KISI-KISI RESPON INSIDEN SIBER UNTUK SERVER ADMINISTRATOR

Berikut adalah tips untuk memeriksa sistem dan memutuskan apakah perlu dilakukan eskalasi pada respons insiden.

Menilai Situasi yang Mencurigakan

Untuk mempertahankan jejak penyerang, hindari mengambil tindakan yang mengakses banyak file ataupun melakukan pemasangan alat.

Lihat log dari sistem, keamanan, dan aplikasi untuk mengetahui apakah kejadian (*event*) yang tidak biasa.

Lihat detail konfigurasi jaringan dan koneksi; catat pengaturan, *session* atau *port* yang tidak normal.

Lihat daftar pengguna untuk akun yang tidak sah atau yang sudah tidak aktif.

Lihat daftar proses yang sedang berjalan atau aktivitas terjadwal yang tidak seharusnya ada.

Cari program terkonfigurasi yang tidak biasa yang berjalan secara otomatis saat sistem mulai.

Periksa pengaturan ARP and DNS; lihat isi dari file *host* untuk entri yang tidak seharusnya ada,

Cari file yang tidak biasa dan verifikasi integritas OS dan file aplikasi.

Gunakan *sniffer* jaringan (pada sistem atau tersedia secara eksternal) untuk mengamati aktivitas yang tidak biasa.

Rootkit kemungkinan dapat menyembunyikan kebocoran dari alat; percayalah pada insting Anda jika merasa ada yang tidak tepat pada sistem.

Periksa masalah yang baru-baru ini dilaporkan, deteksi intrusi, dan peringatan terkait untuk sistem.

Jika Anda percaya adanya Kebocoran

Libatkan tim respon insiden (CSIRT) untuk langkah selanjutnya, dan beri tahu manajer Anda.

Jangan panik atau membiarkan orang lain menyerbu Anda; konsentrasi untuk menghindari melakukan kesalahan yang ceroboh.

Saat menghentikan serangan yang sedang berlangsung, cabut sistem dari jaringan; jangan melakukan reboot atau mematikan sistem.

Catat dengan cermat untuk melacak apa yang Anda amati, kapan, dan dalam keadaan apa.

Pemeriksaan Sistem Awal Windows

Lihat event logs	`eventvwr`
Memeriksa konfigurasi jaringan	`arp -a`, `netstat -nr`
Daftar koneksi jaringan dan detail terkait	`netstat -nao`, `netstat -vb`, `net session`, `net use`
Daftar pengguna dan grup	`lusrmgr`, `net users`, `net localgroup administrators`, `net group administrators`
Melihat aktivitas terjadwal	`schtasks`
Melihat program yang auto-start	`msconfig`
Daftar proses	`taskmgr`, `wmic process list full`
Daftar layanan (*service*)	`net start`, `tasklist /svc`
Memeriksa pengaturan DNS dan file *host*	`ipconfig /all`, `ipconfig /displaydns`, `more %SystemRoot%\System32\Drivers\etc\hosts`
Periksa integritas dari file OS (mempengaruhi banyak file!)	`sigverif`
Teliti file yang terakhir dimodifikasi (mempengaruhi banyak file!)	`dir /a/o-d/p %SystemRoot%\System32`

Hindari menggunakan Windows Explorer, karena dapat memodifikasi detail sistem file yang berguna; gunakan Command Prompt atau Windows Powershell.

Pemeriksaan Sistem Awal Unix

Lihat pada file *event log* di direktori (lokasi bervariasi)	`/var/log`, `/var/adm`, `/var/spool`
Daftar *security event*	`wtmp`, `who`, `last`, `lastlog`
Periksa konfigurasi jaringan	`arp -an`, `route print`
Daftar koneksi jaringan dan detail terkait	`netstat -nap` (Linux), `netstat -na` (Solaris), `lsof -i`
Daftar pengguna	`more /etc/passwd`
Lihat aktivitas terjadwal	`more /etc/crontab`, `ls /etc/cron.*`, `ls /var/at/jobs`
Periksa pengaturan DNS dan file *host*	`more /etc/resolv.conf`, `more /etc/hosts`
Verifikasi integritas paket yang di-*install* (mempengaruhi banyak file!)	`rpm -Va` (Linux), `pkgchk` (Solaris)
Melihat layanan auto-start	`chkconfig --list` (Linux), `ls /etc/rc*.d` (Solaris), `smf` (Solaris 10+)
Daftar proses	`ps aux` (Linux, BSD), `ps -ef` (Solaris), `lsof +L1`
Menemukan file yang terakhir dimodifikasi (mempengaruhi banyak file!)	`ls -lat /`, `find / -mtime -2d -ls`

Komunikasi Insiden Respon

Jangan berbagi detail insiden dengan orang-orang di luar tim respon insiden (CSIRT).

Hindari mengirim data sensitif melalui email atau instant messenger tanpa enkripsi.

Jika Anda mencurigai jaringan telah terkompromi, komunikasikan menggunakan jalur lain, misalnya telepon non-VoIP.

Kunci Utama pada Tahapan Respon Insiden

1. Persiapan: Kumpulkan dan pelajari alat-alat yang diperlukan, kenali lingkungan Anda.
2. Identifikasi: Mendeteksi insiden, menentukan cakupannya, dan melibatkan pihak yang sesuai.
3. Penahanan: Menahan insiden untuk meminimalkan dampaknya pada sumber daya TI yang terkait.
4. Penghapusan: Hapus artifak yang terkompromi, jika diperlukan, sebagai proses menuju tahap pemulihan.
5. Pemulihan: Kembalikan sistem ke operasi normal, mungkin melalui *install* ulang atau *backup*.
6. Rangkuman: Dokumentasikan detail kejadian, kumpulkan data, dan bahas *lesson learned* insiden.

Authored by Lenny Zeltser, who leads a security consulting team at SAVVIS, and teaches malware analysis at SANS Institute. Special thanks for feedback to Lorna Hutcheson, Patrick Nolan, Raul Siles, Ed Skoudis, Donald Smith, Koon Yaw Tan, Gerard White, and Bojan Zdrnja.