UTS Cyber Security

1. Program yang dibuat khusus untuk melakukan hal-hal tertentu tanpa sepengetahuan pengguna disebut sebagai ...

a. Virus

b. Ransome Ware

c. Trojan

d. Malicious Code

e. Bloat Ware

2. Sebuah aturan yang menitikberatkan pada proses pengecekan keabsahan dan keaslian terhadap informasi, sumber maupun tujuan termasuk dalam aspek ...

a. Confidentiality

b. Authenticity

c. Integrity

d. Non-Repudiation

e. Availability

3. Orang yang tidak memiliki otoritas tidak hanya dapat mengakses tapi juga mengubah ataupun merusak sumber daya. Tindakan mengubah isi pesan, atau mengacak program termasuk dalam kelompok ...

a. Intruder

b. Interruption

c. Modification

d. Fabrication

e. Interception

4. Yang termasuk ancaman fisik dari jaringan komputer adalah ...

a. Kerusakanpada sistem operasi ataupun program maupun aplikasi

b. Ancaman serangan Virus

c. Distributed Denial of Attack Service

d. Pencurian perangkat keras komputer ataupun jaringan

e. Pendekatan secara individu kepada target yang akan diserang

5. Sebuah program yang dapat menangkap data dari paket yang lewat di jaringan disebut ...

a. Packet Sniffer

b. Malicious Code

c. Rootkit

d. Remote Access Tools

e. Spoofing

6. Proses pengenalan peralatan, sistem operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer disebut ...

a. Enkripsi

b. Dekripsi

c. Accounting

d. Authorization

e. Authentication

7. Jaringan khusus yang bersifat private dengan memanfaatkan media jaringan yang bersifat publik (internet) untuk menghubungkan antara 2 titik atau lebih disebut ...

a. Samba

b. SSH

c. IPSec

d. VPN

e. MPLS

8. Sebuah sistem atau perangkat yang melakukan pengendalian dan pengamanan lalu lintas data maupun komunikasi di dalam jaringan sesuai dengan aturan yang telah ditentukan disebut ...

a. Router

c. Anti Virus

b. Application Management

d. Software Security

e. Firewall

9. Pintu masuk ke dalam sebuah sistem komputer (server) yang biasa digunakan untuk melayani layanan berbasis jaringan dikenal dengan istilah ...

a. Protocol

b. Port

c. Service

d. Back Door

e. SSH

10. Jenis serangan yang digunakan untuk membajiri trafik server dengan menggunakan banyak komputer atau yang biasa disebut sebagai komputer zombie adalah ...

a. Spoofing

b. Sniffing

c. Brute Force

d. DoS

e. Phising

11. Tools yang dapat digunakan untuk melakukan scanning status port pada sebuah sistem komputer yaitu …

a. Brutus

b. Wireshark

c. TCPDump

d. Burp Suite

e. NMAP

12. Teknik serangan yang memanfaatkan celah keamanan pada sebuah aplikasi untuk menyerang sistem informasi lain yang berada di dalam satu sistem komputer (server) dikenal dengan istilah ...

a. Injection

b. XSS

c. Brute Force

d. Buffer Overflow

e. Defacing

13. Sistem yang digunakan untuk membantu melakukan antisipasi dengan melakukan deteksi awal terhadap paket-paket yang ditransmisikan melalui jaringan dan dapat memberikan peringatan bila ada aktifitas yang tidak wajar disebut ...

a. IDS

b. IPS

c. Firewall

d. DVWA

e. Honeypot

14. Berikut yang bukan merupakan motif penyerang melakukan penyerangan terhadap sebuah sistem, yaitu ...

a. Kriminal

c. Terorisme

d. Hardening

e. Patriotisme

b. Spionase

15. Berikut ini adalah merupakan serangan yang bukan termasuk dalam kelompok Denial of Service yaitu ...

a. Smurf Attack

b. Ping of Death

c. Amplification

d. ARP Poisoning

e. Slowloris

Aspek Keamanan

- Confidentiality (kerahasiaan)
  Proteksi untuk mencegah penggunaan tanpa izin terhadap sebuah informasi yang bersifat penting atau rahasia.
- Integrity (integritas)
  Deteksi terhadap terjaganya akurasi dan lengkapnya sebuah informasi.
- Availability (ketersediaan)
  Kontrol terhadap pengguna yang benar-benar sah dan tepat untuk mendapatkan informasi secara tepat waktu.

Model Penyerangan

- Interruption
  Penyerang melumpuhkan sistem atau ketersediaan layanan.
- Interception
  Penyerang mencuri data yang bersifat pribadi atau rahasia.
- Modification
  Penyerang mengubah informasi selama perpindahan atau penyimpanan, seperti memodifikasi pesan email atau mengubah jumlah uang dalam transaksi keuangan.
- Fabrication
  Penyerang membuat atau mengirimkan data palsu ke dalam sistem atau pengguna untuk medapatkan keuntungan.

Metodologi Penyerangan (Hacking)

1. Footprinting
   Penyerang mencoba mengumpulkan informasi mengenai lingkungan jaringan tertentu dari suatu target.
2. Scanning
   Penyerang melakukan pemindaian jaringan untuk mengidentifikasi sumber daya yang aktif, port yang terbuka, layanan yang berjalan, dan kerentanan potensial.
3. Enumeration
   Penyerang mencoba mengumpulkan informasi penting tentang sistem target yang dapat digunakan untuk merencanakan serangan lebih lanjut.
4. Gaining Access
   Penyerang berhasil mendapatkan akses secara tidak sah ke sistem target dengan melakukan eksploitasi kerentanan, penyusupan, dan teknik lainnya.
5. Escalating Privilage
   Setelah medapatkan hak akses, penyerang berusaha meningkatkan hak akses dalam sistem target dengan mengambil alih akun administrator.
6. Pilfering
   Penyerang mengambil data berharga dari sistem target yang bersifat penting dan rahasia.
7. Covering Tracks
   Setelah melakukan penyerangan, penyerang menghilangkan jejak dengan menghapus segala jenis aktivitas penyerangan.

8. Creating Back Door
   Penyerang membuat jalur pintu belakang agar mereka kemudian dapat dengan bebas masuk ke dalam sistem tanpa harus melakukan langkah penyerangan dari awal.
9. Denial of Service
   Penyerang membanjiri server atau jaringan dengan tujuan untuk melumpuhkan sistem.