Prova de coneixements sobre ciberseguretat

Aquesta prova no compta per l'avaluació, però heu de respondre sense fer trampa ni consultar Internet ;-)

1. A què es corresponen les sigles AES? De què tracta, aquesta tecnologia?
AES és l'acrònim de Advanced Encryption Standard. Permet el xifratge de bits d'informació tot agafant un bloc de 128 d'aquests bits i donant com a sortida un altre bloc de 128 bits, però xifrat en funció d'una clau. Aquesta clau es farà servir també per desxifrar.

2. Quin problema tenen les signatures digitals de 64 bits fetes fa 20 anys als documents electrònics?
Una manera de trencar la criptografia que protegeix la informació (com és el cas de les signatures digitals, que autentifiquen les dades que signen) és per mitjà dels atacs de força bruta: anar provant totes les possibles combinacions que es poden fer amb una clau. Fer un atac de força bruta amb 64 bits implica 2^{64} comprovacions. Fa 20 anys això trigaria molt temps, però amb la força computacional actual (incloent milers de màquines treballant en paral·lel) trencar-ho seria factible. Cal, doncs, tornar a signar els documents usant una criptografia que faci servir més bits.

3. A quina tecnologia correspon aquesta regla de configuració? Què fa?

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
```

Correspon a un tallafoc, concretament iptables. El que fa és acceptar totes aquelles connexions que entrin a la màquina (input) i que vagin dirigides al port 80 (habitualment on escolten els navegadors web).

4. A quina tecnologia correspon aquesta regla de configuració? Què fa?

```
alert tcp any any -> 192.168.1.10 80 (msg: "Connection attempt to web server";)
```

Correspon a un sensor de xarxa, anomenat Snort. Aquest és un component essencial dels IDS (sistemes de detecció d'intrusions). Avisarà cada cop que entri un paquet cap a la IP i ports especificats.

5. A què es corresponen les sigles PGP? De què tracta, aquesta tecnologia?

Pretty Good Privacy, privadesa prou bona. És un sistema de seguretat de la informació (xifratge i signatures) utilitzat en determinats àmbits.

6. Què permeten les eines Telnet i SSH? Quina diferència hi ha?
Les dues eines permeten connectar remotament a una màquina per mitjà d'un terminal. La diferència és que Telnet envia la informació tal i com la genera l'aplicació, mentre que SSH hi aplica xifratge i autentificació, cosa que va bé per evitar espionatge de dades.

7. Quina longitud té la clau *keystream* amb la qual es fa la XOR en el xifratge de flux?
El xifratge de flux implica que un bit del contingut a xifrar i un bit de la clau *keystream* s'uneixen amb la funció XOR. La propietat de simetria d'aquest sistema fa que una mateixa clau pugui servir per xifrar i desxifrar. Com que per cada bit de contingut cal un bit de la clau, aquesta ha de ser tan llarga com el contingut a xifrar! Per superar aquest problema, aquesta "clau de flux" es genera a partir d'un generador de números pseudoaleatori, el qual genera una seqüència de bits aparentment aleatòria (i per tant, segura i difícil d'endevinar), però de manera determinista i en funció d'una determinada "llavor" (que actua, al capdavall, de clau del sistema).

8. Quin problema suposa l'ús de HTTP en la validació d'usuaris en una xarxa social?
Doncs que les dades s'envien en clar, sense xifrar. Si fem servir HTTPS la cosa canvia.

9. Què és el *phishing*? I el *ransomware*?
El primer és el robatori de dades, en general credencials de comptes, de bancs, etc. Per mitjà de l'enginyeria social i el fet de respondre un correu fraudulent. El segon és la infecció d'un equip o dispositiu i el seu bloqueig, ... tot torna a la normalitat quan es paga un rescat a l'atacant, habitualment amb una criptomoneda.

10. Quin problema de seguretat pot suposar utilitzar *pendrives* en una empresa?
Poden ser l'origen d'una infecció i/o atac als equips de l'empresa.