UNIVERSITAS TEUKU UMAR
PROSEDUR OPERASIONAL

Prosedur : Keamanan dan Pengamanan Jaringan dan Server pada UPT. TIK UTU	No. Dokumen :	Tanggal terbit :	Revisi :

1. **TUJUAN**
Prosedur ini dibuat sebagai pedoman dalam menjaga jaringan dan server dari gangguan baik dari internal maupun eksternal

2. RUANG LINGKUP
Prosedur ini mencakup kegiatan Perlindungan jaringan dan server dari gangguan baik dari internal maupun ekseternal dalam bentuk gangguan terhadap perangkat keras dan perangkat lunak melalui proses investigasi dan pemeriksaan rutin

3. ISTILAH
- Intruder/intrusion
- Hacking
- Attacking
- Network Trouble
- DOS/DDOS
- Reconnaissance Activity
- Unautorized Access
- Pemeriksaan Rutin
- Password
- Temuan admin jaringan/server
- Laporan user tentang kondisi fisik dan system yang berisi bentuk malfunction/malcondition dari system
- Troubleshooting

4. TANGGUNG JAWAB
Dilakukan sepenuhnya oleh Admin Jaringan dan Server/Admin security

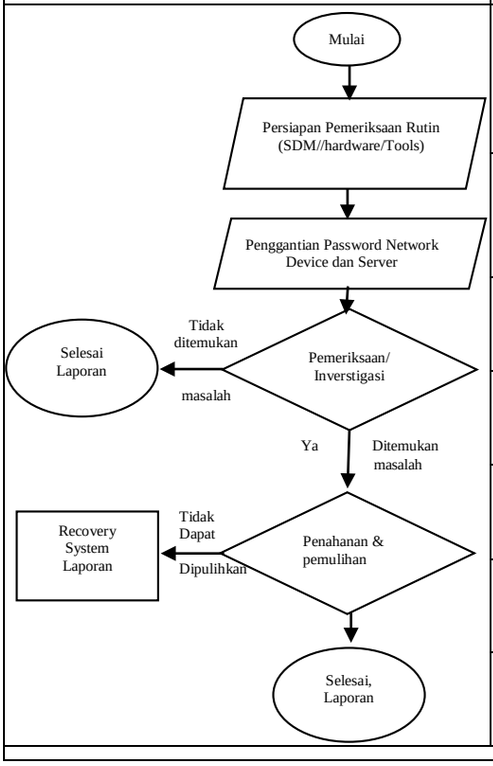
5. LAMPIRAN
Laporan Temuan/hasil investigasi admin jaringan/server dan Laporan hasil Pemulihan/

6. PERUBAHAN DOKUMEN TANGGUNG JAWAB
- Nama Dokumen : PROSEDUR PENGAMANAN JARINGAN dan SERVER
- Nomor Dokumen :

No. Rev	TGL. Rev	URAIAN GANGGUAN	DIPERIKSA	HASIL	TINDAK LANJUT

No. Rev	TGL Rev	PEMERIKSAAN RUTIN	DIPERIKSA	HASIL	TINDAK LANJUT

7. FLOWCHART Pemeriksaan Rutin Jaringan dan Server LPTIK Universitas Teuku Umar



Proses	PIC	Detail Proses	Waktu	Dokumen
	Admin/Security Admin server dan jaringan	Persiapan pemeriksaan rutin	15 menit	Form pemeriksaan rutin
	Admin/Security Admin server dan jaringan	Penggantian password network device dan server	15 menit	Form pemeriksaan rutin
	Admin/Security Admin server dan jaringan	Melakukan pemeriksaan rutin menggunakan tools yang terkait	45 menit	Form pemeriksaan rutin
	Admin/Security Admin server dan jaringan	Jika tidak ditemukan masalah, laporan	5 menit	Form pemeriksaan rutin, Laporan
	Admin/Security Admin server dan jaringan	Jika Ya, ditemukan masalah, lakukan penahanan, ereadikasi dan pemulihan	60 menit	Form pemeriksaan rutin
	Admin/Security Admin server dan jaringan	Jika tidak dapat dipulihkan lakukan recovery system	30 menit	Form pemeriksaan rutin
	Admin/Security Admin server dan jaringan	Jika dapat dipulihkan, laporan	5 menit	Form pemeriksaan rutin, Laporan

8. URAIAN TAMBAHAN

Pekerjaan yang dikelola oleh Petugas (admin) yang ditunjuk pada UPT. Teknologi Informasi dan Komunikasi Universitas Teuku Umar

Pmeriksaan rutin dilakukan sedikitnya 1 bulan 1 kali
Persiapan meliputi :

1. Persiapan SDM
2. Persiapan teknologi/tools (virus removal, network packet analyzer, system exploit)
3. Persiapan dokumen daftar dari alamat IP yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan insiden dan menyiapkan dokumen topologi jaringan, termasuk semua alamat IP yang paling up to date.
4. Persiapan komponen keamanan (Anti Malware, Firewall, IDS/IPS

Pemeriksaan rutin dan inverstigasi gangguan dilakukan terhadap :

1. Denial of Service
   - *Single or distributed (DoS or DDoS)*
   - *Inbound or outbound*
2. Reconnaissance activity
   - *Port scanning*
   - *Network vulnerability scanning*
   - *Unauthorized network monitoring*
3. Unauthorized access
   - *Unauthorized access to network*
   - *Inappropriate Usage*

Langkah-langkah yang bisa diambil pada tahap ini adalah :

1. Menentukan apakah jaringan organisasi merupakan target utama atau korban dari imbas, berdasarkan indikasi-indikasi :
   - Melambatnya lalu-lintas jaringan
   - Melambatnya proses pada komputer client
   - Penggunaan ruang disk yang bertambah
   - Waktu login yang lama, bahkan ditolak
   - Perubahan pada beberapa password
   - Log penuh
   - Anomali pada fungsi port
2. Memahami aliran logis dari serangan
3. Menentukan jenis lalu lintas yang sedang digunakan, seperti alamat IP, port dan protokol
4. Mempertimbangkan untuk menggunakan alat analisis jaringan untuk menentukan jenis lalu lintas yang digunakan dalam serangan itu (misalnya, n m a p , tcpdump, wireshark, Snort).
5. Me-*review* log yang tersedia untuk memahami serangan dan apa yang menjadi sasaran.
6. Memberitahu personil yang tepat, ini mungkin termasuk manajemen senior dan tim hukum
7. Mengidentifikasi aset dan layanan pada jaringan yang masih dapat diberikan oleh organisasi.
8. Mengidentifikasi apakah seluruh perangkat lunak selalu up to date dengan patch terbaru.
9. Apakah pada jaringan menjalankan layanan yang tidak perlu seperti Telnet atau FTP.
10. Menonaktifkan semua lalu lintas yang jelas palsu (misalnya, alamat IP internal yang seharusnya tidak boleh masuk atau keluar dari)
11. Menetapkan prosedur tentang cara untuk memisahkan jaringan yang satu dengan jaringan yang lain apabila terjadi serangan pada suatu jaringan. Sementara, menggunakan perangkat jaringan yang ada, seperti router dan switch terkelola untuk mempertahankan terhadap serangan jaringan. Sedapat mungkin menerapkan penyaringan layanan pada router terluar untuk mengurangi beban pada perangkat keamanan seperti firewall.
12. Menonaktifkan semua layanan yang tidak perlu dan membatasi akses ke dan dari semua host kritis, berdasarkan karakteristik lalu lintas jaringan normal.
13. Memahami perilaku "normal" dari lalu lintas jaringan, penggunaan CPU, sambungan dan penggunaan memori dari host dalam kondisi normal sehingga alat monitoring jaringan akan memicu peringatan pada perubahan abnormal.
14. Menentukan dampak dari tingkat keparahan yang terjadi

Penahanan

a. Tidak melakukan perubahan/modifikasi pada sistem
b. Menghubungi ISP untuk meminta penerapan penyaringan.
c. Jika memungkinkan, memblokir lalu lintas yang dekat dengan cloud jaringan (router, firewall, load balancer, dll).
d. Merelokasi target ke alamat IP lain jika suatu host tertentu sedang ditargetkan. Ini adalah solusi sementara.
e. Jika aplikasi tertentu sedang ditargetkan, pertimbangkan untuk menonaktifkan sementara.
f. Mengidentifikasi dan memperbaiki kerentanan atau kelemahan yang tereksploitasi. Sebagai contoh, misalnya layanan tidak terpakai yang sengaja diaktifkan dan tertinggal pada perangkat untuk melayani publik atau sistem operasi yang tidak dipatched.
g. Melakukan penyaringan berdasarkan karakteristik serangan, salah satu contohnya adalah memblokir paket echo ICMP.
h. Menerapkan rate limiting untuk protokol tertentu, mengijinkan dan membatasi jumlah paket per detik untuk protokol tertentu mengakses suatu host.
i. Mengidentifikasi lokasi dan/atau pemilik sistem yang terlibat dalam insiden tersebut dengan memeriksa hal-hal berikut:

- Tabel ARP jaringan untuk memetakan alamat IP ke alamat MAC
- Catatan log DHCP untuk alamat MAC dan hostname
- Perintah "nbtscan" untuk query informasi pada master NetBIOS
- Sistem kontrol jaringan untuk semua komputer yang digunakan
- Perangkat lunak manajemen jaringan (radius)
- Sistem manajemen log file (misal 'Qradar')

j. Menentukan apakah komputer yang telah diblokir masih memiliki akses jaringan. Jika demikian, hal ini dapat dicapai dalam beberapa cara oleh tim jaringan:
   - Pemeriksaan pada port switch , interface router , perimeter jaringan
   - Memblokir alamat MAC pada semua jaringan nirkabel
   - Menonaktifkan akses dial-up modem
   - Nonaktifkan akses VPN

k. Daftar komputer yang telah diblokir harus diumumkan ke semua anggota organisasi. Prosedur untuk memblokir/membuka blokir komputer yang telah terserang harus tersedia.Sebuah alternatif untuk memblokir semua akses jaringan, jika tersedia bisa berfungsi untuk menempatkan komputer dalam jaringan yang dikarantina.

l. Mungkin ada kasus ketika sebuah protokol (TCP/UDP) atau port tertentu perlu diblokir pada perimeter jaringan beberapa antarmuka jaringan lainnya untuk mencegah penyebaran.

m. Memberi tahu kepada administrator sistem dan/atau pengguna yang bertanggung jawab atas sistem.

n. Mengisolasi komputer yang terkena dampak, baik dengan cara mencabut kabel jaringan (lebih disukai) atau mematikan komputer. Mencabut kabel jaringan dan membiarkan komputer masih nyala, merupakan cara yang terbaik karena dengan cara shutdown dapat mengubah atau menghancurkan bukti, seperti infeksi malware pada memori. Bisa dilakukan (mematikan komputer) apabila memory telah dicopy untuk proses forensic (optional).

o. Melakukan analisa digital forensik

Eradikasi

Tahap eradication merupakan tahap untuk melakukan analisa lebih dalam terhadap barang bukti yang telah ditahan, pada tahap ini dilakukan proses analisa terhadap beberapa log file yang terdapat pada server, peralatan aktif jaringan, IDS, Firewall, sistem file, dan aplikasi. Pada tahap ini dilakukan analisa forensik dari barang bukti

Pemulihan

Memulihkan system menggunakan back-up system yang tersedia

PENGESAHAN			
	DISUSUN OLEH	**DIPERIKSA OLEH**	**DISAHKAN OLEH**
TANGGAL			
NAMA			
.JABATAN			
TANDA TANGAN			
NIP.			