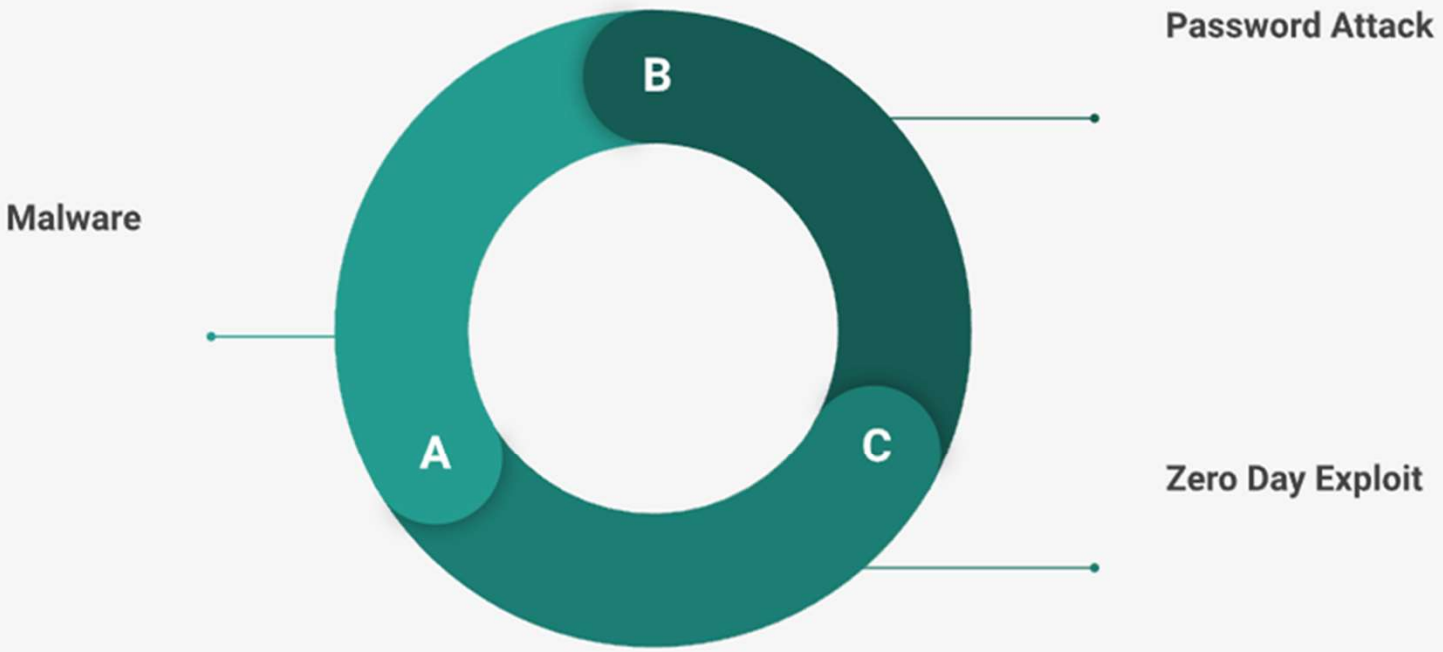
Pertemuan 3

Ancaman Keamanan & Pencegahannya “Software”

PRU/SPMI/FR-BM-18/0222

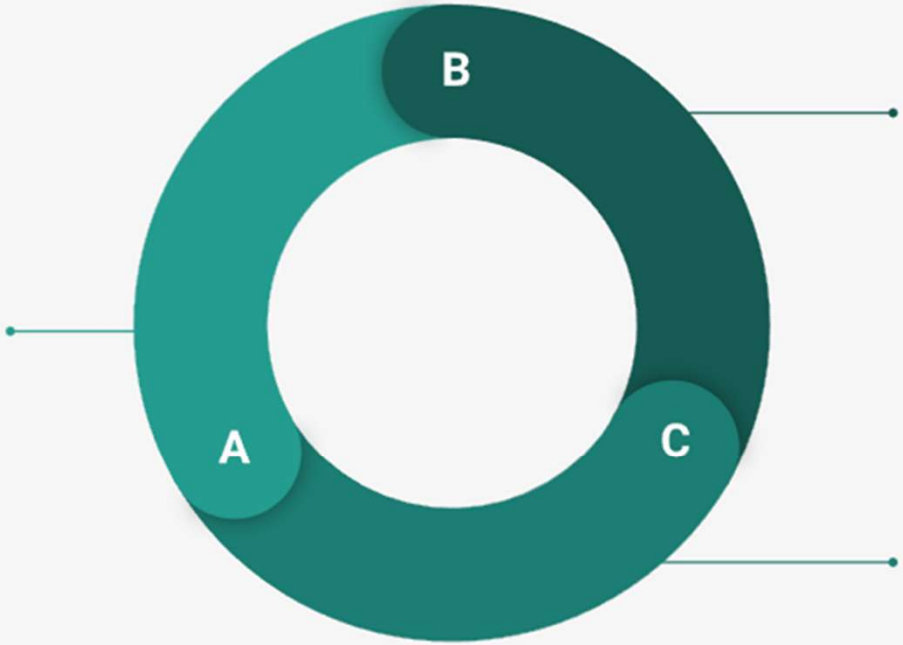
Pembahasan dan Sub Pembahasan Ancaman Keamanan Software



Pembahasan dan Sub Pembahasan Ancaman Keamanan Software

Malware

Apa itu malware dan jenis-jenisnya, Bahaya malware, Teknik penyebaran malware dan **Bagaimana pencegahan ancaman malware**.



Password Attack

Perbedaan password dengan hash, Demo password attack dan **Bagaimana pencegahan ancaman password attack**.

Zero Day Exploit

Perbedaan Vulnerability, Exploit dan Zero Day Exploit, Demo Salah Satu Bahaya Exploit, Vidio salah satu Exploit, **Bagaimana pencegahan ancaman.**

A. Ancaman Keamanan “Malware”

- Malware atau malicious software adalah perangkat lunak yang dirancang khusus untuk ***mengganggu***, ***merusak*** atau ***mengakses sebuah sistem komputer*** secara tidak sah.
- Jenis-jenis malware :

1949	1974	1988
Virus	**Trojan**	**Worm**
“Theory of self-reproducing automata” By. John Von Neuman	Derived from the ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.	It takes advantage of bugs and security holes to travel from network to network. By. Robert Morris

- Virus + Trojan + Worm menjadi satu ?

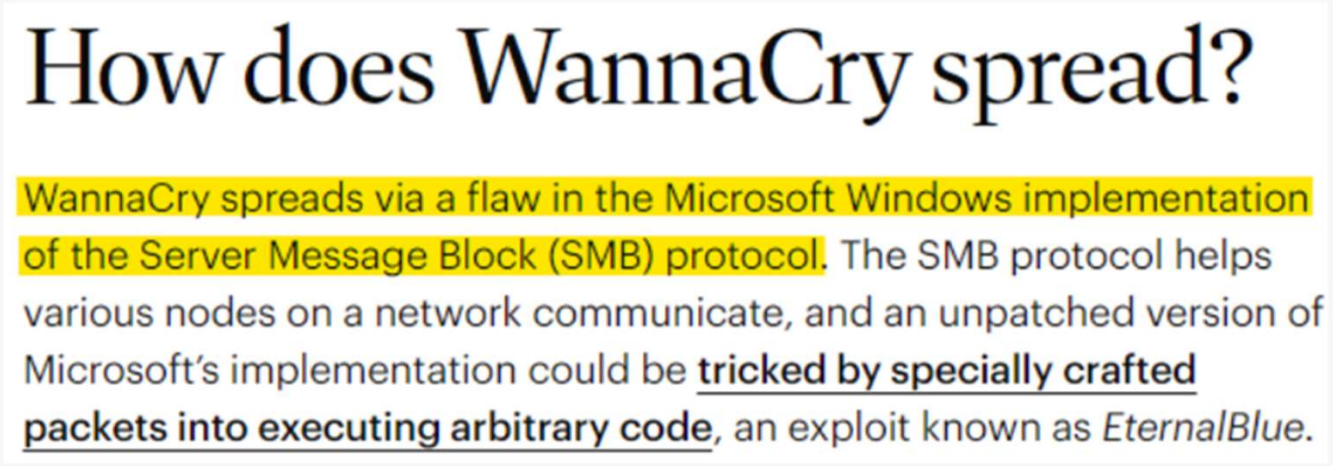
LIVE DEMO TROJAN PRORAT

Bagaimana melakukan pencegahan malware ?

Bagaimana teknik penyebaran malware ?

Bagaimana teknik penyebaran malware ?

a. Melalui media penyimpanan USB atau jaringan, biasanya malware memanfaatkan kerentanan atau celah yang ada pada sistem operasi.
   - Fitur Auto Run di Windows
   - Vulnerabilities : SMBv1 (Server Message Block version 1), Common Log File System (CLFS), Bash Bug



How does WannaCry spread?

WannaCry spreads via a flaw in the Microsoft Windows implementation of the Server Message Block (SMB) protocol. The SMB protocol helps various nodes on a network communicate, and an unpatched version of Microsoft's implementation could be **tricked by specially crafted packets into executing arbitrary code**, an exploit known as *EternalBlue*.

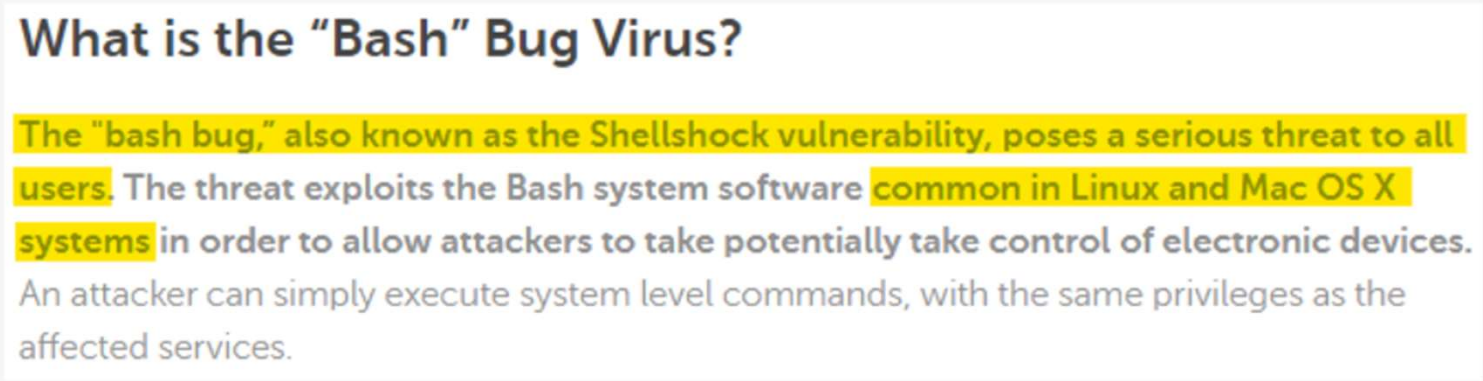
Bagaimana teknik penyebaran malware ?

a. Melalui media penyimpanan USB atau jaringan, biasanya malware memanfaatkan kerentanan atau celah yang ada pada sistem operasi.
   - Fitur Auto Run di Windows
   - Vulnerabilities : SMBv1 (Server Message Block version 1), Common Log File System (CLFS), Bash Bug

> According to Kaspersky, the Nokoyawa ransomware gang has used other exploits targeting the Common Log File System (CLFS) driver since June 2022, with similar yet distinct characteristics, linking them all to a single exploit developer.
>
> The group has used at least five more CLFS exploits to target multiple industry verticals, including but not limited to retail and wholesale, energy, manufacturing, healthcare, and software development.

Bagaimana teknik penyebaran malware ?

a. Melalui media penyimpanan USB atau jaringan, biasanya malware memanfaatkan kerentanan atau celah yang ada pada sistem operasi.
   - Fitur Auto Run di Windows
   - Vulnerabilities : SMBv1 (Server Message Block version 1), Common Log File System (CLFS), Bash Bug



What is the "Bash" Bug Virus?

The "bash bug," also known as the Shellshock vulnerability, poses a serious threat to all users. The threat exploits the Bash system software common in Linux and Mac OS X systems in order to allow attackers to take potentially take control of electronic devices. An attacker can simply execute system level commands, with the same privileges as the affected services.

b. Melalui *E-mail*, *media social* dan *aplikasi bajakan* dengan teknik *phishing* atau *fishing*.

Teknik *phishing* juga disebut teknik *social engineering* karena memanfaatkan kerentanan atau celah yang ada pada manusia sebagai pengguna komputer untuk membahayakan atau menyerang sebuah sistem komputer.

Kerentanan yang biasa dijadikan celah :

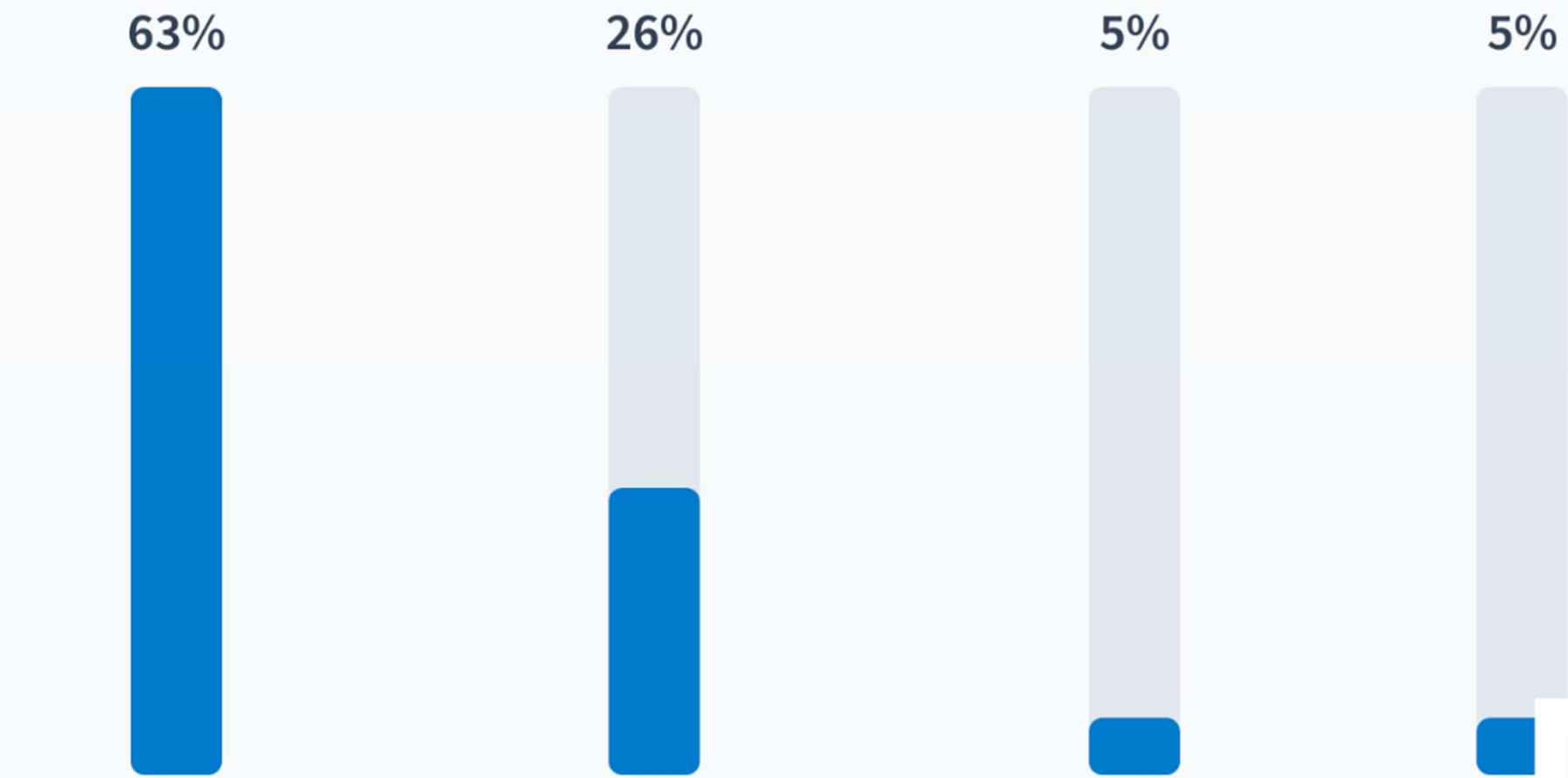
- Rasa penasaran/ketertarikan
- Rasa takut/khawatir
- Kebutuhan
- Ketidaktahuan
- Ketidaktelitian

Pencegahan dari ancaman malware

Teknik penyebaran malware	Pencegahan
Melalui USB Memory Drive	Mematikan fitur Autorun USB di SO windows
Melalui Vulnerabilities/Bug Software	Rutinkan update SO dan aplikasi
Melalui E-mail, medsos dan aplikasi bajakan	Selalu verifikasi sebelum membuka link, mengizinkan akses atau menginstall aplikasi

Kapan terakhir kali anda melakukan update sistem operasi dikomputer anda ?

19



B. Ancaman Keamanan “password sistem operasi”

- Password membatasi **otoritas** pengguna komputer dalam mengakses atau mengubah data di dalam sebuah komputer.
- Password dengan Hash password

- Lokasi penyimpanan hash password di sistem operasi :

  Windows : /Windows/System32/config/SAM

  Linux : /etc/shadow

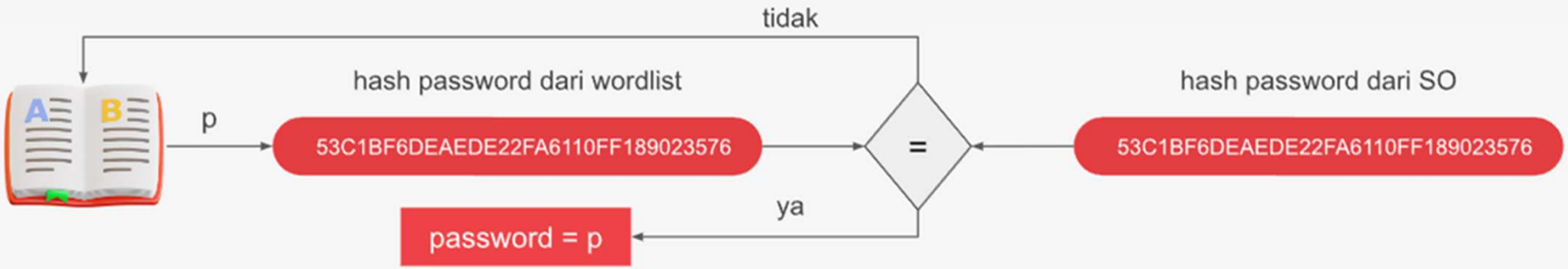
1. Ancaman Remove Password SO Windows

Demo, Hapus Password Windows 10 Tanpa Login

a. Software : chntpw
b. File Password : /Windows/System32/config/**SAM**

2. Ancaman Cracking Password SO ?

Alur Cracking Password Menggunakan Teknik Bruteforce



Demo, Crack Password Linux

a. Software : John The Ripper
b. File Password : /etc/shadow

LIVE DEMO

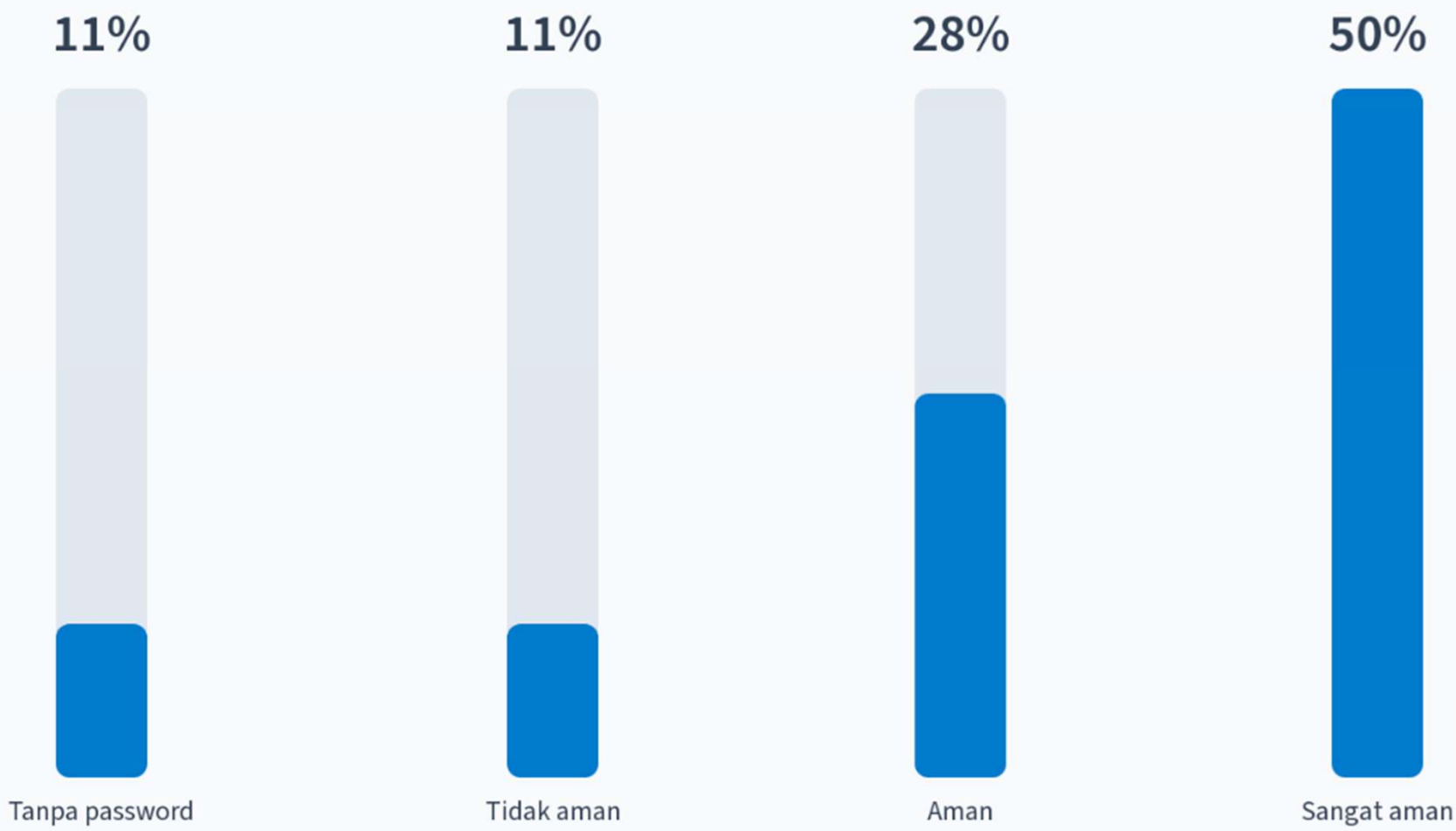
Perintah 1 : sudo cp /etc/shadow /etc/passwd ~/Documents
Perintah 2 : sudo unshadow passwd shadow >> unshadow.txt
Perintah 3 : sudo john unshadow.txt --wordlist /usr/share/wordlists/fasttrack.txt --format=crypt

Pencegahan ancaman keamanan password sistem operasi

Ancaman	Pencegahan
Password Cracking	1. Panjang password minimal 8 karakter 2. Jangan gunakan kata-kata yang ada didalam kamus, kata-kata yang umum, nama orang dan nama tempat 3. Gunakan gabungan huruf kecil, huruf besar, angka dan simbol
Password Remove	1. Enkripsi partisi system 2. …

Seberapa amankah menurut anda, password yang anda gunakan dikomputer anda ?

18



C. Ancaman Keamanan “Zero Day Exploit”

- Vulnerability adalah kualitas atau keadaan sebuah software yang memiliki celah/bug yang membahayakan sistem komputer.
- Exploit adalah sebuah **script**, **perangkat lunak** atau **dokumen** yang memanfaatkan Vulnerability atau Kerentanan yang ada di sebuah software termasuk sistem operasi untuk mendapatkan akses sebuah sistem komputer tanpa proses autentikasi.
- Zero Day Exploit adalah Exploit yang baru berumur 0 hari atau baru dibuat dan belum ada patch atau perbaikan pada Vulnerability-nya.

LIVE DEMO

Pencegahan dari ancaman Exploit

Ancaman	Pencegahan
Exploit	Rutinkan update SO dan aplikasi
Zero Day Exploit	-

Tugas # Keamanan Internet - Pertahanan Internet

Banyak negara yang mengalami kesulitan dalam menghadapi berbagai serangan siber dari kriminal negara lain. Salah satu usaha untuk mengatasinya dengan mendirikan CSIRT. Pertanyaannya adalah, siapa yang seharusnya mengalokasikan dana untuk membiayai lembaga ini mengingat begitu banyaknya titik-titik penting yang harus dilindungi di sebuah negara!

Berapa persen anggaran yang harus disisihkan untuk membangun sistem pengamanan yang baik?

TERIMA KASIH
PERTANYAAN ?