BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini menegaskan pentingnya penggunaan OSINT dalam pengelolaan risiko keamanan siber, khususnya di lingkungan akademik. Penggunaan metode ini tidak hanya efisien tetapi juga mematuhi prinsip non-intrusif, sehingga dapat diterapkan secara luas di berbagai institusi. Berdasarkan hasil penelitian yang dilakukan menggunakan Open Source Intelligence (OSINT) untuk menentukan risk assessment website UPN Veteran Jakarta (UPNVJ), beberapa poin penting dapat disimpulkan:

1. Identifikasi Kerentanan

   Pemanfaatan OSINT berhasil mengidentifikasi berbagai kerentanan pada website UPNVJ, termasuk subdomain yang diretas untuk aktivitas ilegal seperti judi online. Kerentanan tersebut muncul karena lemahnya pengelolaan subdomain, keamanan sistem, atau minimnya kontrol terhadap aksesibilitas aset digital.
2. Analisis Risiko

   Kombinasi antara kemungkinan ancaman dan dampaknya menunjukkan tingkat risiko yang signifikan. Risiko ini dapat mengakibatkan kerugian reputasi, pelanggaran hukum, serta ancaman terhadap integritas data dan privasi pengguna.
3. Efektivitas OSINT

   Teknik OSINT terbukti menjadi alat yang efektif dalam mengidentifikasi risiko tanpa melakukan tindakan invasif terhadap sistem. Dengan alat seperti Maltego, SecurityTrails, VirusTotal, dan Pentest-Tools,

penelitian mampu mengumpulkan informasi penting untuk analisis risiko secara efisien.

4. Rekomendasi Mitigasi

   Berdasarkan penilaian risiko, langkah mitigasi yang direkomendasikan meliputi perbaikan konfigurasi sistem, pemantauan subdomain secara berkala, edukasi keamanan siber, serta peningkatan pengelolaan akses dan aset digital.

5. Tingkat Kerentanan Website

   Website UPNVJ, khususnya subdomain seperti ejournal.upnvj.ac.id, ditemukan memiliki kerentanan yang signifikan, termasuk penyalahgunaan subdomain untuk aktivitas ilegal (contoh: konten judi online). Pengelolaan subdomain yang kurang ketat menjadi salah satu faktor utama yang memungkinkan kerentanan ini terjadi.

5.2 Saran

Penggunaan Open Source Intelligence (OSINT) untuk menentukan risk assessment pada website UPN Veteran Jakarta (UPNVJ) memberikan ruang untuk berbagai pengembangan di penelitian selanjutnya. Berikut adalah beberapa saran untuk pengembangan penelitian lebih lanjut:

1. Simulasi dan Pengujian Risiko Aktif (Penetration Testing)

   Setelah menggunakan OSINT, penelitian lanjutan dapat menggabungkan metode aktif seperti penetration testing untuk memberikan gambaran yang lebih akurat tentang kerentanan yang bisa dieksploitasi.

2. Melakukan patching dan menutup kerentanan
3. Melakukan monitoring pada aset teknologi secara rutin, selama 24x7 terhadap keamanan jaringan, dengan melakukan monitoring baik dari sisi security control maupun trafic pada jaringan.
4. Memperluas Ruang Lingkup OSINT

Penelitian berikutnya bisa mencakup penggunaan OSINT pada berbagai subdomain lain dari UPNVJ atau institusi serupa untuk mengidentifikasi ancaman yang lebih luas dan pola serangan siber yang spesifik.

5. Harus adanya SOP/Playbook mengenai mekanisme keamanan siber pada aset teknologi/IT
6. Menghapus subdomain yang tidak digunakan
7. Karena terdeteksi adanya C2 server, penulis menyarankan command and control, melakukan full scaning pada bagian network, melakukan scaning menggunakan antivirus pada endpoint(workstation maupun server), melakukan digital forensik untuk mengetahui koneksi antara C2 server dengan environment IT UPNVJ.
8. Studi Perbandingan Antar Institusi

   Penelitian selanjutnya dapat melakukan studi komparatif dengan universitas lain untuk memberikan rekomendasi berbasis konteks pada institusi pendidikan tinggi terkait manajemen risiko keamanan siber.