PANDUAN TEKNIS

PROSES IDENTIFIKASI DAN ANALISIS

Dokumen ini menjelaskan secara teknis proses identifikasi dan analisis untuk memastikan bahwa insiden yang telah terjadi dapat diketahui sumber serangannya. Selain itu juga untuk mengumpulkan informasi yang cukup tentang insiden tersebut sehingga tim dapat memprioritaskan langkah selanjutnya dalam menangani insiden. Dalam melakukan proses identifikasi insiden, tim yang bertugas diharuskan melakukan proses dengan menggunakan akun administrator atau root. Rincian proses identifikasi dan analisis adalah sebagai berikut :

A. Identifikasi dan Analisis Kerentanan

Proses	Penjelasan	Tools
Identifikasi Kerentanan Sistem	Melakukan identifikasi kerentanan dengan menggunakan tools baik yang Open Source maupun Lisensi. Proses ini bertujuan untuk menemukan kerentanan dengan berdasarkan teknik scanning atau secara otomatis dengan tools. Analisis dilakukan dengan memeriksa tingkat kerentanan yang ditemukan oleh tools tersebut, High/Medium/Low. Dan lakukan verifikasi dengan melakukan akses pada halaman/aplikasi yang terdapat kerentanan.	Open Source (Kali Linux): • Nikto • Burp Suite Lisensi : • Accunetix • Nessus Online Scanning : • Virus Total (https://virustotal.com) • Sucuri (https://sitecheck. sucuri.net)
Identifikasi Kerentanan Sistem File atau Direktori	Melakukan identifikasi sistem File atau Direktori dengan menggunakan tools atau scanning secara otomatis. Proses ini bertujuan untuk menemukan File atau Direktori yang bersifat Publik dan terdapat kerentanan pada File atau Direktori tersebut. Analisis dilakukan dengan memeriksa secara langsung File atau Direktori yang ditemukan dan melakukan	Open Source (Kali Linux) : • Uniscan Command : # uniscan -u <url> -qwed Contoh : # uniscan -u https://govcsirt.bssn.go.id -qwed

	verifikasi pada halaman yang terdapat kerentanan File atau Direktori.	
Identifikasi Kerentanan Content Management System (CMS)	Melakukan identifikasi sistem website yang menggunakan CMS secara otomatis dengan tools scanning. Tujuannya untuk menemukan kerentanan baik Versi/Plugins/Library yang telah usang (Old Version). Analisis dilakukan dengan memeriksa hasil scanning dan memverifikasi pada Website CVE Details dan Exploit-DB.	Open Source (Kali Linux) : • CMS Wordpress # wpscan -u https://x123.com • CMS Joomla # joomscan -u https://x123.com • CMS Drupal # droopalscan -u https://x123.com
Identifikasi Kerentanan Listening Port (Port yang terbuka)	Melakukan identifikasi Listening Port dengan menggunakan tools untuk menemukan Layanan yang dibuka. Analisis dilakukan dengan memeriksa hasil scanning dan memverifikasi pada Website Exploit-DB atau via Google Dork dengan keyword Nama dan Versi Layanan yang ditemukan.	Open Source (Kali Linux) : • Nmap Command : # nmap -A target # nmap -v -sU -sS -p- -A -T4 target Contoh : # nmap -A 192.168.8.120 # nmap -v -sU -sS -p- -A -T4 192.168.8.120

B. Identifikasi dan Analisis Environment System

Proses	Penjelasan	Command
Identifikasi Rute Jaringan (Network Routing)	Melakukan identifikasi jaring komunikasi yang terhubung dari Server menuju koneksi internet. Analisis dilakukan dengan memeriksa daftar perangkat atau IP address yang terkoneksi server menuju koneksi internet global	Untuk Debian Varian : # traceroute 8.8.8.8 Untuk RHEL/Centos : # tracepath 8.8.8.8 Untuk Windows : C:\> netstat -r

Identifikasi Versi Sistem Operasi	Melakukan identifikasi versi dan distribusi sistem operasi yang digunakan. Analisis dilakukan dengan memeriksa hasil yang ditemukan dan memverifikasi pada Website Exploit-DB atau via Google Dork dengan keyword Nama dan Versi Sistem Operasi yang ditemukan.	Mencetak versi kernel (Debian/RHEL/Centos) : # uname -a Mencetak distribusi Debian OS : # cat /etc/lsb-release Mencetak distribusi RHEL/CentOS : # cat /etc/redhat-release Untuk Windows : C:\> ver C:\> set

C. Identifikasi dan Analisis Aplikasi / Layanan

Proses	Penjelasan	Command
Identifikasi Daftar Layanan/Proses yang Berjalan	Melakukan identifikasi layanan/proses yang berjalan dengan menggunakan tools yang telah ada pada sistem operasi. Hal ini bertujuan untuk mencari layanan/proses yang menggunakan resource sangat tinggi atau malicious service. Analisis dilakukan dengan memeriksa layanan/proses yang menggunakan resource yang tinggi, lalu memvalidasi user yang menggunakan serta ID Layanan tersebut.	Debian/RHEL/CentOS : # ps -aux Windows : C:\> net start C:\> sc query C:\> sc query <service> C:\> sc queryex state= all
Identifikasi Daftar Aplikasi yang Berjalan	Melakukan identifikasi daftar aplikasi yang berjalan dengan menggunakan tools yang telah ada pada sistem operasi. Hal ini bertujuan untuk mencari aplikasi yang menggunakan resource sangat tinggi atau malicious application.	Debian/RHEL/CentOS : # top Windows : C:\> tasklist

	Analisis dilakukan dengan memeriksa aplikasi yang menggunakan resource yang tinggi, lalu memvalidasi user yang menggunakan serta ID Aplikasi tersebut.	
Identifikasi Riwayat/History Sistem Operasi	Melakukan identifikasi seluruh program/aplikasi/layanan yang telah dijalankan oleh user. Analisis dilakukan dengan memeriksa daftar program/aplikasi/layanan tersebut yang merupakan program/aplikasi/layanan bersifat maliciuos serta melakukan analisis kegiatan yang dilakukan dari User tersebut.	Debian/RHEL/CentOS : # history
Identifikasi Aplikasi Terjadwal	Melakukan identifikasi terhadap aplikasi yang berjalan secara terjadwal baik per menit, per jam, per hari. Analisis dilakukan dengan menemukan daftar tersebut dan memverifikasi terkait adanya malicious aplikasi terjadwal.	Debian/RHEL/CentOS : # ls /etc/cron* # crontab -l Untuk Windows : C:\> schtask C:\> wmic startup list full C:\> wmic startup get Caption, Command

D. Identifikasi dan Analisis Jaringan Komunikasi

Proses	Penjelasan	Command
Identifikasi Jaringan Komunikasi yang Dibuka	Melakukan identifikasi dengan menampilkan daftar layanan/aplikasi/port yang terbuka atau bersifat Listening Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious application/port.	Debian/RHEL/CentOS : # netstat -tulnp Windows : C:\> netstat -nao C:\> netstat -nao 5

Identifikasi Jaringan Komunikasi yang Dibuka	Melakukan identifikasi dengan menampilkan daftar layanan/aplikasi/port yang telah terbangun (Established). Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious connection.	Debian/RHEL/CentOS : # netstat -antup | grep "ESTA" Windows : C:\> netstat -nao
Identifikasi Koneksi ke Server	Melakukan identifikasi dengan menampilkan daftar User dan IP yang sedang melakukan akses interface (TTY) seperti contoh akses SSH, akses onBoard ke OS Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious application/port.	Debian/RHEL/CentOS : # w Windows : C:\> net session C:\> net share C:\> net use
Identifikasi DNS dan Hostname	Melakukan identifikasi terkait dengan konfigurasi DNS dan hostname yang ada pada sistem operasi. Analisis dilakukan dengan memeriksa setiap konten pada file konfigurasi DNS dan Hostname.	Debian/RHEL/CentOS : # cat /etc/resolv.conf # cat /etc/hostname # cat /etc/hosts Windows : C:\> ipconfig /displaydns

E. Identifikasi dan Analisis User

Proses	Penjelasan	Command
Identifikasi Daftar User	Melakukan identifikasi terkait dengan daftar user yang ada pada sistem operasi. Dan melakukan identifikasi user yang punya akses terminal atau bash system. Analisis dilakukan dengan memeriksa setiap user pada file daftar user tersebut.	Debian/RHEL/CentOS : # cat /etc/passwd | grep "bash" Windows : C:\> net user C:\> net user nama_user C:\> net localgroup C:\> net localgroup administrators
Identifikasi Daftar User Logged In	Melakukan identifikasi terkait dengan user yang pernah melakukan	Debian/RHEL/CentOS : # lastlog

	Login serta waktu dilakukannya aktivitas login. Analisis dilakukan dengan memeriksa setiap user yang telah login dan waktu login.	# last

F. Identifikasi dan Analisis Direktori

Proses	Penjelasan	Command
Identifikasi Direktori Web Server	Melakukan identifikasi direktori penyimpanan file aplikasi/website yang terkena insiden. Identifikasi dilakukan dengan time analysis yaitu memfilter berdasarkan waktu terakhir file/direktori dilakukan perubahan. Analisis dilakukan dengan memeriksa setiap file/folder pada direktori tersebut.	Debian/RHEL/CentOS : # ls -alrt /var/www/html Windows : C:\> tree /F /A <drive> C:\> wmic environment get Description, VariableValue
Identifikasi Direktori Konfigurasi Web Server	Melakukan identifikasi direktori penyimpanan file konfigurasi web server yang terkena insiden. Analisis dilakukan dengan memeriksa konfigurasi web pada direktori tersebut.	Debian : # cat /etc/apache2/apache2.conf # ls -alrt /etc/apache2/conf-available/ RHEL/CentOS : # cat /etc/httpd/conf/ httpd.conf # ls -alrt /etc/httpd/conf.d/

G. Identifikasi dan Analisis Malicious File

Proses	Penjelasan	Command
Identifikasi Malicious File / Backdoor	Melakukan identifikasi file-file yang diasumsikan merupakan malicious file atau backdoor file. Identifikasi dilakukan dengan memfilter tiap file	Debian/RHEL/CentOS : # grep -RPn "(passthru|shell_exec |system|phpinfo|base64_decode |chmod|mkdir|fopen|fclose|fclose| readfile) *" nama_direktori

	yang mempunyai konten string mengakses bash/shell, eksekusi file/aplikasi, membuka/menutup file, dll Analisis dilakukan dengan memeriksa setiap file yang ditampilkan.	# grep -Rinw nama_direktori -e "nama_string" Contoh : # grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *" /var/ww/html # grep -Rinw /var/www/html -e "Hacked" Windows : C:\> find "nama_string_dicari"

H. Identifikasi dan Analisis Log

Proses	Penjelasan	Command
Identifikasi Direktori Access Log	Melakukan identifikasi direktori penyimpanan file log baik aplikasi, web server, ataupun error log. Analisis dilakukan dengan memeriksa secara detail mengenai konten dari setiap log tersebut. command tail -200 digunakan untuk menampilkan 200 baris terakhir dari file command tail -f digunakan untuk menampilkan baris-baris terakhir secara live pada file	Debian : # ls -alrt /var/log/apache2/ # tail -200 /var/log/apache2/access_log # tail -f /var/log/apache2/access_log # tail -200 /var/log/apache2/ssl_access_log RHEL/CentOS : # ls -alrt /var/log/httpd/ # tail -200 /var/log/httpd/access_log # tail -f /var/log/httpd/access_log # tail -200 /var/log/httpd/ssl_access_log Windows : C:\> eventvwr.msc

		(Security >> Special Logon (4672)) Export to *.evtx file
Identifikasi Log Berdasarkan Malicious File	Melakukan identifikasi malicious file yang ditemukan pada file Log. Analisis dilakukan dengan memeriksa identitas, timestamp, status code yang melakukan akses pada malicious file	Debian : # cat /var/log/apache2/ access_log | grep "nama_malicious_file" RHEL/CentOS : # cat /var/log/httpd/ access_log | grep "nama_malicious_file"
Identifikasi Log Berdasarkan IP Address	Melakukan identifikasi alamat IP yang melakukan malicious connection. Analisis dilakukan dengan memeriksa aktivitas yang dilakukan oleh alamat IP yang ditemukan.	Debian : # cat /var/log/apache2/ access_log | grep "ip_address" RHEL/CentOS : # cat /var/log/httpd/ access_log | grep "ip_address"

I. Identifikasi dan Analisis Database

Proses	Penjelasan	Command
Identifikasi Database	Melakukan identifikasi malicious string pada sistem database yang digunakan. Analisis dilakukan dengan memeriksa tabel dan string pada database.	Debian/RHEL/CentOS : # mysql -u root -p nama_database > nama_file_export.sql Lalu masukan password root. Contoh : # mysql -u root -p csirt_db > export_db.sql

J. Identifikasi dan Analisis IP Address

Proses	Penjelasan	Tools
Identifikasi Alamat IP	Melakukan analisis sebuah alamat IP, baik pemilik IP, reputasi IP, IP report.	Whois IP : https://www.ultratools.com/tools/ipWhoisLookupResult IP Analyze : - https://www.ipalyzer.com/ - https://mxtoolbox.com/blacklists.aspx - https://www.abuseipdb.com/ IP Reputation : https://www.talosintelligence.com/reputation_center