunakan Java dengan fungsi *bruteforce* seperti yang terlihat pada Gambar 5.



Gambar 5. contoh penggunaan aplikasi untuk deteksi keamanan *wireless router*

4. KESIMPULAN

Pada beberapa koneksi internet dengan ekosistem rumah cerdas pada rumah maupun café yang telah diuji cobakan, ditemukan sebagian besar dengan menggunakan *username* dan *password* administrator yang telah tersebar di internet, peneliti dapat mengakses router tersebut. Apabila aktivitas ini dilakukan dengan niat jahat (*mens rea*), seperti melakukan *wifi cracking*, *password sniffing*, mematikan akses internet pengguna lain, atau aktivitas yang merugikan lainnya, tentu ini menjadi sebuah ancaman serius yang dapat merugikan setiap invidu lain yang menggunakan jaringan internet tersebut. Oleh sebab itu, Keamanan jaringan tidak hanya dibutuhkan pada area perkantoran, namun area rumah tempat tinggal yang memiliki jaringan internet juga wajib untuk dilindungi. Hal ini dapat dijadikan sebagai masukan kepada setiap internet provider untuk melindungi setiap *wireless router* yang mereka miliki agar hanya orang-orang yang berhak saja yang boleh mengaksesnya.

Model pengujian konfigurasi jaringan nirkabel 2.4 GHz pada ekosistem rumah cerdas menggunakan aplikasi yang dikembangkan khusus untuk pemeriksaan celah keamanan *misconfiguration* diharapkan dapat memperluas penelitian celah keamanan infrastruktur jaringan berdasarkan kerangka NIST 800-115. Namun Aplikasi yang dikembangkan masih terbatas untuk jaringan satu tingkat, yaitu jaringan yang langsung mengakses wifi router dari penyedia layanan internet. Pada penelitian selanjutnya, diharapkan ada pengembangan aplikasi uji keamanan ini untuk publik area, seperti café dan mall yang menyediakan layanan internet gratis.

UCAPAN TERIMAKASIH

Ucapan terima kasih diberikan kepada LPPM UIN Sunan Kalijaga Yogyakarta atas dukungan yang diberikan berupa bantuan dana penelitian dalam skema Penelitian Pembinaan/Kapasitas dosen pemula tahun pelaksanaan 2022.

DAFTAR PUSTAKA

[1] D. Indonesia, “APJII: Pengguna Internet Indonesia Tembus 210 Juta pada 2022,” Dataindonesia.id. Accessed: Dec. 19, 2022. [Online]. Available: https://dataindonesia.id/digital/detail/apjii-pengguna-internet-indonesia-tembus-210-juta-pada-2022

[2] “Badan Pusat Statistik.” Accessed: Dec. 19, 2022. [Online]. Available: https://www.bps.go.id/publication/2022/09/07/bcc820e694c537ed3ec131b9/statistik-telekomunikasi-indonesia-2021.html

[3] D. Cearley *et al.*, “Top 10 strategic technology trends for 2020: A Gartner trend insight report.”

[4] K. Patel, S. Patel, P. Scholar, and C. Salazar, *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*. 2016.

[5] S. Garfinkel, G. Spafford, and A. Schwartz, *Practical Unix & Internet Security, 3rd Edition*, 3rd edition. Beijing ; Sebastopol, CA: O'Reilly Media, 2003.
[6] O. Anthony, "INTRUSION DETECTION IN INTERNET OF THINGS (IOT)," *International Journal of Advanced Research in Computer Science*, vol. 9, pp. 504–509, Feb. 2018, doi: 10.26483/ijarcs.v9i1.5429.
[7] E. Handoyo, "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 1, no. 2, Art. no. 2, Oct. 2020, doi: 10.37859/coscitech.v1i2.2199.
[8] M. S. Mulya, I. Yustiana, and I. L. Khrisma, "Rancang Bangun Sistem Keamanan dan Monitoring Kendaraan Berbasis IoT dan *Mobile* Apps," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 2, Art. no. 2, Aug. 2022, doi: 10.37859/coscitech.v3i2.3934.
[9] R. Sahtyawan, "PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)," *Journal of Information System Management (JOISM)*, vol. 1, no. 1, Art. no. 1, Jul. 2019, doi: 10.24076/joism.2019v1i1.18.
[10] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical Guide to Information Security Testing and Assessment," National Institute of Standards and Technology, NIST Special Publication (SP) 800-115, Sep. 2008. doi: 10.6028/NIST.SP.800-115.
[11] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in *2016 IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 636–654. doi: 10.1109/SP.2016.44.
[12] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-centric Computing and Information Sciences*, vol. 7, no. 1, p. 6, Mar. 2017, doi: 10.1186/s13673-017-0087-4.
[13] M. Purweni, D. Hariyadi, F. E. Nastiti, and F. Fazlurrahman, "Model Inspeksi Keamanan Jaringan Nirkabel Dengan Teknik Wardrving Berbasis ChatBot," *1*, vol. 6, no. 2, Art. no. 2, Nov. 2022, doi: 10.31603/komtika.v6i2.7943.
[14] P. Herzog, "Open-Source Security Testing Methodology Manual." Accessed: Dec. 24, 2022. [Online]. Available: https://untrustednetwork.net/files/osstmm.en.2.1.pdf
[15] Z. Akram, M. A. Saeed, and M. Daud, "Wardriving and its Application in Combating Terrorism," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Apr. 2018, pp. 1–5. doi: 10.1109/CAIS.2018.8442035.
[16] H. S. Shreenidhi, S. Prabakar, and P. A. Kumar, "Intrution detection system Using IoT device for safety and security," in *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Mar. 2021, pp. 340–344. doi: 10.1109/ICCIKE51210.2021.9410730.
[17] T. Mahmud and M. Monirujjaman Khan, "A Medical App based Automated Disease Predicting Doctor," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, Apr. 2021, pp. 478–485. doi: 10.1109/ICCMC51019.2021.9418435.