

Aula 05

*TJ-PR (Técnico Judiciário) Passo
Estratégico de Informática - 2025
(Pós-Edital)*

Autor:
Diego Carvalho

20 de Agosto de 2025

Índice

1) O que é mais cobrado no assunto - Malwares - AOCP	3
2) Roteiro de Revisão - Malwares	4
3) Aposta Estratégica - Malwares	11
4) Questões Estratégicas - Malwares - AOCP	13
5) Questionário de Revisão - Malwares	18
6) Lista de Questões Estratégicas - Malwares - AOCP	26
7) Gabarito de Questões Estratégicas - Malwares - AOCP	28
8) Referências Bibliográficas - Malwares	29



O QUE É MAIS COBRADO DENTRO DO ASSUNTO?

A análise estatística refere-se ao período de 2021 a 2025, abrangendo provas realizadas pela banca organizadora do concurso de níveis médio e superior (em informática, não há diferenciação do nível de questões). Por fim, quando não há quantidade razoável de questões para analisar, nós consideramos percentuais de incidências de bancas similares.

TÓPICO	% DE COBRANÇA [AACP]
Vírus	43%
Spyware	10%
Ransomware	08%
Worm	08%
Trojan Horse	06%
Phishing Scam	05%
Adwares	05%
Backdoor	04%
Rootkit	03%
Engenharia Social	02%
Bot e Botnet	01%
Conceitos Básicos	<1%
Keyloggers	<1%
Screenloggers	<1%
Sniffer	<1%
Bombas Lógicas	<1%
Exploits	<1%
Hijacker	<1%
Força Bruta	<1%
Denial of Service (DoS)	<1%
IP Spoofing	<1%
E-Mail Spoofing	<1%
Smishing	<1%
Pharming	<1%
Hoax	<1%
Man in the Middle	<1%
Defacement	<1%
SQL Injection	<1%
Furto de Identidade	<1%
Fraude de Antecipação de Recursos	<1%



ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

MALWARES

Códigos maliciosos (Malwares, do inglês Malicious Softwares) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Malwares (Malicious Softwares) - também chamados de Softwares Maliciosos ou Pragas Virtuais - são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Eles são inseridos intencionalmente em um sistema computacional com um propósito prejudicial. Algumas das formas como eles podem infectar ou comprometer um computador são:

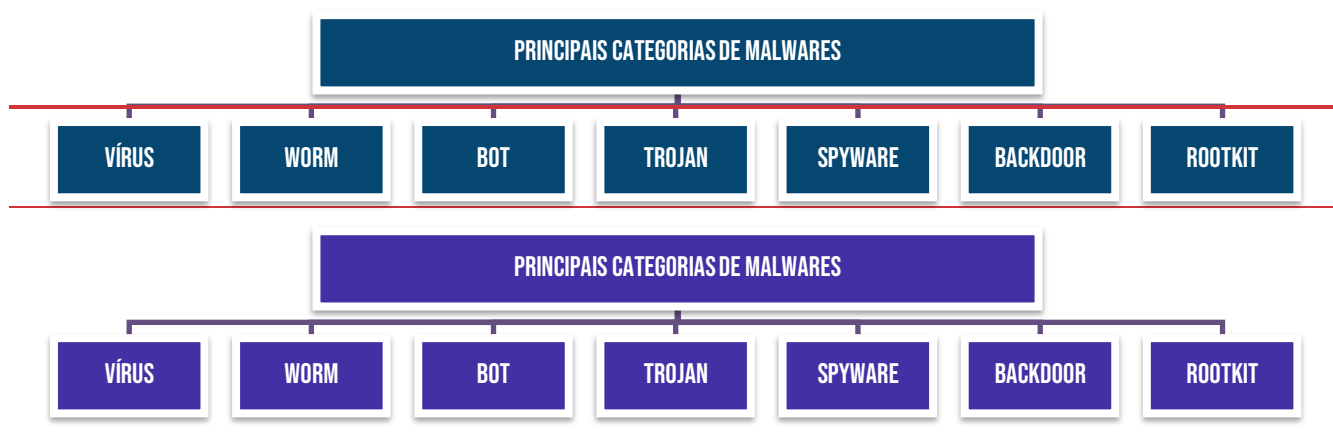
FORMAS COMUNS DE INFECÇÃO DE MALWARES

Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;

Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.

Os códigos maliciosos são muitas vezes utilizados como intermediários e possibilitam a prática de golpes virtuais, a realização de ataques e a disseminação de spam (mensagens indesejadas). Em suma: o termo malware abrange qualquer tipo de software indesejado, instalado sem o devido consentimento no computador do usuário. As principais categorias de malware são: Vírus, Worm, Bot, Trojan, Spyware, Backdoor e Rootkit.



Agora vamos falar rapidamente sobre diversos tipos de malwares, começando pelos mais famosos: **vírus de computador**.



DEFINIÇÃO DE VÍRUS

Programa ou parte de um programa, normalmente malicioso, que se propaga infectando, inserindo cópias de si mesmo, anexando-se ou hospedando-se em arquivos ou programas existentes na máquina.

Um vírus é composto basicamente de três partes: **um mecanismo de infecção**, **um mecanismo de ativação** e **uma carga útil**. Vejamos como essas partes são definidas:

COMPOSIÇÃO DE UM VÍRUS

MECANISMO DE INFECÇÃO	MECANISMO DE ATIVAÇÃO	CARGA ÚTIL
Meios ou formas pelas quais um vírus se propaga, habilitando-o a se reproduzir. É também conhecido como Vetor de Infecção.	Evento ou condição que determina quando a carga útil é ativada ou entregue. Às vezes, é conhecido como Bomba Lógica.	O que o vírus faz, além de se espalhar. A carga útil pode envolver algum dano ou atividade benigna, porém notável.

Existem diversos tipos de vírus de computador:

TIPOS DE VÍRUS	DESCRIÇÃO
VÍRUS DE SCRIPT	Escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.
VÍRUS DE MACRO	Tipo específico de vírus de script normalmente recebido ao acessar páginas web ou por e-mail e que tenta infectar arquivos manipulados por aplicativos que utilizam essas linguagens mencionadas anteriormente como os arquivos que compõe o Microsoft Office.
VÍRUS DE BOOT	Também conhecido como Vírus de Setor de Carga ou Vírus de Setor de Inicialização, ele é ativado quando o computador é ligado e é carregado na memória antes do sistema operacional.
VÍRUS DE ARQUIVO	Também conhecido como Vírus de Programa ou Parasitário, trata-se do vírus mais tradicional e comum. Ele infecta e causa danos ao se conectarem a arquivos executáveis (.exe, .com, .dll, etc), sobrescrevendo o código original e causando danos quase sempre irreparáveis.
VÍRUS POLIMÓRFICO	Também conhecido como Vírus Mutante, é capaz de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.
VÍRUS METAMÓRFICO	Trata-se de um vírus que se transforma a cada infecção, mas que - diferentemente do polimórfico - se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção.
VÍRUS STEALTH	Projetados explicitamente para não serem detectados pelo antivírus e têm a capacidade de se remover da memória temporariamente para evitar que o antivírus o detecte.
VÍRUS TIMEBOMB	Conhecido como Vírus Bomba Relógio, trata-se de um vírus que - após infectar a máquina - permanece latente (oculto), apenas se replicando, e seu código



malicioso é programado para ser ativado em um determinado momento específico, executando sua carga útil.

Agora vamos partir para outros tipos de malwares:

TIPOS DE MALWARES	DESCRIÇÃO
WORM	Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.
BOT	Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.
BOTNET	Rede formada por centenas ou milhares de computadores zumbis e que permitem potencializar as ações danosas executadas pelos bots.
CAVALO DE TROIA	O Trojan é um programa que age utilizando o princípio do Cavalo de Troia, em um arquivo é enviado se fazendo passar por um aplicativo útil, como um “presente de grego”, mas que na verdade possui funcionalidades maliciosas escondidas. Muitas vezes, o trojan abre portas de comunicação para que através da Internet a máquina possa ser invadida ou monitorada.
RANSOMWARE	Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate (Ransom, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.
SPYWARE	Software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.
KEYLOGGER	Trata-se de um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor.
SCREENLOGGER	Trata-se de um spyware – similar ao keylogger – capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.
ADWARE	Trata-se de um spyware projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas



	livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas são direcionadas.
SNIFFER	Um Sniffer é programa que age monitorando o tráfego na rede, através da captura de pacotes de dados, em busca de informações sensíveis como o endereço dos sites acessados, senhas de acesso, e-mails, etc.
BACKDOOR	Um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
ROOTKIT	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
BOMBAS LÓGICAS	Trata-se de um software malicioso normalmente instalado por um usuário autorizado, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento, como por exemplo o caso de ficar mais de 30 dias sem efetuar login.
EXPLOITS	Trata-se de um software criado por hackers para permitir explorar vulnerabilidades conhecidas de sistemas e assim permitir que iniciantes (Script Kiddies) possam praticar ações de invasões sem conhecimentos avançados.
HIJACKER	O Hijacker (sequestro, em inglês) é um software malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente, inserindo botões inadvertidamente.

TIPOS DE ATAQUES	DESCRIÇÃO
ENGENHARIA SOCIAL	Trata-se de uma técnica muito utilizada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.
FORÇA BRUTA	Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.
NEGAÇÃO DE SERVIÇO	Negação de serviço (Denial of Service - DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service - DDoS).
IP SPOOFING	O IP Spoofing (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada quando o mecanismo de autenticação de uma rede é



	baseado em endereços IP, isto é, quando a identificação de um usuário é realizada baseado em seu número de endereço IP.
E-MAIL SPOOFING	Técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Essa técnica é possível devido a características do protocolo SMTP (Simple Mail Transfer Protocol) que permitem que campos do cabeçalho sejam falsificados.
PHISHING SCAM	Fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de phishing é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou um arquivo malicioso.
PHARMING	Ataque que possui como estratégia corromper o DNS e direcionar o endereço de um site para um servidor diferente do original. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Nesse caso, quando o usuário tenta acessar um site legítimo, o navegador web é redirecionado, de forma transparente, para uma página falsa.
HOAX	Trata-se de uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.
MAN IN THE MIDDLE	Trata-se de um ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque, a comunicação é interceptada pelo atacante e retransmitida. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.
DEFACEMENT	Trata-se de uma técnica que consiste em alterar o conteúdo da página web. Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.
SQL INJECTION	Trata-se de uma vulnerabilidade de segurança que ocorre quando um invasor insere instruções SQL maliciosas em uma entrada de dados, como campos de formulário ou parâmetros de URL, com o objetivo de manipular o banco de dados subjacente. Essa técnica é amplamente explorada em sistemas que utilizam consultas SQL dinâmicas para interagir com um banco de dados.



RESUMO DE CÓDIGOS MALICIOSOS

	VÍRUS	WORM	BOT	TROJAN	SPYWARE	BACKDOOR	ROOTKIT
FORMA DE OBTENÇÃO							
RECEBIDO AUTOMATICAMENTE PELA REDE		X	X				
RECEBIDO POR E-MAIL	X	X	X	X	X		
BAIXADO DE SITES NA INTERNET	X	X	X	X	X		
COMPARTILHAMENTO DE ARQUIVOS	X	X	X	X	X		
USO DE MÍDIAS REMOVÍVEIS INFECTADAS	X	X	X	X	X		
REDES SOCIAIS	X	X	X	X	X		
MENSAGENS INSTANTÂNEAS	X	X	X	X	X		
INSERIDO POR UM INVASOR		X	X	X	X	X	X
AÇÃO DE OUTRO CÓDIGO MALICIOSO		X	X	X	X	X	X
FORMA DE INSTALAÇÃO							
EXECUÇÃO DE UM ARQUIVO INFECTADO	X						
EXECUÇÃO EXPLÍCITA DO CÓDIGO MALICIOSO		X	X	X	X		
VIA EXECUÇÃO DE OUTRO CÓDIGO MALICIOSO						X	X
EXPLORAÇÃO DE VULNERABILIDADES		X	X			X	X
FORMA DE PROPAGAÇÃO							
INSERE CÓPIA DE SI PRÓPRIO EM ARQUIVOS	X						
ENVIA CÓPIA DE SI PRÓPRIO AUTOMATICAMENTE PELA REDE		X	X				
ENVIA CÓPIA DE SI PRÓPRIO AUTOMATICAMENTE POR EMAIL		X	X				
NÃO SE PROPAGA				X	X	X	X
AÇÕES MALICIOSAS MAIS COMUNS							
ALTERA E/OU REMOVE ARQUIVOS	X			X			X
CONSUME GRANDE QUANTIDADE DE RECURSOS		X	X				
FURTA INFORMAÇÕES SENSÍVEIS			X	X	X		
INSTALA OUTROS CÓDIGOS MALICIOSOS		X	X	X			X
POSSIBILITA O RETORNO DO INVASOR						X	X
ENVIA SPAM E PHISHING			X				
DESFERE ATAQUES NA INTERNET		X	X				
PROCURA SE MANTER ESCONDIDO	X				X	X	X





APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais.

Eu listei abaixo o ponto com maior probabilidade de cobrança no contexto de **Softwares Maliciosos**. Estas são as minhas apostas:

TIPOS DE MALWARES	DESCRIÇÃO
WORM	Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.
CAVALO DE TROIA	O Trojan é um programa que age utilizando o princípio do Cavalo de Troia, em um arquivo é enviado se fazendo passar por um aplicativo útil, como um “presente de grego”, mas que na verdade possui funcionalidades maliciosas escondidas. Muitas vezes, o trojan abre portas de comunicação para que através da Internet a máquina possa ser invadida ou monitorada.
RANSOMWARE	Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate (Ransom, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.
SPYWARE	Software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.
BACKDOOR	Um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

TIPOS DE ATAQUES	DESCRIÇÃO
ENGENHARIA SOCIAL	Trata-se de uma técnica muito utilizada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.
FORÇA BRUTA	Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os



	mesmos privilégios deste usuário. Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.
NEGAÇÃO DE SERVIÇO	Negação de serviço (Denial of Service - DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service - DDoS).
PHISHING SCAM	Fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de phishing é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou um arquivo malicioso.



QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.

1. (AOCF / UFS - 2024) Malwares são programas maliciosos que podem assumir várias formas e realizar ações prejudiciais nos sistemas. Entre os diferentes tipos de malwares, o "vírus" é um dos mais conhecidos. Assinale a alternativa que apresenta a definição correta do malware "vírus".

- a) É um tipo de malware que se anexa a arquivos ou programas legítimos e se replica quando esses arquivos ou programas são executados.
- b) É um tipo de malware que se disfarça como software legítimo, mas realiza ações maliciosas sem o conhecimento do usuário.
- c) É um programa autônomo que se replica e se espalha para outros computadores em uma rede ou pela internet.
- d) É um malware que registra todas as teclas digitadas em um teclado, capturando informações confidenciais, como senhas e informações de cartão de crédito.
- e) Envolve a distribuição de malware por meio de anúncios maliciosos exibidos em sites legítimos.

Comentários:

- (a) Correto. Um vírus é um tipo de malware que se anexa a arquivos ou programas legítimos e se replica quando esses arquivos são executados pelo usuário. Ele pode causar danos ao sistema, como corrupção de arquivos e consumo de recursos;
- (b) Errado. A descrição corresponde a um Cavalo de Troia (Trojan), que se disfarça como software legítimo para enganar o usuário e realizar ações maliciosas;
- (c) Errado. A definição se aplica a um worm, que é um malware autônomo que se replica automaticamente sem a necessidade de um arquivo hospedeiro ou ação do usuário;



(d) Errado. Esse comportamento é típico de um keylogger, um tipo de malware usado para capturar dados digitados, como senhas e informações bancárias;

(e) Errado. Essa técnica é conhecida como malvertising, que utiliza anúncios maliciosos para distribuir malware, mas não é uma característica de vírus especificamente.

Gabarito: Letra A

2. (AOCF / IF-MA - 2023) Utilizando-se dos conceitos de malwares, qual é o nome do programa malicioso capaz de se propagar automaticamente e explorar vulnerabilidades existentes ou falhas em softwares, dispondo de um mecanismo de comunicação com o invasor, permitindo que seu controle seja realizado remotamente?

- a) Worm
- b) Storm
- c) Firewall
- d) Proxy
- e) Bot

Comentários:

(a) Errado. Worms se propagam automaticamente explorando vulnerabilidades, mas não possuem, necessariamente, um mecanismo de comunicação com o invasor para controle remoto;

(b) Errado. Storm não é um tipo de malware, mas pode se referir à Storm Botnet, uma rede de computadores infectados usada para ataques cibernéticos;

(c) Errado. Firewall não é um malware, mas sim um mecanismo de segurança que controla o tráfego de rede para proteger sistemas contra acessos não autorizados;

(d) Errado. Proxy é um servidor intermediário que pode ser usado para segurança, controle de tráfego ou anonimato na navegação, sem relação com malwares;

(e) Correto. Um bot é um programa malicioso que pode se propagar automaticamente e explorar vulnerabilidades. Além disso, ele permite controle remoto por um invasor, geralmente sendo parte de uma botnet, usada para ataques coordenados.

Gabarito: Letra E



3. (AOCP / IF-MA - 2023) Em relação aos softwares maliciosos, assinale a alternativa que apresenta uma característica de um malware classificado como WORM.

- a) Configura-se em uma rede composta por inúmeros equipamentos zumbis utilizados para potencializar as ações danosas provenientes de um ataque.
- b) Permite que um invasor retorne ao equipamento comprometido, por meio da criação ou modificação de serviços no sistema.
- c) Monitora a operação de um computador, coleta e envia as informações coletadas ao invasor.
- d) Armazena teclas digitadas por um ou mais usuários no teclado físico de um computador.
- e) Propaga-se de forma automatizada pelas redes ao explorar vulnerabilidades nos aplicativos instalados nos computadores, enviando cópias de si mesmo de computador para computador.

Comentários:

- (a) Errado. A descrição refere-se a uma botnet, que é uma rede de computadores infectados (zumbis) controlados remotamente para realizar ataques coordenados, como DDoS;
- (b) Errado. Essa característica é típica de um backdoor, que permite ao invasor acesso remoto ao sistema comprometido, sem que o usuário perceba;
- (c) Errado. O malware que monitora operações do computador e coleta informações sem consentimento é um spyware, usado para espionagem;
- (d) Errado. Um keylogger é um software malicioso que armazena as teclas digitadas pelo usuário, sendo usado para roubo de credenciais e senhas;
- (e) Correto. Worms são malwares que se propagam automaticamente por redes, explorando vulnerabilidades em sistemas e aplicativos. Eles podem replicar-se sem intervenção do usuário, consumindo recursos e causando lentidão na rede.

Gabarito: Letra E

4. (AOCP / BANESE - 2022) A rede corporativa começou a apresentar lentidão. Os analistas da rede constataram que um tipo bem específico de software malicioso atingiu o ambiente através da rede corporativa, explorando vulnerabilidades encontradas em



sistemas operacionais das estações de trabalho e consumindo recursos da rede. Além do que foi relatado, nenhum outro problema foi causado. Pela descrição desse software malicioso, a classificação mais adequada para ele seria

- a) vírus.
- b) cavalo de Troia.
- c) worm.
- d) spyware.
- e) ransomware.

Comentários:

(a) Errado. Vírus normalmente precisa de um arquivo hospedeiro para se espalhar e não se propaga automaticamente pela rede, diferentemente do cenário descrito;

(b) Errado. Cavalos de Troia (Trojans) são malwares que se disfarçam de softwares legítimos para enganar usuários e permitir acesso não autorizado ao sistema, mas não se propagam automaticamente pela rede;

(c) Correto. Worms são malwares autônomos, que se propagam automaticamente pela rede explorando vulnerabilidades em sistemas operacionais. Eles consomem recursos de rede, causando lentidão, sem necessariamente danificar arquivos ou exigir resgates;

(d) Errado. Spyware é um malware usado para espionagem, coletando informações do usuário sem permissão, mas não causa consumo excessivo de recursos de rede como descrito no problema;

(e) Errado. Ransomware criptografa arquivos e exige um pagamento para restaurá-los, mas o problema descrito na questão não menciona bloqueio de dados, apenas lentidão na rede.

Gabarito: Letra C

5. (AOCP / SANESUL - 2021) Assinale a alternativa que apresenta uma característica de malware do tipo ransomware.

- a) Exibição de propagandas para o usuário.
- b) Captura de dados digitados no teclado.
- c) Gravação dos dados exibidos na tela do usuário.
- d) Programa que captura dados bancários e envia ao invasor.
- e) Exige quantia em dinheiro para descriptografar dados do usuário.



Comentários:

- (a) Errado. A exibição de propagandas indesejadas é característica de adware, e não de ransomware;
- (b) Errado. A captura de dados digitados no teclado é característica de keyloggers, utilizados para espionagem e roubo de credenciais;
- (c) Errado. A gravação da tela do usuário pode ser feita por spyware, um tipo de malware que coleta informações sem consentimento;
- (d) Errado. Malwares especializados em roubo de dados bancários são conhecidos como trojans bancários, que monitoram atividades financeiras e enviam informações aos atacantes;
- (e) Correto. O ransomware criptografa os arquivos da vítima e exige um pagamento (resgate) para fornecer a chave de descryptografia, bloqueando o acesso aos dados até que o resgate seja pago.

Gabarito: Letra E



QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível! Vamos ao nosso questionário:

Perguntas

- 1. O que são malwares?**
- 2. Quais são as formas comuns de infecção de malwares?**
- 3. Quais são os principais procedimentos de segurança para evitar malwares?**
- 4. O que é um Vírus de Computador?**
- 5. Quais são as fases de execução de um vírus?**
- 6. O que é um Worm?**
- 7. Quais são as ações maliciosas mais comuns de um Worm?**
- 8. O que são vírus de macro?**
- 9. O que é um Vírus de Boot?**



10. O que é um Bot?
11. O que é uma Botnet?
12. Quais são as fases de funcionamento de uma Botnet?
13. O que é um Trojan Horse (Cavalo de Troia)?
14. Quais são os tipos de Trojan Horse?
15. O que é um Spyware?
16. Quais são os tipos mais comuns de Spyware?
17. O que é um Backdoor?
18. O que é um Rootkit?
19. Qual é a diferença entre um Rootkit e um Backdoor?
20. O que é um Ransomware?
21. Quais são os tipos de Ransomware?
22. O que é um Keylogger?
23. O que é um Screenlogger?
24. O que é um Adware?
25. O que é um Sniffer?
26. O que são Bombas Lógicas?
27. O que são Exploits?
28. O que é um Hijacker?
29. O que é Engenharia Social?
30. O que é um Ataque de Força Bruta?
31. O que é Denial of Service (DoS)?
32. O que é IP Spoofing?
33. O que é E-mail Spoofing?



- 34. O que é Phishing Scam?
- 35. Quais são exemplos de Phishing Scam?
- 36. Como se prevenir contra Phishing?
- 37. O que é Spear Phishing?
- 38. O que é Smishing?
- 39. O que é Pharming?
- 40. O que é um Hoax?
- 41. O que é Man in the Middle?
- 42. O que é Defacement?
- 43. O que é SQL Injection?
- 44. O que é Furto de Identidade?
- 45. O que é Fraude de Antecipação de Recursos?



Perguntas com Respostas

1. O que são malwares?

Malwares são programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador, inseridos intencionalmente com um propósito prejudicial.

2. Quais são as formas comuns de infecção de malwares?

Por exploração de vulnerabilidades, auto-execução de mídias removíveis, acesso a páginas maliciosas, execução de arquivos infectados obtidos de anexos de e-mails, mídias removíveis ou da web.

3. Quais são os principais procedimentos de segurança para evitar malwares?

Manter programas atualizados, utilizar apenas softwares originais, aplicar atualizações, usar mecanismos de proteção, fazer backup dos dados, usar configurações de segurança e ser cuidadoso ao enviar para manutenção.

4. O que é um Vírus de Computador?

É um programa que se propaga infectando outros arquivos e programas, replicando-se e causando danos, dependendo da execução de um hospedeiro para se ativar e continuar a infecção.

5. Quais são as fases de execução de um vírus?

Dormência, Propagação, Ativação e Ação.

6. O que é um Worm?

Um Worm é um programa autorreplicante que se espalha automaticamente de computador para computador sem infectar arquivos, explorando vulnerabilidades ou se propagando diretamente pela rede.

7. Quais são as ações maliciosas mais comuns de um Worm?

Consumem muitos recursos, afetando o desempenho de redes, e podem instalar outros códigos maliciosos, enviar e-mails não autorizados e desferir ataques na internet.

8. O que são vírus de macro?

São vírus que infectam documentos contendo macros (scripts) e se propagam por anexos de documentos, geralmente usados em aplicativos como o Microsoft Office.

9. O que é um Vírus de Boot?



É um vírus que infecta o setor de inicialização de sistemas, ativando-se durante o procedimento de boot e afetando a execução do sistema operacional.

10. O que é um Bot?

Bot é um programa que permite controle remoto do computador infectado, com mecanismos de comunicação que permitem ao invasor enviar instruções para executar ações maliciosas.

11. O que é uma Botnet?

Botnet é uma rede de computadores infectados por bots (zumbis), controlados remotamente, usada para potencializar ações maliciosas como ataques de negação de serviço e envio de spam.

12. Quais são as fases de funcionamento de uma Botnet?

Propagação de bots para infectar computadores; 2. Zumbis ficam à espera de comandos; 3. Controlador envia comandos; 4. Zumbis executam os comandos; 5. Espera de novos comandos.

13. O que é um Trojan Horse (Cavalo de Troia)?

Trojan Horse é um software malicioso que aparenta ser útil, mas também executa funções ocultas e maliciosas, como abrir portas de comunicação para invasores controlarem o computador.

14. Quais são os tipos de Trojan Horse?

Downloader (baixa outros malwares), Dropper (instala malwares), Backdoor (acesso remoto), DoS (negação de serviço), Destrutivo, Clicker, Proxy, Spy (roubo de dados), Trojan Banker (roubo de dados bancários).

15. O que é um Spyware?

Spyware é um software espião que coleta informações do usuário sem o seu conhecimento, podendo ser legítimo ou malicioso. Pode monitorar navegação, senhas, e enviar dados para terceiros.

16. Quais são os tipos mais comuns de Spyware?

Keyloggers (captura de teclas), Screenloggers (captura de tela), Adwares (exibição de anúncios indesejados).

17. O que é um Backdoor?

Backdoor é um software malicioso que permite ao invasor acessar remotamente um computador já comprometido, sem que seja necessário repetir o método de invasão original.

18. O que é um Rootkit?



Rootkit é um conjunto de programas que permite esconder a presença de um invasor ou malware em um computador, alterando o sistema operacional para camuflar atividades e permitir controle contínuo.

19. Qual é a diferença entre um Rootkit e um Backdoor?

Rootkit é mais avançado e camufla a presença do invasor, podendo alterar o sistema operacional. Já o Backdoor foca em permitir o retorno do invasor sem precisar repetir a invasão.

20. O que é um Ransomware?

Ransomware é um código malicioso que bloqueia o acesso a dados de um equipamento e exige pagamento de resgate (ransom) para restaurar o acesso, geralmente utilizando criptografia.

21. Quais são os tipos de Ransomware?

Ransomware Locker: impede o acesso ao equipamento; 2. Ransomware Crypto: impede o acesso aos dados utilizando criptografia.

22. O que é um Keylogger?

Keylogger é um tipo de spyware que registra e armazena as teclas digitadas no teclado, enviando essas informações a um invasor, podendo capturar senhas e dados pessoais.

23. O que é um Screenlogger?

Screenlogger é um spyware que captura imagens da tela do computador ou a posição do cursor, principalmente para capturar dados inseridos em teclados virtuais.

24. O que é um Adware?

Adware é um software que exibe propagandas automaticamente, muitas vezes instalado sem o consentimento do usuário. Pode ser legítimo ou malicioso, exibindo anúncios conforme a navegação do usuário.

25. O que é um Sniffer?

Sniffer é um software que monitora e captura pacotes de dados em uma rede, podendo ser utilizado de forma legítima por administradores ou de forma maliciosa para interceptar dados confidenciais.

26. O que são Bombas Lógicas?

Bombas Lógicas são softwares maliciosos programados para causar danos quando um evento específico ocorre, como a demissão de um funcionário ou uma data pré-determinada.

27. O que são Exploits?



Exploits são softwares que exploram vulnerabilidades conhecidas em sistemas, permitindo que invasores realizem ataques, como roubo de informações ou propagação de vírus.

28. O que é um Hijacker?

Hijacker é um software malicioso que altera o comportamento do navegador, modificando páginas iniciais, abrindo páginas automaticamente ou inserindo botões inadvertidamente.

29. O que é Engenharia Social?

Engenharia Social é uma técnica que manipula e engana pessoas para que revelem informações confidenciais ou realizem ações prejudiciais, como fornecer senhas ou acessar sites maliciosos.

30. O que é um Ataque de Força Bruta?

Ataque de Força Bruta é uma técnica de adivinhar senhas ou chaves de segurança por meio de tentativas repetitivas e automáticas, utilizando listas de palavras ou combinações.

31. O que é Denial of Service (DoS)?

Denial of Service (DoS) é um ataque que visa exaurir os recursos de um serviço, computador ou rede, tornando-o indisponível para seus usuários legítimos.

32. O que é IP Spoofing?

IP Spoofing é a falsificação de endereços IP para fazer com que um atacante se passe por um usuário autorizado, obtendo acessos não autorizados na rede.

33. O que é E-mail Spoofing?

E-mail Spoofing é a falsificação do remetente de um e-mail para enganar o destinatário, frequentemente usado em golpes de phishing e propagação de malware.

34. O que é Phishing Scam?

Phishing Scam é uma fraude que tenta enganar usuários para obter dados pessoais e financeiros, por meio de mensagens que parecem ser de fontes confiáveis, mas redirecionam para páginas falsas ou instalam malwares.

35. Quais são exemplos de Phishing Scam?

Páginas falsas de bancos ou comércio eletrônico; 2. Mensagens contendo formulários para inserir dados; 3. Links para códigos maliciosos; 4. Solicitações de cadastramento falso.

36. Como se prevenir contra Phishing?

Fique atento a mensagens suspeitas, evite clicar em links sem verificar a autenticidade, use programas de segurança, e verifique se o site usa conexão segura (https).



37. O que é Spear Phishing?

Spear Phishing é um ataque direcionado a indivíduos, empresas ou organizações específicas, com o objetivo de roubar dados ou instalar malwares.

38. O que é Smishing?

Smishing é uma forma de phishing realizada por mensagens SMS, em que o golpista tenta enganar a vítima para obter informações pessoais ou financeiras sensíveis.

39. O que é Pharming?

Pharming é um ataque que corrompe o serviço de DNS, redirecionando o usuário para sites falsos, mesmo quando ele digita o endereço correto de um site legítimo.

40. O que é um Hoax?

Hoax é uma mensagem falsa ou alarmante que se propaga com o objetivo de espalhar desinformação ou boatos, ocupando espaço nas caixas de e-mails e comprometendo a credibilidade das pessoas envolvidas.

41. O que é Man in the Middle?

Man in the Middle é um ataque em que o invasor intercepta, registra e possivelmente altera a comunicação entre duas partes, sem que elas percebam.

42. O que é Defacement?

Defacement é a desfiguração de uma página web por invasores que alteram o conteúdo do site, geralmente explorando vulnerabilidades ou acessando o servidor.

43. O que é SQL Injection?

SQL Injection é uma técnica de ataque em que o invasor insere comandos SQL maliciosos em entradas de dados, manipulando o banco de dados para obter informações confidenciais ou comprometer o sistema.

44. O que é Furto de Identidade?

Furto de Identidade é quando uma pessoa tenta se passar por outra, usando suas informações pessoais para obter vantagens indevidas, como abrir contas ou acessar serviços em nome da vítima.

45. O que é Fraude de Antecipação de Recursos?

Fraude de Antecipação de Recursos é um golpe em que a vítima é induzida a realizar um pagamento adiantado, com a promessa de obter um benefício futuro que nunca se materializa.



LISTA DE QUESTÕES ESTRATÉGICAS

1. (AOCP / UFS - 2024) Malwares são programas maliciosos que podem assumir várias formas e realizar ações prejudiciais nos sistemas. Entre os diferentes tipos de malwares, o "vírus" é um dos mais conhecidos. Assinale a alternativa que apresenta a definição correta do malware "vírus".

- a) É um tipo de malware que se anexa a arquivos ou programas legítimos e se replica quando esses arquivos ou programas são executados.
- b) É um tipo de malware que se disfarça como software legítimo, mas realiza ações maliciosas sem o conhecimento do usuário.
- c) É um programa autônomo que se replica e se espalha para outros computadores em uma rede ou pela internet.
- d) É um malware que registra todas as teclas digitadas em um teclado, capturando informações confidenciais, como senhas e informações de cartão de crédito.
- e) Envolve a distribuição de malware por meio de anúncios maliciosos exibidos em sites legítimos.

2. (AOCP / IF-MA - 2023) Utilizando-se dos conceitos de malwares, qual é o nome do programa malicioso capaz de se propagar automaticamente e explorar vulnerabilidades existentes ou falhas em softwares, dispondo de um mecanismo de comunicação com o invasor, permitindo que seu controle seja realizado remotamente?

- a) Worm
- b) Storm
- c) Firewall
- d) Proxy
- e) Bot

3. (AOCP / IF-MA - 2023) Em relação aos softwares maliciosos, assinale a alternativa que apresenta uma característica de um malware classificado como WORM.

- a) Configura-se em uma rede composta por inúmeros equipamentos zumbis utilizados para potencializar as ações danosas provenientes de um ataque.



- b) Permite que um invasor retorne ao equipamento comprometido, por meio da criação ou modificação de serviços no sistema.
- c) Monitora a operação de um computador, coleta e envia as informações coletadas ao invasor.
- d) Armazena teclas digitadas por um ou mais usuários no teclado físico de um computador.
- e) Propaga-se de forma automatizada pelas redes ao explorar vulnerabilidades nos aplicativos instalados nos computadores, enviando cópias de si mesmo de computador para computador.

4. (AOCP / BANESE - 2022) A rede corporativa começou a apresentar lentidão. Os analistas da rede constataram que um tipo bem específico de software malicioso atingiu o ambiente através da rede corporativa, explorando vulnerabilidades encontradas em sistemas operacionais das estações de trabalho e consumindo recursos da rede. Além do que foi relatado, nenhum outro problema foi causado. Pela descrição desse software malicioso, a classificação mais adequada para ele seria

- a) vírus.
- b) cavalo de Troia.
- c) worm.
- d) spyware.
- e) ransomware.

5. (AOCP / SANESUL - 2021) Assinale a alternativa que apresenta uma característica de malware do tipo ransomware.

- a) Exibição de propagandas para o usuário.
- b) Captura de dados digitados no teclado.
- c) Gravação dos dados exibidos na tela do usuário.
- d) Programa que captura dados bancários e envia ao invasor.
- e) Exige quantia em dinheiro para descriptografar dados do usuário.



GABARITO

1. LETRA A
2. LETRA E
3. LETRA E
4. LETRA C
5. LETRA E



REFERÊNCIAS BIBLIOGRÁFICAS

1. CERT.BR. Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/>. Acesso em: 8 set. 2024.
2. CERT.BR. Glossário de Segurança. Disponível em: <https://cartilha.cert.br/glossario/>. Acesso em: 8 set. 2024.
3. CERT.BR. Mitos sobre Segurança na Internet. Disponível em: <https://cartilha.cert.br/mitos/>. Acesso em: 8 set. 2024.



ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.