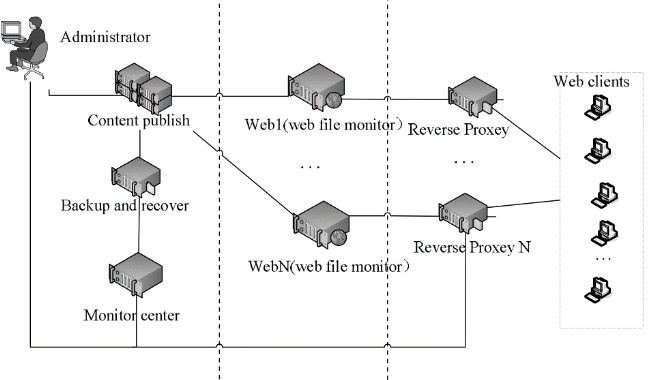
1. Jelaskan perbedaan model keamanan antara protokol SSH dan FTP melalui data dari hasil capture wireshark? sample capture : <https://wiki.wireshark.org/SampleCaptures>

JAWAB :

1. Protokol SSH : merupakan jaringan koneksi yang aman, jika Anda menggunakan jaringan ini maka akan memiliki pilihan untuk dalam melakukan autentikasi dari pengguna remote sebelum terkoneksi jaringan. Sistem ini juga mampu mengirimkan input dari SSH client kepada host atau server pusat, lalu mengirim kembali hasil ke server client.



1. File Transfer Protocol (FTP) adalah protokol jaringan standar yang digunakan untuk mentransfer file komputer antara klien dan server di jaringan komputer. FTP dibangun di atas arsitektur model klien-server menggunakan kontrol terpisah dan koneksi data antara klien dan server. Dengan menggunakan FTP maka user dapat mengirim dan mengunduh file.
2. Jelaskan beberapa istilah berikut:

**A. Bugs**

**B. Vulnerability**

**C. Sniffing**

**D. IDS/IPS**

**E. Penetration Testing**

JAWAB :

1. **Bugs**

bug merupakan error yang terjadi pada source code yang mengakibatkan output menjadi tidak sesuai dengan yang telah direncanakan.

1. **Vulnerability**

Suatu cacat pada system/infrastruktur yang memungkinkan terjadinya akses tanpa izin dengan meng exploitasi kecacatan sistem.Cacat ini terjadi akibat kesalahan dalam merancang,membuat atau mengimplementasikan sebuah sistem.

1. **Sniffing**

Tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi sensitive secara illegal. Cara kerja sniffing adalah ketika Anda terhubung ke jaringan yang bersifat public, saat Anda melakukan proses transfer data dari client server dan sebaliknya. Karena data yang mengalir pada client dan server yang bersifat bolak-balik, sniffing ini akan menangkap paket-paket yang dikirimkan dengan cara illegal menggunakan tools pembantu.

1. **IDS/IPS**

IDS (Intrution Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap lalulintas (traffic) jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan.

IPS (Intrusion Prevention System) adalah sebuah sistem yang menggabungkan fungsi firewall dan fungsi IDS dengan proporsional.

1. **Penetration Testing**

Suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi / perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut penetration tester (disingkat pentester). Penetration Testing mempunyai standar resmi sebagai acuan dalam pelaksanaannya. Standar ini bisa dilihat di pentest-standard.org.

1. Enkripsi lah dengan caesar cipher, shift code: 10, untuk kata (sesuaikan dengan nama dan nim masing2) : NIM Nama Lengkap → contoh : 88991001 Agung Nugroho (enkripsi kata2 tersebut). Sertakan langkah-langkah ekripsinya.

JAWAB :

155410042 Bsjkv Jkbnobi Zbklkgk Zedbk

1. Decrypt encrypt text berikut, tuliskan algoritma yang digunakan :

a. 76c0bdd75a03ba69adb38bdb31d47ae5a7d41f37

b. satgdv gmago-phzxq muru, vmdmwtgrd lzzdmghdrr gj, iquwq rvsuxaq xvunronwiy. key: jagadiri

c. YWtha29tOmxpYnVyaXR1YmVsYWphcmRpcnVtYWg=

JAWAB:

1. NqCnb5nsfe8ktPF8GQR8G19+kFuaDSOYIEbpyguwxwfgu6QFLKKlIvNtYrkvsFbpbcdhTj+rSkN/BzFyPQAu6w==
2. vzAXbeiqBW9459ussuIz8jl7sWvQ/+mPoHoJaZb4Zb5oFFjGRCORYIe3INOxonDv6X+RrakwRXTf7LwRNWTZw7NUB21F4vDmTXwYQMNqW3AVrKTw3AVICDQPX6rulApG
3. 7supwhLh3eCcIuvR6njcD40A7fzu4Dmaa5TYNyzvCoVA/pJS5EcghFj+CBUxiKA9GblUZaVP1b6nB/UfIStliw==