1- (SDET) Usuários humanos (e administradores também) de um sistema operacional costumam ser os elos mais fracos na cadeia de segurança. Oual termo descreve as tentativas de coletar informações dos usuários por meio de e-mail enganoso, mensagens instantâneas ou mesmo mensagens enviadas a celulares por meio dos aplicativos de comunicação?

A) Pharming
B) Worm
C) Phishing
D) NFS

2- (SDET) No contexto de segurança, um dos princípios filosóficos mais básicos na segurança de informações é informalmente conhecido como a "tríade CIA/CID", assinale a alternativa correta referente à tal acrônimo

A) Confiabilidade, integridade e autenticidade
B) Confiabilidade, integridade e disponibilidade
C) Confiabilidade, indeterminação e delegação
D) Confidencialidade, integridade e disponibilidade.

3- (SDET) Os hackers mais astutos tentam esconder suas pegadas e evitar detecção. Frequentemente, eles esperam continuar utilizando o sistema que fora atacado para distribuir softwares ilegalmente, investigar outras redes, ou até mesmo lançar ataques contra outros sistemas. 0 programa malicioso que possui tais funções e metas são conhecidos como:

A) Trojan
B) DOS
C) Rootkits
D) Engenharia social

4-SDET) É um sistema que utiliza autenticação criptográfica para confirmar a identidade de um usuário e criptografa todo o fluxo de comunicações entre dois hosts. Marque a alternativa correta.

A) SSH
B) PGP
C) SMTP

D)HTTP

5- SDET) Bob deseja enviar uma mensagem secreta a Alice utilizando a criptografia de chave simétrica, Alice irá descriptografar a mensagem recebida de Bob utilizado a chave:

A) Protegida dada por bob
B) Pública de alice
C) Privada dada por bob
D) Particular dada por bob

6- (SDET) Neste método de criptografia, cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um “disfarce”, preservando a ordem dos símbolos no texto. Assinale a alternativa correta referente a esse modo.

A) Cifras de transposição
B) Cifras de substituição
C) Cifra de chave pública
D) Cifra de chave secreta

7-SDET) A autenticidade de muitos documentos legais, financeiros e outros tipos é determinada pela presença de uma assinatura manual autorizada. Para que o sistema de mensagens computadorizadas possa substituir o transporte físico de documentos em papel e tinta, fora encontrada um método que permite assinar os documentos de modo que não possa ser forjado, tal método é conhecido como:

A) Assinatura digital
B) Hash
C) Assinatura de cartório
D) Assinatura unidimensional

8- (SDET) É uma parte da rede que se encontra fora do perímetro de segurança, também conhecida como *zona desmilitarizada.* Assinale a alternativa correta referente à tal conceito.

A)Dos
B)VPN
C)DNS

D)DMZ

9- (SDET) Neste tipo de ataque, o atacante utiliza apenas uma máquina e envia milhares de solicitações de conexão no intuito de tirar do ar um site, servidor ou até mesmo uma rede. Assinale a alternativa correta referente ao conceito.

A) DoS
B) DDoS
C) DMZ
D) DDDoS

10- (SDET) Neste tipo de ataque, o atacante utiliza centenas de máquinas infectadas espalhadas pelo mundo e envia milhares de solicitações de conexão no intuito de tirar do ar um site, servidor ou até mesmo uma rede. Assinale a alternativa correta referente ao conceito.

A) Dos
B) DDos
C) DMZ
D) TROJAN INJECTER

11- (SDET) Assinale a alternativa que NÃO REPRESENTE um tipo de golpe aplicado na Internet.

A) Boato (hoax)
B) E-mail spoofing
C) Pharming
D) Phishing

12. Tem como objetivo enganar um servidor DNS fazendo- o instalar um falso endereço IP é uma ação chamada:

A) Boato(hoax)
B) E-mail spoofing

C) Pharming

D) Phishing

13- (SDET) É um programa que combina as características de trojan e backdoor, já que permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário:

A) Rootkit
B) Botnet
C) RAT
D) Ransomware

14- No contexto de segurança da informação, cavalo de troia, trojan ou *trojan-horse,* é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário; existem diversos tipos de trojan, correlacione as colunas abaixo com seus respectivos conceitos e marque a alternativa com a sequência correta.

( )Altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

( )Redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

( )Instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.

( )Instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

( ) Coleta dados bancários dos usuários, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados.

Tipos de trojan:
1- Proxy
2- Banker

3- Spy
4- Destrutivo
5- Clicker

A) 4-1-5-3-2
B) 1-4-3-2-5,
C) 3-4-2-1-5
D) 4-5-1-3-2

15- Um certificado emitido sob um processo mais rigoroso de validação do solicitante é conhecido como:

A) Certificado Auto assinado
B) Certificado EV SSL
C) Certificado TCP
D) Autoridade certificadora

16- No contexto de segurança da informação sobre o uso segura da Internet, um usuário ao navegar pela Web pode se deparar com diversos tipos de conexão, sobre tais tipos, correlacione as colunas com seus respectivos conceitos e marque a alternativa com sequência correta.

( ) É a que deve ser utilizada quando dados sensíveis são transmitidos, geralmente usada para acesso a sites de Internet Banking e de comércio eletrônico. Provê autenticação, integridade de confidencialidade.
( ) É usada na maioria dos acessos realizados a sites. Não provê requisitos de segurança.
( ) Provê um maior grau de confiabilidade quanto à identidade do site e de seu dono, pois utiliza um certo certificado para dar mais segurança.

1- Padrão
2- Segura
3- Segura com EV SSL

A) 3-1-2
B) 1-2-3
C) 2-1-3
D) 3-2-1

17- É um tipo de protocolo que permite a sincronização dos relógios dos dispositivos de uma rede, como servidores, estações de trabalho, roteadores e outros equipamentos, a partir de referências de tempo confiáveis. Assinale a alternativa que corresponda à tal protocolo.

A)Network Time Protocol (NTP)
B)Network Time Control Protocol (NTCP)
C)Simple Method Time Protocol (SMTP)
D)Network Synchronization Time Protocol (NSTP)

18- (SDET) Assinale a alternativa referente ao programa, ou o conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

A) Hoax
B) WPS
C) IDS
D) IPS

19-(SDET) No contexto de segurança de redes, quando um atacante introduz ou substitui um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, assim permitindo a captura de senhas de acesso e informações que possam trafegar por tal dispositivo é conhecido como ataque de:

A) Força Bruta

B) Negação de Serviço

C) Personificação

D) Interceptação de Tráfego

20- O Método criptográfico que gera um resultado único, independente do tamanho da informação de entrada, é conhecido como função de resumo. Assinale a alternativa que nomeia o resultado desse método.

A) Hash

B) IPsec

C) MMU

D) Locking

21) Dentre as alternativas abaixo, no contexto de segurança da informação, assinale a que representa corretamente um método hash.

A) RC4
B) RSA
C) SSL
D) MD5

22- Assinale a alternativa que corresponda a um método criptográfico de chave simétrica.,

A) Rsa

B) Rc4

C) Ecc

D) Das

23- Sabemos que, no contexto de segurança da informação, temos que guardar nossas senhas a todo custo, não facilitando e nem deixando brechas durante a sua criação, uma boa senha é aquela que é difícil de ser descoberta, analise as alternativas abaixo e marque a que NÃO REPRESENTE um elemento que deverá ser usado durante a elaboração de senhas.

A)Números aleatórios
B)Grande quantidade de caracteres
C)Substituição de caracteres

D)Número de telefone

24) É uma técnica utilizada por *spammers* que consiste em coletar endereços de e-mail por meio de varreduras em páginas Web e arquivos de listas de discussão.Assinale a alternativa correta.

A) Malvertising
B) Harvesting
C) SPAM
D) Pharming

25) *"Ransomware: uma empresa sofre o segundo ataque de ransomware no Brasil."*

→ O ataque hacker mencionado acima é um programa malicioso que tem como característica:
Assinale a alternativa correta.

A)Executar as funções para as quais foi aparentemente projetado, mas também executar outras funções, normalmente maliciosas e sem o conhecimento do usuário.
B)Propagar-se inserindo cópias de si mesmo e se tornar parte de outros programas e arquivos.
C)Tornar inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e exigindo pagamento de resgate para restabelecer o acesso ao usuário.
D)Permitir o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

26 - Um tipo de ataque que envolve personagens, tais como, Master (máquina que recebe os parâmetros para o ataque e comanda os agentes) e Agentes (máquinas que efetivamente concretizam o ataque contra uma ou mais vítimas), que inundam os servidores alvo com um volume enorme de pacotes é denominado

A) Flooding.
B) DDoS.
C) Buffer Overflow.
D) Spoofing.
E) Sniffers.

27) Uma ferramenta utilizada por hackers para capturar dados digitados pelas vítimas é um software analisador de tráfego, que inspeciona pacotes de dados que circulam pela rede e extrai informações deles.
Esse programa é conhecido por:

A) Keylogger
B) Sniffer
C) Cookie
D) Spoofing
E) Phishing

28) Sobre DDoS, assinale a alternativa correta.

A) É uma forma de ataque repetitivo a um determinado endereço, visando descobrir através de algoritmos o login e senha de um determinado serviço em um servidor em questão.

B) DDoS é quando temos um software intruso dentro de nosso servidor, esse software faz ataque a outros servidores sem nossa autorização.

C) Esse ataque é classificado quando um intruso tem sob seu comando centenas de computadores, e comanda um ataque ao mesmo alvo e ao mesmo instante.

D) DDoS é um protocolo responsável para envio e recebimento de e-mails.

E) DDoS é o nome dado ao Firewall mais utilizado em servidor Red Hat Enterprise Linux 6.

29- A respeito de segurança da informação, assinale a opção correta.

A)O Cavalo-de-troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.

B) A disponibilidade da informação é a garantia de que a informação não será alterada durante o trânsito entre o emissor e o receptor, além da garantia de que ela estará disponível para uso nesse trânsito.

C) O uso de um programa anti-spam garante que software invasor ou usuário mal-intencionado não acesse uma máquina conectada a uma rede.

D) A criptografia é uma das formas de garantir que a informação fique em uma área fora da rede, cujos dados somente são acessados, fisicamente, por pessoas autorizadas.
E) Uma das formas de se garantir a segurança das informações de um website é não colocá-lo em rede, o que elimina a possibilidade de acesso por pessoas intrusas.

30- Analise os itens e aponte a opção incorreta:

I. Em segurança da informação, de acordo com o princípio da confidencialidade, somente o remetente e o destinatário pretendido podem entender o conteúdo da mensagem transmitida.

II. A integridade da mensagem é desejável em uma comunicação segura. Neste princípio, devemos garantir que o conteúdo de sua comunicação não seja alterado durante a transmissão.

III. Um dos princípios básicos da segurança da informação é a disponibilidade. Neste princípio, devemos garantir que os usuários são quem eles realmente dizem ser.

IV. Em criptografia, a função de uma chave criptográfica é personalizar o processo de criptografia, uma vez que o processo a ser realizado utilizará a combinação do algoritmo desejado com a chave informada pelo usuário.

A) I e III, somente;
B) II, somente;
C) II e III, somente;
D) III somente;
E) IV, somente.