BASIC COMPUTER NETWORK

Week - 15

Fundamental of Network Security

Universitas Kristen Wira Wacana Sumba
Lecturer - Fajar Hariadi

Contents

01

Konsep Keamanan

Prinsip Keamanan

- Terdapat 2 bagian dalam prinsip keamanan, yaitu security concept dan security Controls.
- Security Concept merupakan prinsip dasar dan strategi yang digunakan dalam mengamankan suatu data, sistem, atau jaringan komputer dari pihak yang tidak berhak
- Security Controls merupakan parameter yang diterapkan dalam bentuk tindakan perlindungan dan pencegahan untuk melindungi berbagai macam data dan infrastruktur yang dimiliki oleh suatu organisasi

Security Concept

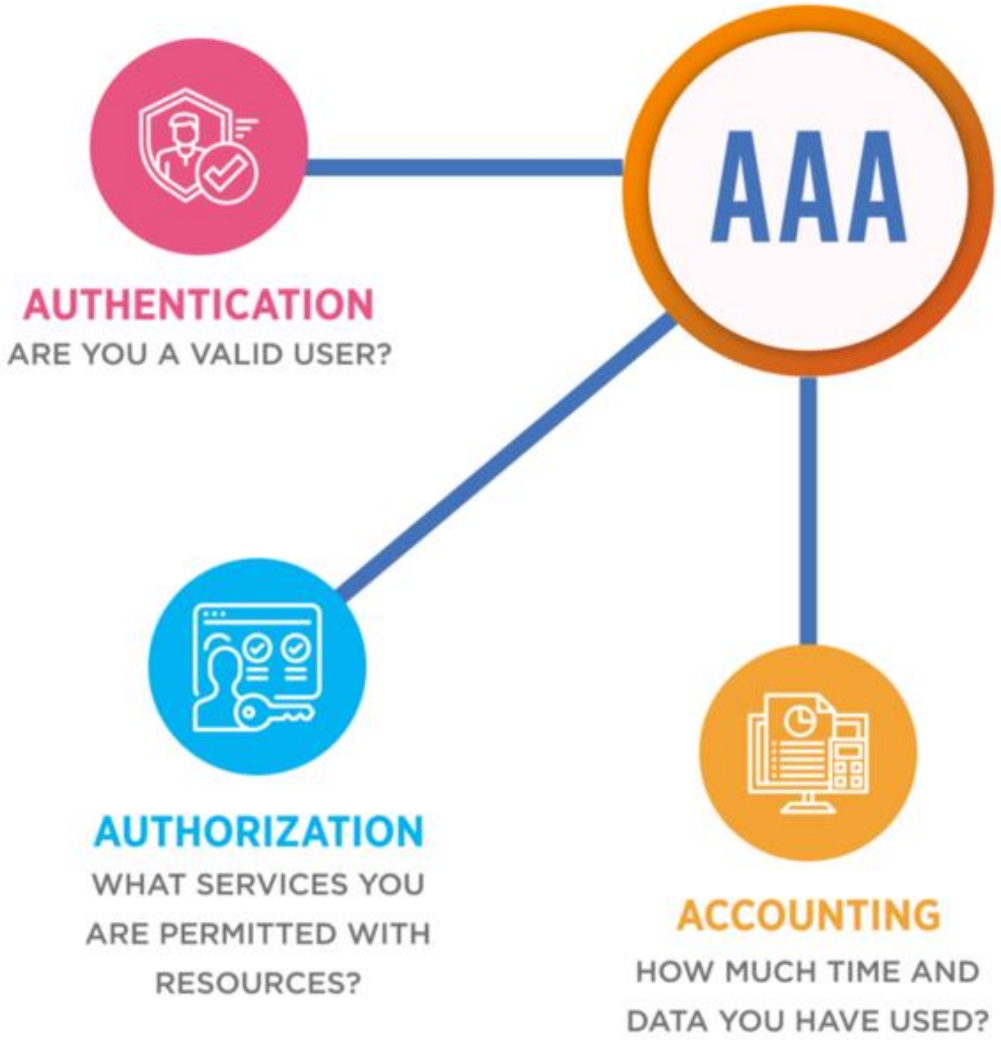
Confidentiality : Hanya orang yang berhak yang dapat melihat data/informasi

Integrity : Data/informasi sesuai dengan data asli/fakta tanpa ada pihak yang melakukan perubahan.

Availability : Data/Informasi dapat diakses oleh pihak yang berwenang kapan saja dibutuhkan

Source: https://www.wallarm.com/what/cia-triad-definition

Security Concept



Source: https://www.height8tech.com/blog.php?blog=aaa-server

Authentication : Memastikan bahwa yang mengakses suatu data, sistem, atau jaringan merupakan orang yang valid

Authorization : Memastikan batasan dan tindakan dapat dilakukan oleh user tersebut

Accounting : Mencatat setiap tindakan yang dilakukan, kapan dan berapa lama

Security Controls

Aksi	Deskripsi	Contoh Skenario	Proses Komputer
Identification /Identifikasi	Memastikan kredensial	Seorang kurir menunjukkan tanda pengenalnya	Memasukkan Username
Authentication /Autentikasi	Memvalidasi kredensial	Security memastikan tanda pengenalnya kurir asli	Memasukkan password
Authorization /Otorisasi	Memberikan ijin untuk memasuki area pegawai	Security membuka pintu untuk dapat dilewati oleh kurir untuk memberikan paket	User dapat mengakses data yang sesuai dengan levelnya
Accounting /Akunting	Mencatat waktu dan ruang yang dimasuki pegawai	Security mencatat waktu datangnya paket dan informasi kurir yang mengantar	Aktivitas user dicatat dalam log

Security control merupakan mekanisme yang digunakan untuk membatasi akses terhadap sebuah aset untuk meminimalisir terjadinya pelanggaran keamanan terhadap aset.

Categories of Controls

kategori	Deskripsi	Contoh
Managerial	Control yang dilakukan melalui metode administrasi	Penerapan aturan terkait website yang tidak boleh dikunjungi di area kampus
Operasional	Control yang diimplementasikan dan dilakukan oleh orang	Mengadakan workshop untuk melatih user membedakan email dan halaman web yang mencurigakan
Technical	Control yang dilakukan sebagian dari hardware, software, dan brainware	Hardware yang di set oleh teknisi untuk memblokir konten berbahaya dari internet
Physical	Control yang dilakukan dengan menerapkan keamanan berdasarkan struktur dan lokasi	Memasang kunci dan pengaman sehingga hanya orang-orang tertentu saja yang dapat memasuki ruangan-ruangan khusus

02

Endpoint Security

Endpoint Security – App based

- Endpoint security merupakan bagian akhir perangkat pengguna yang terhubung dengan jaringan komputer seperti laptop, PC, tablet, smartphone dan berbagai macam perangkat lain
- Terdapat banyak celah dari sisi endpoint namun yang paling sering terjadi adalah celah dari sisi brainware yaitu kemampuan/pengetahuan dari pengguna perangkat dan dari sisi teknologi yang digunakan seperti aplikasi atau sistem yang dipakai

Malware

- Malware / malicius software mendeskripsi perangkat lunak yang didesain untuk meng-interfensi perangkat hingga dapat melakukan tindakan atau eksekusi perintah yang tidak diinginkan penggunanya.

KIDNAP MALWARE

Kindap malware akan mengunci perangkat pengguna hingga tidak dapat digunakan sebelum pengguna dapat memberikan apa yang diminta oleh si pembuat malware

EAVESDROP MALWARE

Malware yang secara diam-diam mengakses resource yang ada pada komputer pengguna seperti spyware atau keylogger

Malware

REMOTE ACCESS MALWARE

Malware ini dapat memberi intruksi kepada komputer korban secara jarak jauh, bisa juga digunakan untuk mengcopy data yang dimiliki oleh pengguna. Contohnya adalah trojan

LAUNCH MALWARE

Malware yang bekerja dengan melaksanakan fungsi spesifik tertentu seperti menghapus seluruh data pengguna, mengcopy, atau membuat setiap program yang dijalankan akan crash. Tipe ini biasanya tidak dapat mengcopy dirinya ke komputer lain, sehingga butuh bantuan pengguna itu sendiri yang menjalankan programnya pada komputer lain melalui hasil copy dari flash atau sejenisnya. Contohnya virus

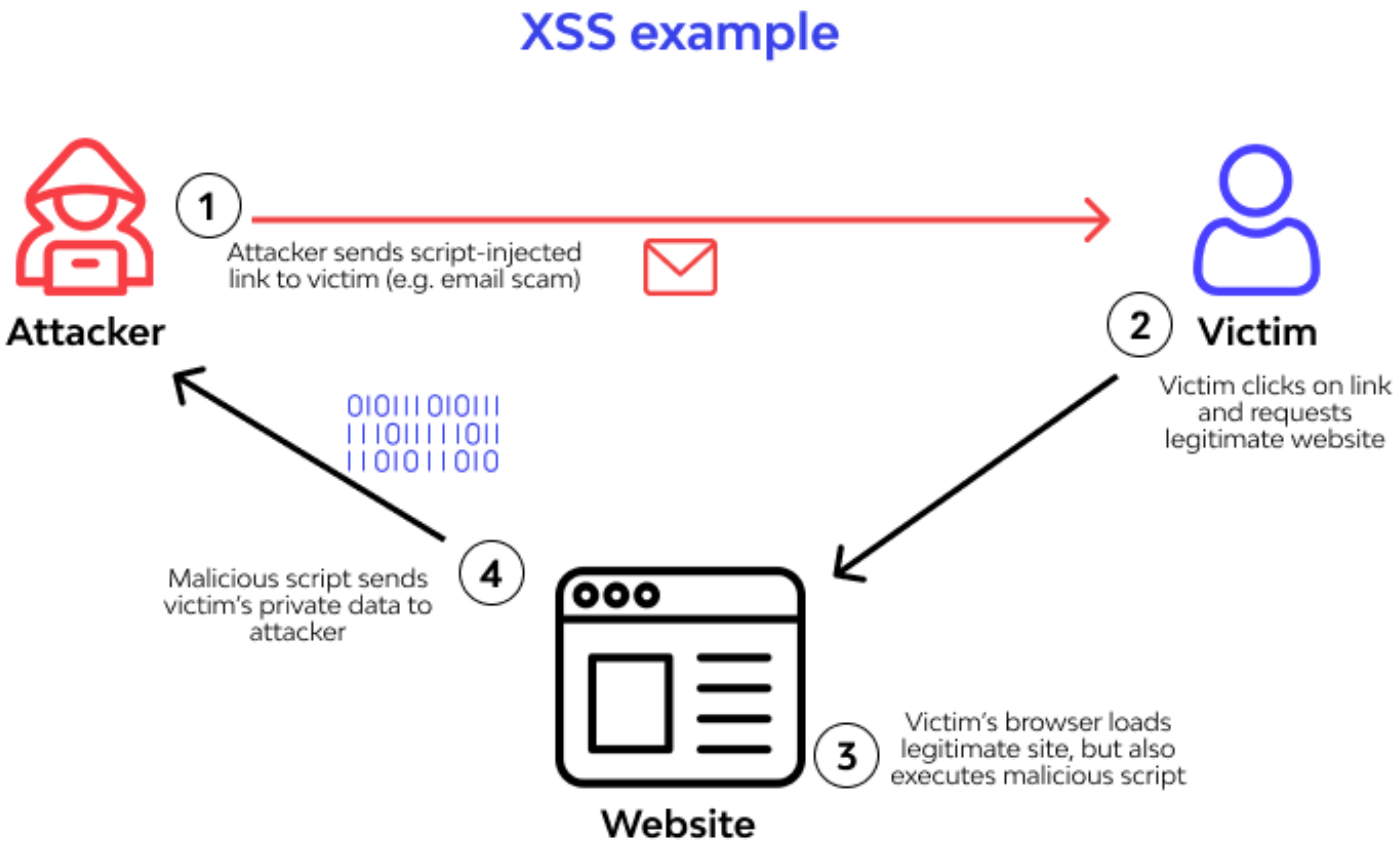
Indikator Serangan

Account Lockout	Concurrent session usage	Blocket Content
User tidak dapat melakukan autentikasi	Terdapat dua sesi mengakses akun yang sama pada lokasi yang berbeda	Data tidak dapat diakses

Impossible Travel	Resource consumption
Dalam waktu singkat user login pada lokasi yang berbeda	Sumber daya komputer seperti penggunaan CPU atau RAM tiba-tiba penuh

Out-of-cycle logging
Log tidak dapat menyimpan kejadian secara benar atau log hilang

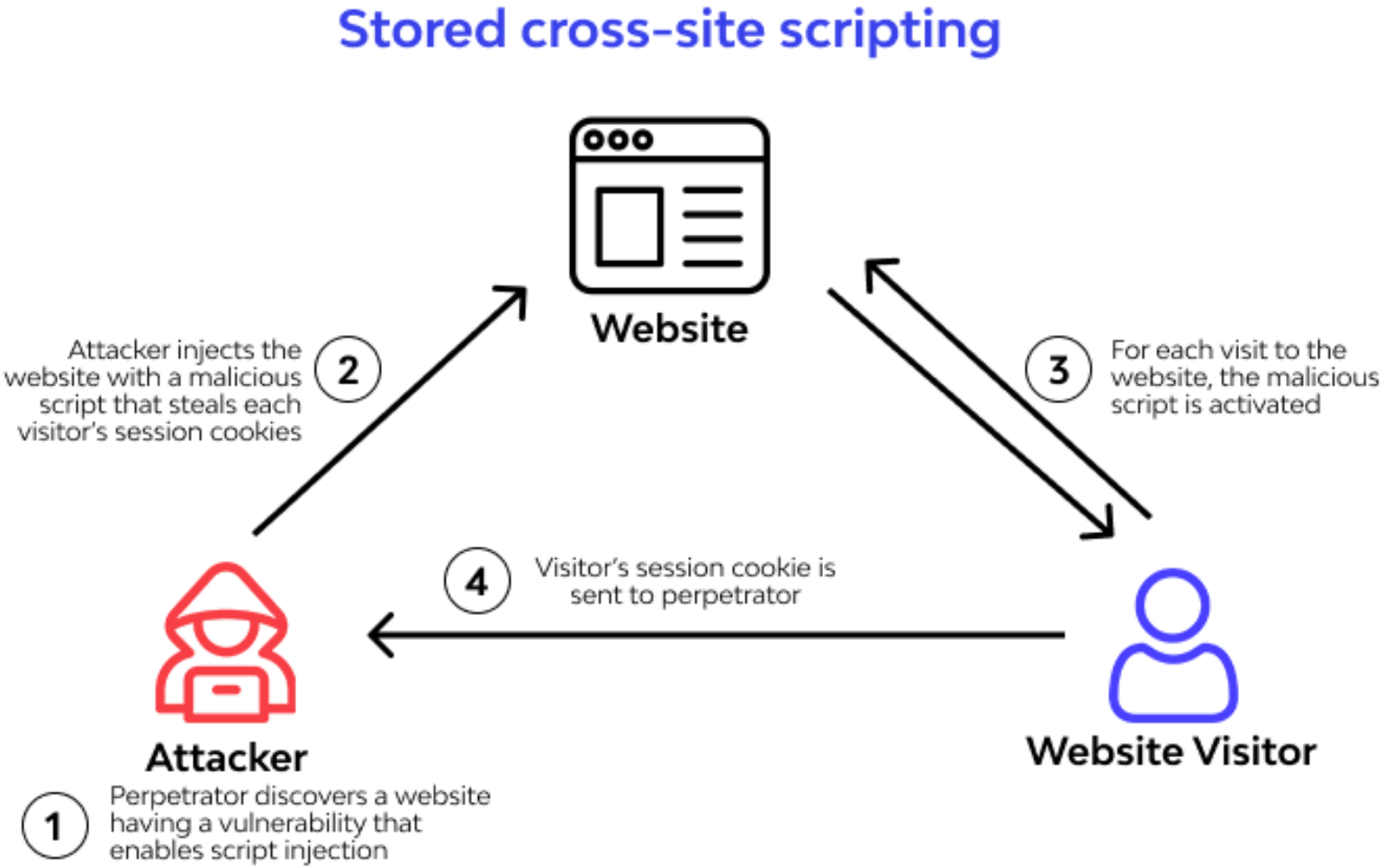
Endpoint Security – Web based



cross-site scripting (XSS) dimulai dengan user mengirimkan link yang telah ditambahkan scripting (biasanya jaavascript). Code ini dapat digunakan hacker untuk menambahkan bagian kodenya sendiri dengan meminta informasi tertentu. Sehingga script tersebut menjadi bagian kode dari server dan dapat berjalan di web browser pengguna lain yang nantinya tidak hanya mengirimkan data ke server tapi juga ke hacker

Source: https://www.wallarm.com/what/what-is-xss-cross-site-scripting

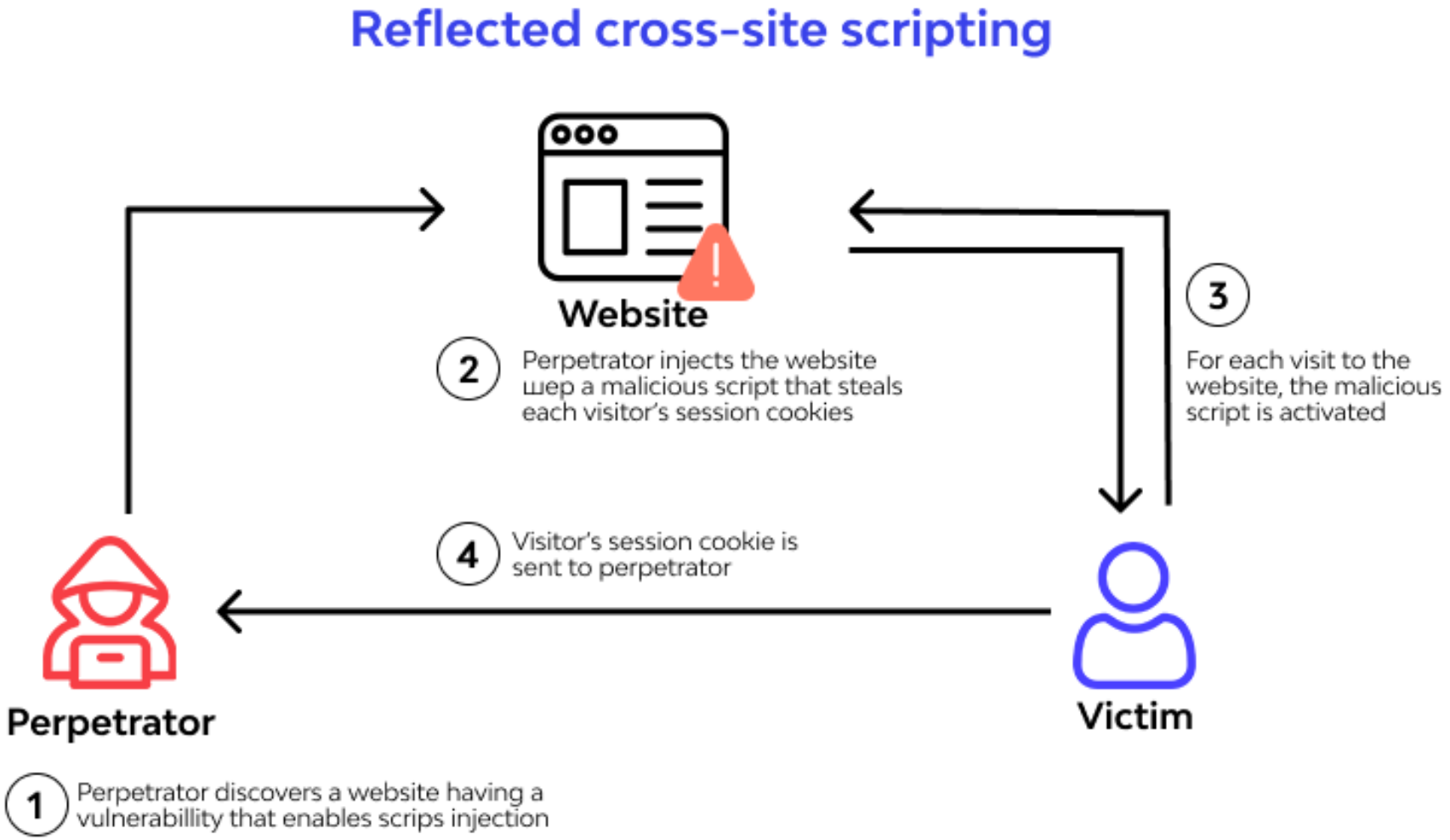
Endpoint Security – Web based



Source: https://www.wallarm.com/what/what-is-xss-cross-site-scripting

Stored cross-site scripting biasanya berjalan pada website yang memiliki code javascript yang berjalan di sisi clinet. Code ini dapat digunakan hacker untuk menambahkan bagian kodenya sendiri menggunakan input form. Sehingga script tersebut menjadi bagian kode dari server dan dapat berjalan di web browser pengguna lain yang nantinya tidak hanya mengirimkan data ke server tapi juga ke hacker

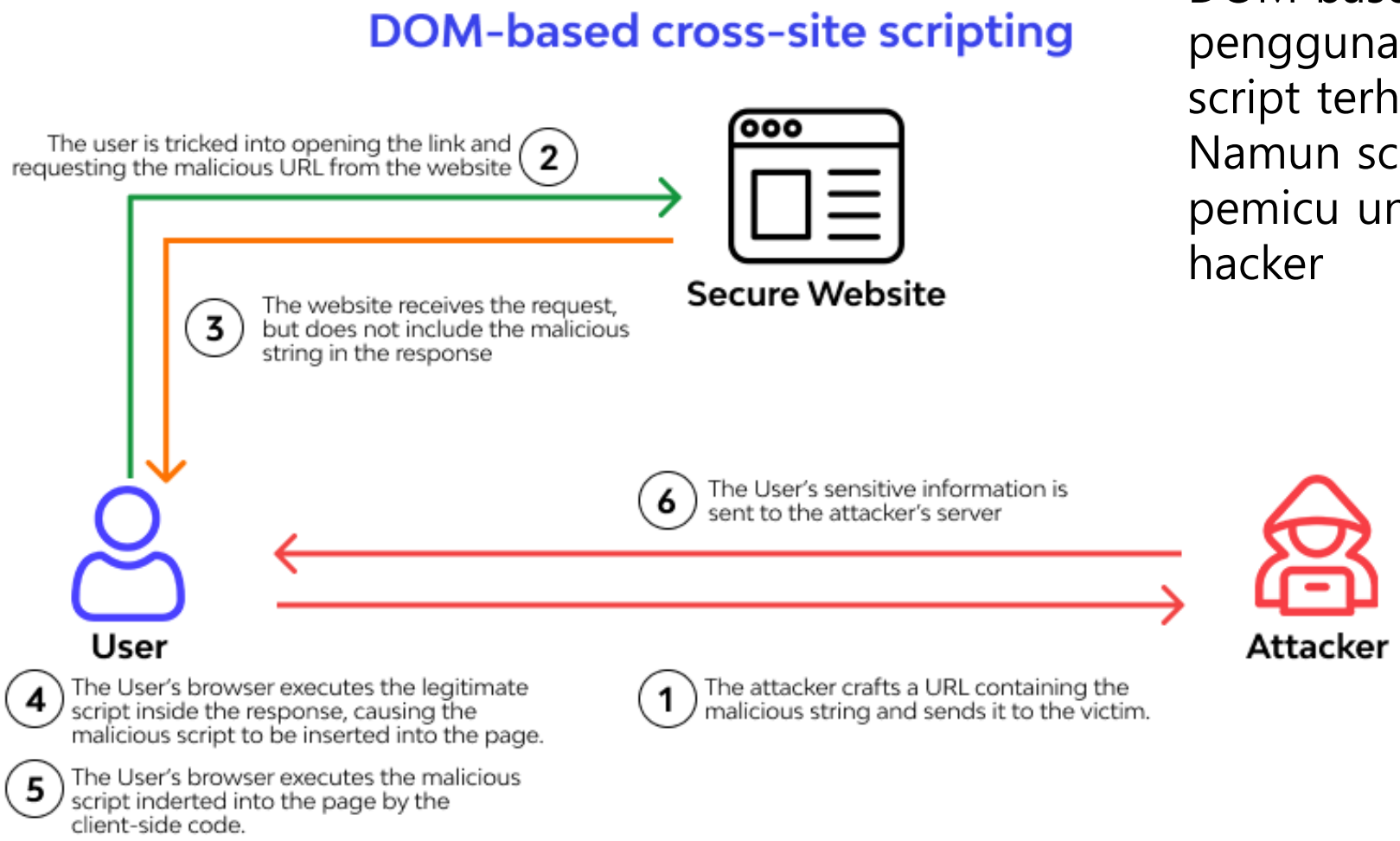
Endpoint Security – Web based



Source: https://www.wallarm.com/what/what-is-xss-cross-site-scripting

Reflected cross-site scripting menyerang sisi server sehingga setiap client yang mengakses server tersebut menjalankan scritp yang ditambahkan hacker untuk yang nantinya tidak hanya membuat pengguna mengirimkan data ke server tapi juga ke hacker

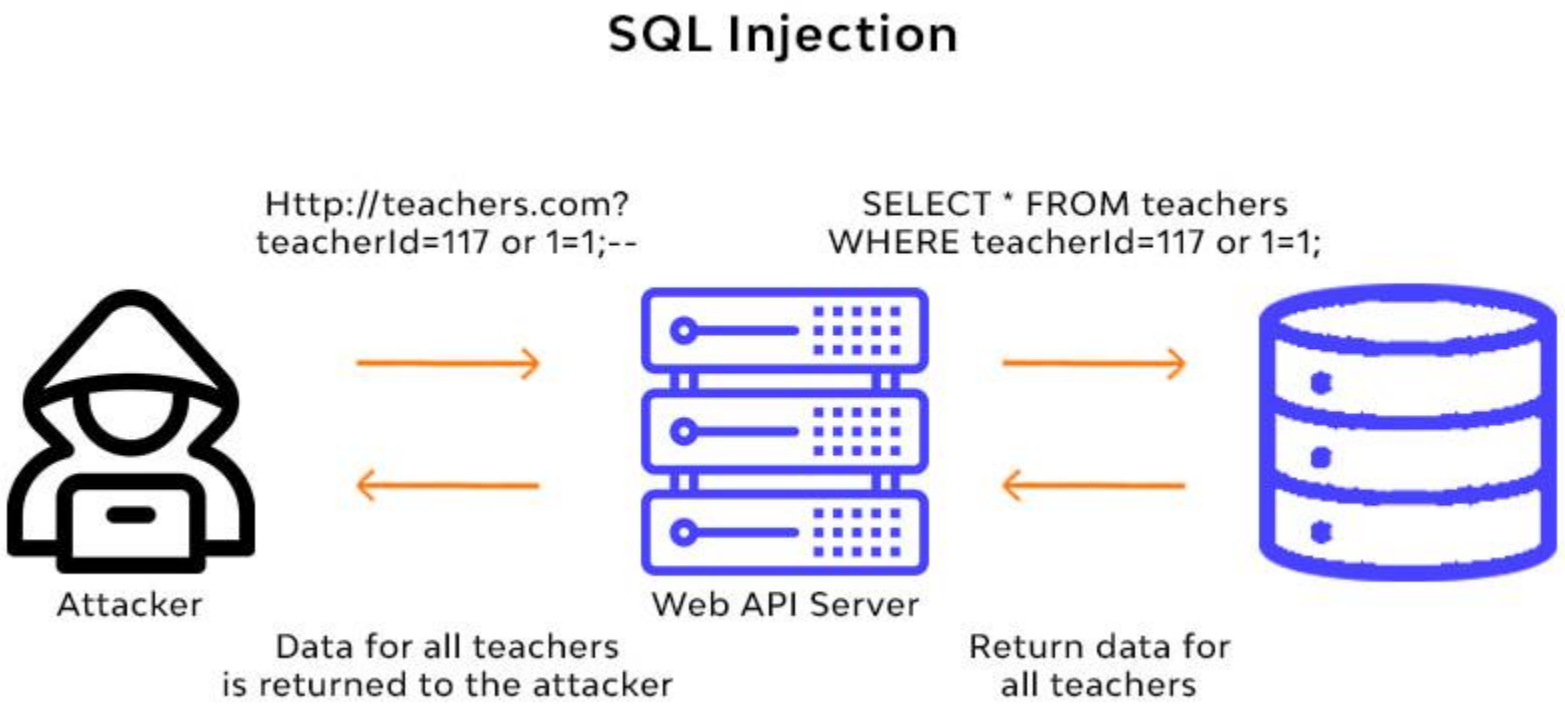
Endpoint Security – Web based



DOM based akan menyerang sisi browser pengguna dengan menambahkan bagian script terhadap respons resmi dari server. Namun script yang ditambahkan menjadi pemicu untuk mengirimkan data pada hacker

Source: https://www.wallarm.com/what/what-is-xss-cross-site-scripting

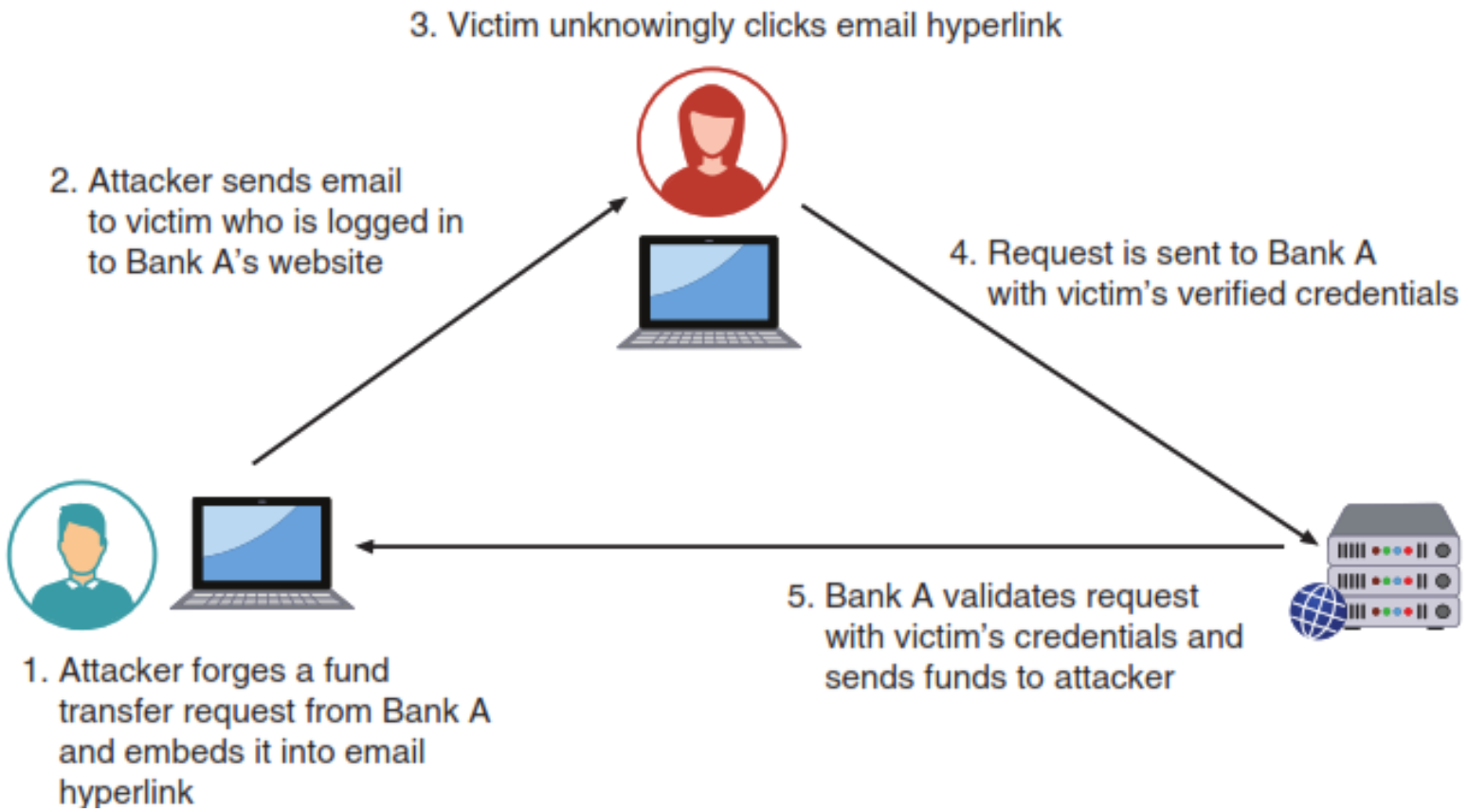
Endpoint Security – Web based



SQL Injection dilakukan dengan memasukkan perintah SQL pada form input atau url yang akan dieksekusi oleh server yang rentan sehingga isi databasenya dapat dibaca oleh penyerang

Source: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

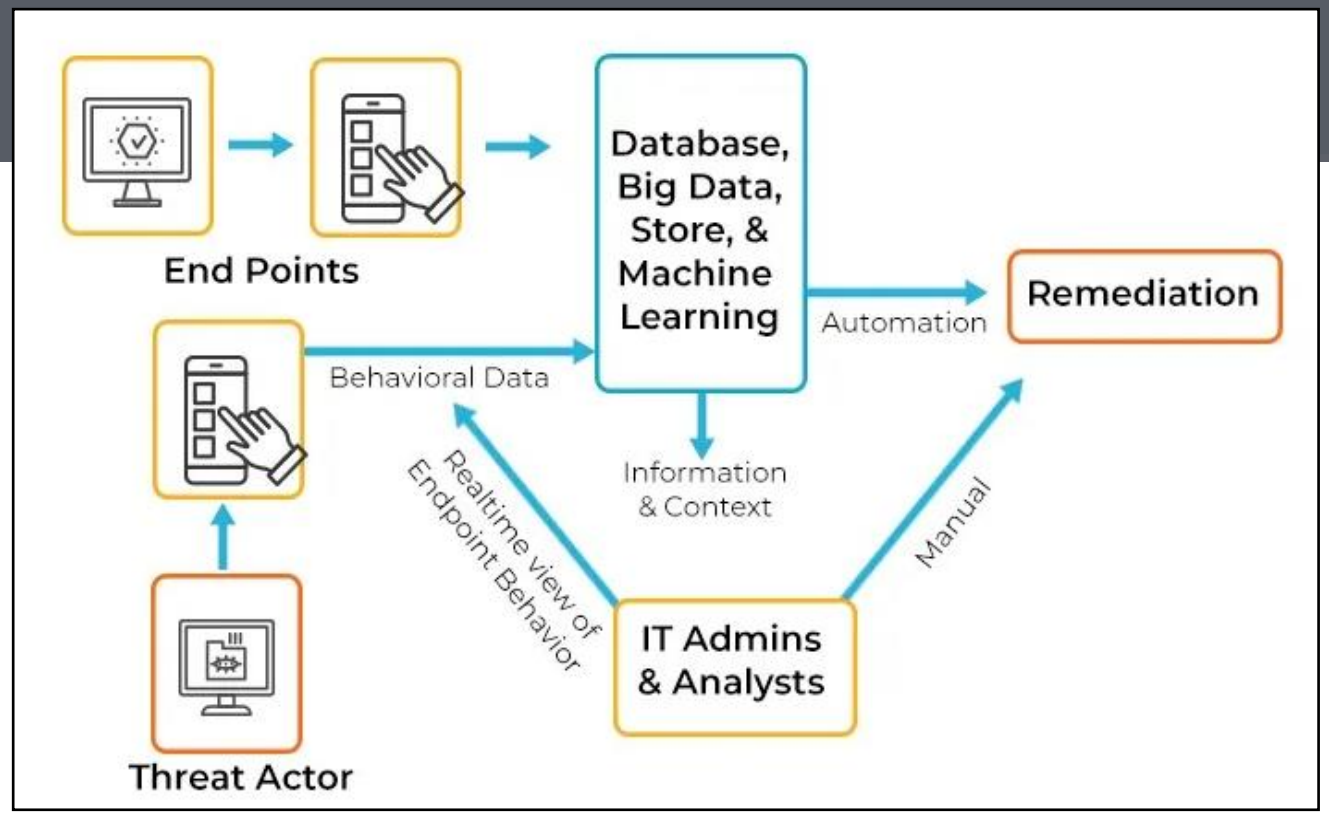
Endpoint Security – Web based



Source: CompTIA Security+ Guide to Network Security Fundamentals Eighth Edition, Mark Ciampa, Cengage Learning, Inc, 2023, page 159

Server-Side Request Forgery (SSRF) dilakukan dengan mengambil keuntungan terhadap server yang melakukan tindakan berdasarkan url, jika url bisa ditambahkan script yang melakukan eksekusi langsung maka dapat dilakukan suatu tindakan pengiriman informasi terhadap korban yang posisinya telah login, sehingga tindakan dianggap sah oleh server

Pengamanan Endpoint



Source: https://medium.com/@kavib/endpoint-detection-and-response-edr-390b7eae4999

Endpoint Detection and Response (EDR)

EDR merupakan cyber security monitoring tools yang dapat memantau aktivitas tidak wajar dari perangkat pengguna sehingga dapat dilakukan tindakan sesegera mungkin

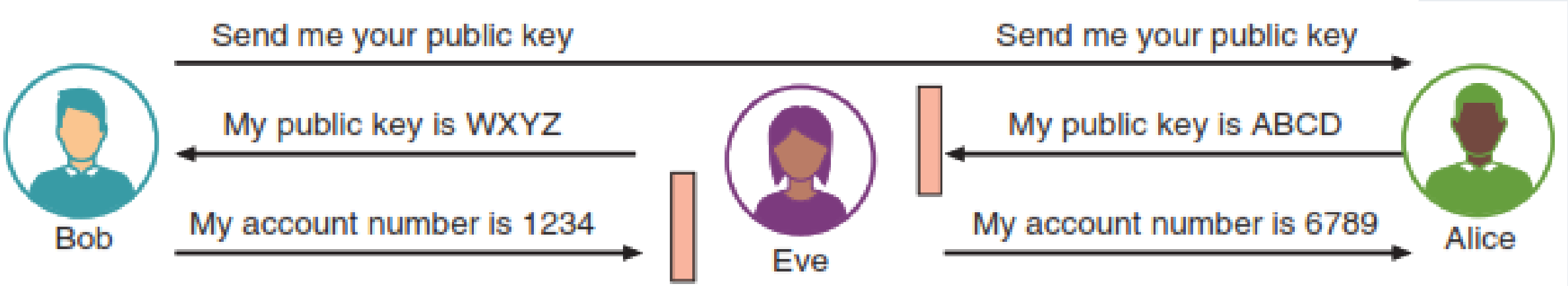
ANTIVIRUS

Penambahan antivirus dapat mencegah menyebarnya malware-malware berbahaya pada perangkat pengguna, tentunya antivirus ini harus memiliki teknologi dan database yang up to date

03

Network Security

Man-in-the-Middle (MITM)

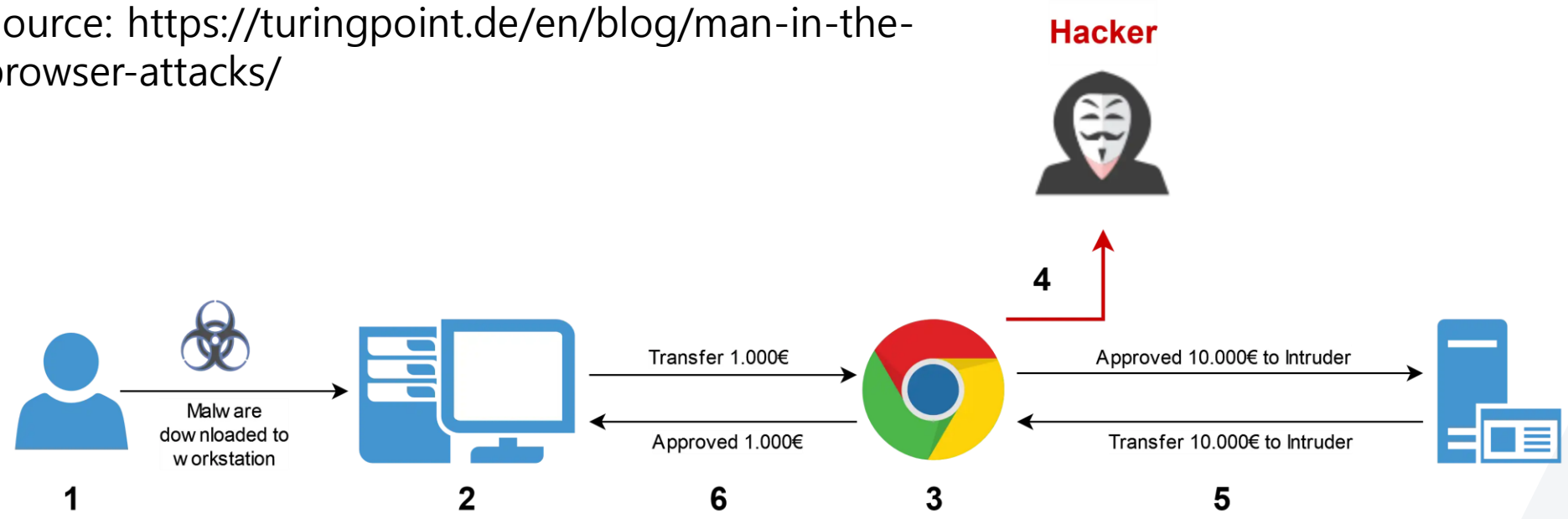


Source: CompTIA Security+ Guide to Network Security Fundamentals Eighth Edition, Mark Ciampa, Cengage Learning, Inc, 2023, page 256

MITM biasanya dilakukan dengan menggunakan algoritma untuk mendekripsi packet dalam lalu lintas jaringan atau dilakukan dengan menjadi perantara antara dua buah koneksi TCP dengan berperan jadi pihak yang hendak berkomunikasi

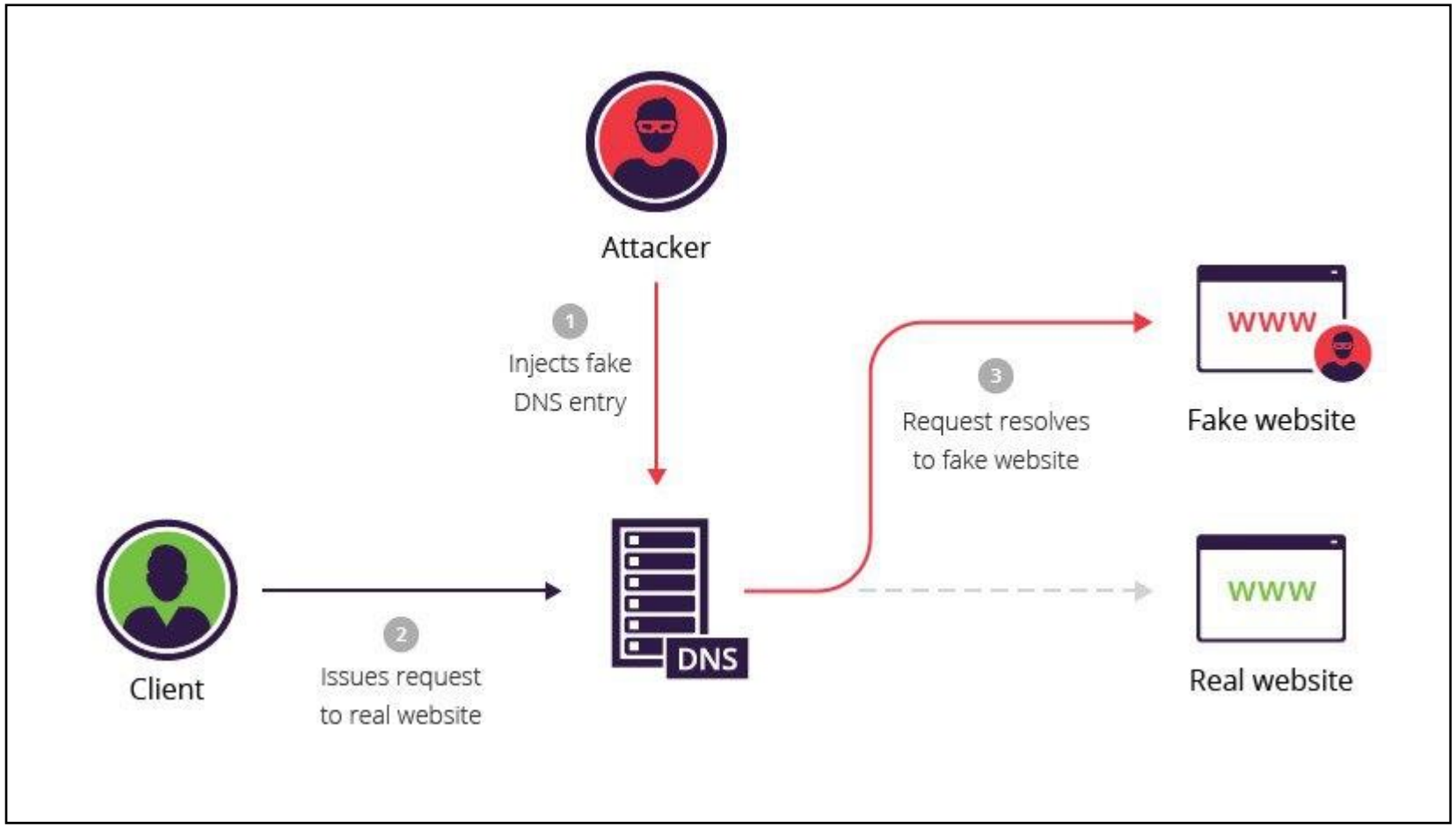
Man-in-the-Browser (MITB)

Source: https://turingpoint.de/en/blog/man-in-the-browser-attacks/



MITB dilakukan dengan memanfaatkan malware yang berperan sebagai extensions dari browser untuk memodifikasi request yang dikirimkan dari browser ke situs tertentu

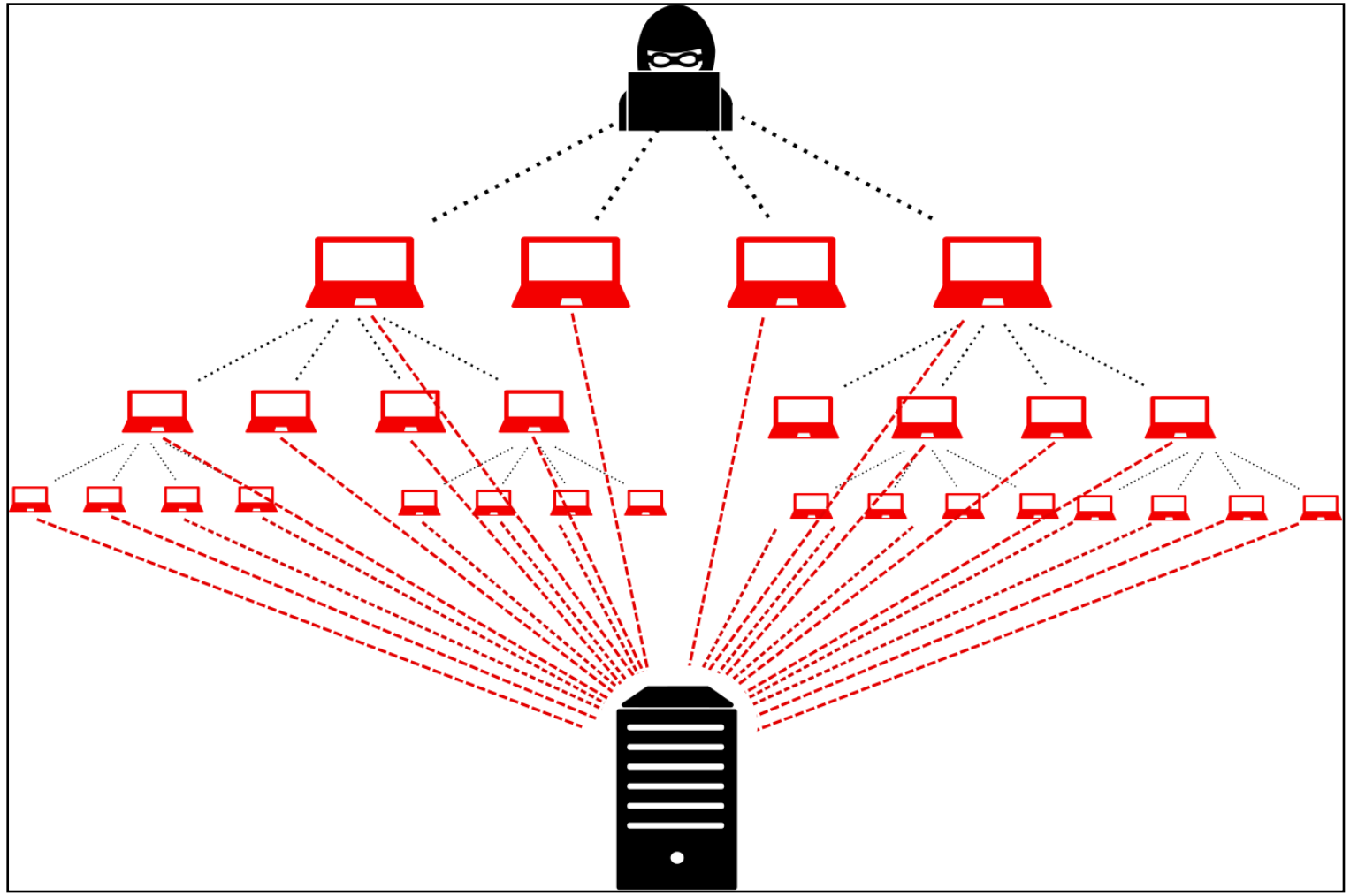
DNS Poisoning



DNS poisoning digunakan untuk memodifikasi DNS chace yang terdapat pada PC client atau DNS lokal sehingga url aslinya ditujukan kepada halaman web palsu yang biasanya dibuat menyerupai halaman web yang asli untuk mendapatkan username dan password

Source: https://www.imperva.com/learn/application-security/dns-spoofing/

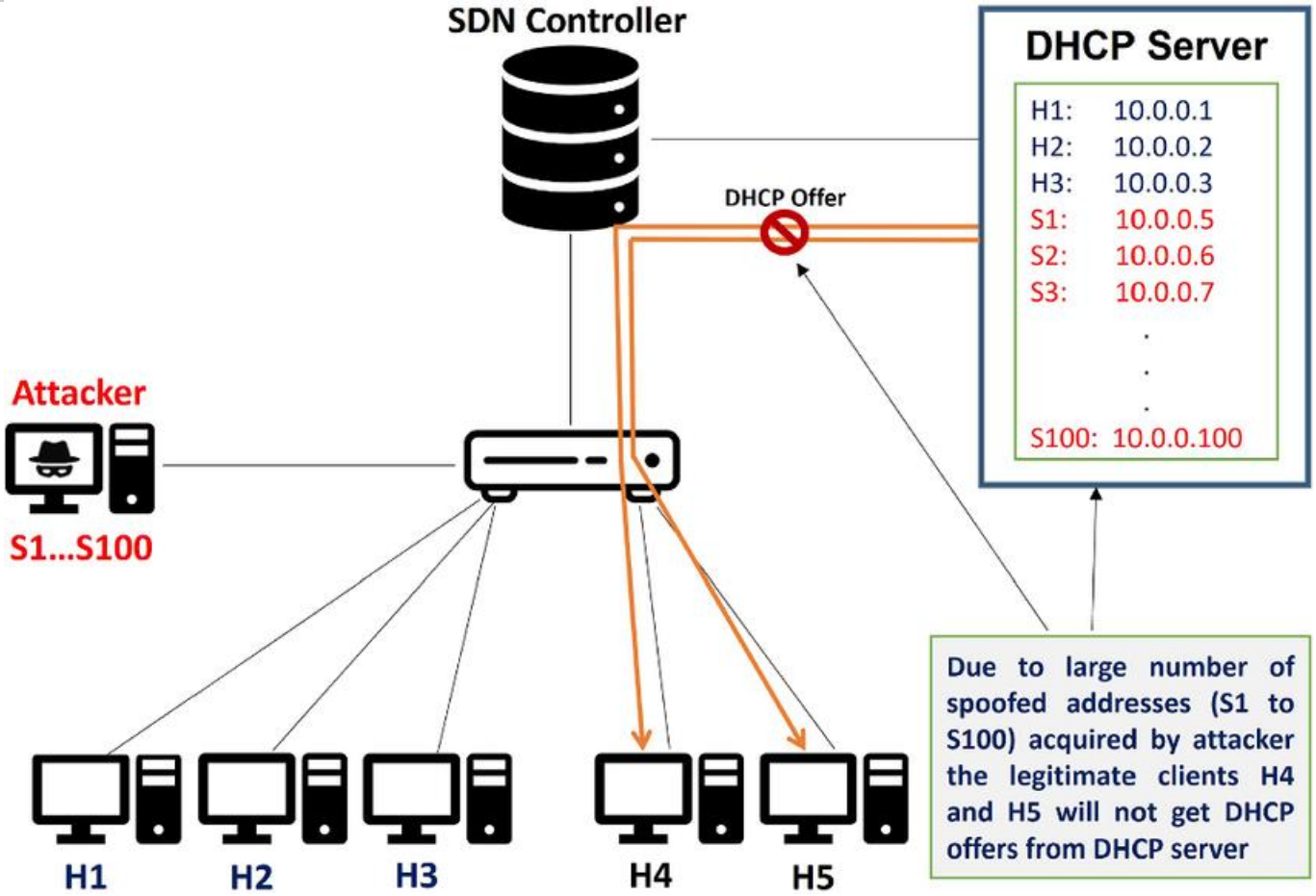
Distributed Denial of Service (DDoS)



DDOS biasanya menggunakan banyak komputer yang telah disusupi malware trojan untuk mengirimkan banyak request dalam waktu bersamaan terhadap komputer target, sehingga komputer target tidak dapat memproses permintaan yang sangat banyak dan menyebabkan lumpuhnya sistem

Source: https://ruggedtooling.com/what-are-ddos-attacks/

DHCP Starvation



Source: Ishtiaq, Hafiz & Bhutta, Areeb & Mian, Adnan. (2023). DHCP DoS and starvation attacks on SDN controllers and their mitigation. Journal of Computer Virology and Hacking Techniques. 20. 1-11. 10.1007/s11416-023-00483-0.

DHCP Starvation dilakukan dengan meminta IP Address sebanyak mungkin menggunakan DHCP offer yang berisi mac address palsu sehingga client lain di dalam jaringan tidak mendapatkan IP Addres, apabila DHCP server diletakkan di router juga akan membuat kinerja router menjadi penuh dengan permintaan DHCP yang membuatnya tidak dapat memforward paket

Pengamanan Network

Physical Location

Mengamankan perangkat jaringan pada ruangan tertentu atau lokasi yang sulit dijangkau oleh orang lain yang tidak memiliki akses untuk melakukan konfigurasi terhadap jaringan komputer

Metode pengamanan Layer 2 dan 3

Lakukan penerapan metode pengamanan pada perangkat jaringan layer 2 dan layer 3 seperti, DHCP Snooping, Port Security, Bridge Filter, dan yang lainnya untuk mengamankan jaringan dari serangan yang berasal dari internal

Pengamanan Network

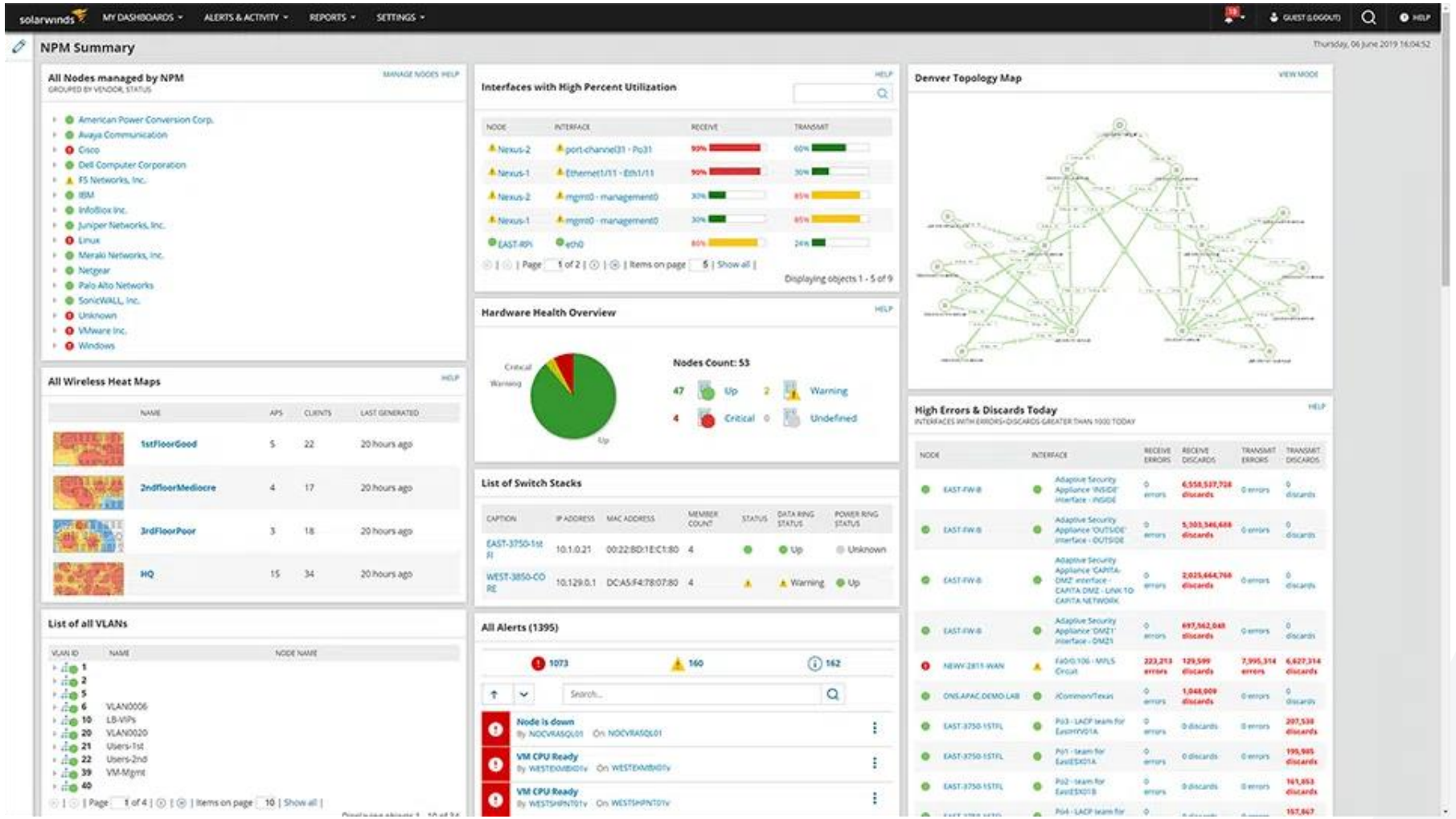
Firewall

Lakukan penerapan firewall pada perangkat layer 3 khususnya di gateway untuk membatasi akses jaringan dari pihak eksternal atau di luar dari LAN

Monitoring Jaringan Secara Berkala

Lakukan monitoring jaringan secara berkala untuk melihat ada tidaknya perangkat jaringan yang tidak terdaftar atau yang bukan dikonfigurasi oleh admin jaringan

Pengamanan Network



Tools Monitoring Traffic

Gunakan tools untuk memonitoring lalu lintas jaringan sehingga dapat mengamati pola permintaan traffic yang tidak wajar

Source: https://blog.netwrix.com/2023/12/27/network-monitoring-tools/

Referensi

- CompTIA Security+ Guide to Network Security Fundamentals Eighth Edition, Mark Ciampa, Cengage Learning, Inc, 2023
- Ishtiaq, Hafiz & Bhutta, Areeb & Mian, Adnan. (2023). DHCP DoS and starvation attacks on SDN controllers and their mitigation. Journal of Computer Virology and Hacking Techniques. 20. 1-11. 10.1007/s11416-023-00483-0.
- Ivan Lee (Accessed: 2024, October 30). CIA Triad Definition. Examples of Confidentiality, Integrity, and Availability. https://www.wallarm.com/what/cia-triad-definition

Referensi

- Height8 Technologies Pvt. Ltd. (Accessed: 2024, October 30). What is AAA?. https://www.height8tech.com/blog.php?blog=aaa-server
- Mukhadin Beschokov (Accessed: 2024, October 30). What is XSS (cross site scripting) attack ?. https://www.wallarm.com/what/what-is-xss-cross-site-scripting
- Mukhadin Beschokov (Accessed: 2024, October 30). Structured query language Injection (SQLi) - Part 1. https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

Referensi

- Kavitha Bangalore (Accessed: 2024, October 30). Endpoint detection and response (EDR). https://medium.com/@kavib/endpoint-detection-and-response-edr-390b7eae4999
- Fabian Gold (Accessed: 2024, October 30). Man-in-the-Browser Attacks. https://turingpoint.de/en/blog/man-in-the-browser-attacks/
- Imperva (Accessed: 2024, October 30). DNS Spoofing. https://www.imperva.com/learn/application-security/dns-spoofing/

Referensi

- Rugged Tooling Oy (Accessed: 2024, October 30). What are DDoS attacks?. https://ruggedtooling.com/what-are-ddos-attacks/
- Dirk Schrader (Accessed: 2024, October 30). Understanding the 4 Types of Network Monitoring Tools and Comparing Available Solutions. https://blog.netwrix.com/2023/12/27/network-monitoring-tools/

Week 16

Final Exam