Qual função de trabalho SOC gerencia todos os recursos do SOC e serve como um ponto de contato para a organização ou cliente maior?

Gerenciador SOC

Qual função de trabalho SOC processa alertas de segurança e encaminha tickets para o nível 2, se necessário?

Analista de segurança cibernética

Qual função de trabalho SOC é responsável pela investigação profunda de incidentes?

Responsável pela resposta a incidentes

Qual dispositivo integra informações de segurança e gerenciamento de eventos em uma única plataforma?

SIEM

Qual dispositivo integra ferramentas e recursos de orquestração para responder automaticamente a eventos de segurança?

SOAR

A qual pessoal de um SOC tem a tarefa de verificar se um alerta acionado pelo software de monitoramento representa um verdadeiro incidente de segurança?

Pessoal de nível 1

Tópico 2.1.0 - Em um SOC, o trabalho de um Analista de Alerta de Nível 1 inclui o monitoramento de alertas recebidos e a verificação de que um verdadeiro incidente de segurança ocorreu.

Depois que um incidente de segurança é verificado em um SOC, um respondedor de incidentes revisa o incidente, mas não consegue identificar a origem do incidente e formar um procedimento de mitigação eficaz. A quem o tíquete de incidente deve ser escalado?

Uma PME para investigação mais aprofundada

Tópico 2.1.0 - Um respondente a incidentes é um profissional de segurança de nível 2 em um SOC. Se o respondente não puder resolver o tíquete de incidente, o tíquete de incidente deve ser encaminhado para o próximo nível de suporte, um Camada 3.Uma PME de nível 3 investigaria mais aprofundadamente o incidente.

Quais dois serviços são fornecidos pelos centros de operações de segurança? (Escolha duas.)

Gerenciamento de soluções abrangentes de ameaças

Monitoramento de ameaças de segurança de rede

Tópico 2.1.0 - Os Centros de Operações de Segurança (SOCs) podem fornecer uma ampla gama de serviços para se defender contra ameaças aos sistemas de informação de uma organização. Esses serviços incluem monitoramento de ameaças à segurança de rede e gerenciamento de soluções abrangentes para combater ameaças. Garantir trocas de roteamento seguras e fornecer conexões seguras à Internet são tarefas normalmente executadas por um centro de operações de rede (NOC). Responder a invasões de instalações é normalmente a função e responsabilidade do departamento de polícia local.

Qual métrica é usada em SOCs para avaliar o tempo médio necessário para identificar que ocorreram incidentes de segurança válidos na rede?

MTTD

Tópico 2.1.0 - Os SOCs usam muitas métricas como indicadores de desempenho de quanto tempo o pessoal leva para localizar, interromper e corrigir incidentes de segurança.

Horas paradas

Tempo Médio para Detectar (MTTD)

Tempo médio de resposta (MTTR)

Tempo Médio para Conter (MTTC)

Tempo para o controle

Qual métrica de KPI o SOAR usa para medir o período de tempo que os atores da ameaça têm acesso a uma rede antes de serem detectados e o acesso dos atores da ameaça ser interrompido?

Horas paradas

Tópico 2.1.0 - As métricas comuns do indicador de desempenho (KPI) compiladas pelos gerentes de SOC são as seguintes:

• Tempo de permanência: o período de tempo que os atores da ameaça têm acesso a uma rede antes de serem detectados e o acesso dos atores da ameaça interrompido

• Mean Time to Detect (MTTD): o tempo médio que o pessoal do SOC leva para identificar incidentes de segurança válidos ocorreu na rede

• Mean Time to Responder (MTTR): o tempo médio necessário para parar e corrigir um incidente de segurança

• Mean Time to Conter (MTTC): o tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados

Qual é a função do SIEM?

Para analisar todos os dados que firewalls, appliances de rede, sistemas de detecção de intrusões e outros dispositivos geram e instituem medidas preventivas

Tópico 2.1.0 - Um sistema de gerenciamento de eventos e informações de segurança (SIEM) faz sentido a todos os dados gerados por firewalls, dispositivos de rede, sistemas de detecção de intrusões e outros dispositivos. Os SIEMs são usados para coletar e filtrar dados, detectar e classificar ameaças e analisar e investigar ameaças. Os sistemas SIEM também podem gerenciar recursos para implementar medidas preventivas e lidar com ameaças futuras.

O que é uma característica da plataforma de segurança SOAR?

Para incluir playbooks predefinidos que permitem a resposta automática a ameaças específicas

Tópico 2.1.0 - As plataformas de segurança SOAR oferecem os seguintes recursos:

• Recolher dados de alarme de cada componente do sistema

• Fornecer ferramentas que permitam que os casos sejam pesquisados, avaliados e investigados

• Enfatizar a integração como um meio de automatizar fluxos de trabalho complexos de resposta a incidentes que permitem respostas mais rápidas e estratégias de defesa adaptativas

• Incluir playbooks predefinidos que permitem a resposta automática a ameaças específicas

Um profissional de segurança de rede solicitou uma posição de Nível 2 em um SOC. O que é uma função de trabalho típica que seria atribuída a um novo funcionário?

Investigar mais incidentes de segurança

Tópico 2.1.0 - Em um SOC típico, o trabalho de um respondedor de incidentes de Nível 2 envolve investigação aprofundada de incidentes de segurança.

Se um SOC tiver uma meta de 99,99% de tempo de atividade, quantos minutos de tempo de inatividade por ano seriam considerados dentro de sua meta?

52.56

Tópico 2.1.0 - Dentro de um ano, há 365 dias x 24 horas por dia x 60 minutos por hora = 525.600 minutos. Com a meta de tempo de atividade 99,99% do tempo, o tempo de inatividade precisa ser controlado sob 525.600 x (1-0,9999) = 52,56 minutos por ano.

Qual organização oferece a certificação CySA+ neutra do fornecedor?

CompTIA

Tópico 2.2.0 - A certificação CompTIA Cybersecurity Analyst (CySA+) é uma certificação profissional de segurança neutra no fornecedor.

Na operação de um SOC, qual sistema é freqüentemente usado para permitir que um analista selecione alertas de um pool para investigar?

Sistema de emissão de bilhetes

Tópico 2.1.0 - Em um SOC, um sistema de tickets é normalmente usado para um sistema de gerenciamento de fluxo de trabalho.

Como um sistema de gerenciamento de eventos e informações de segurança em um SOC pode ser usado para ajudar o pessoal a lutar contra ameaças à segurança?

Coletando e filtrando dados

Tópico 2.1.0 - Um sistema de gerenciamento de eventos e informações de segurança (SIEM) combina dados de várias fontes para ajudar o pessoal da SOC a coletar e filtrar dados, detectar e classificar ameaças, analisar e investigar ameaças e gerenciar recursos para implementar medidas preventivas.

Quais três tecnologias devem ser incluídas em um sistema de gerenciamento de eventos e informações de segurança em um SOC? (Escolha três.)

Inteligência de ameaças

Rastreamento de vulnerabilidades

Monitoramento da segurança

Tópico 2.1.0 - As tecnologias em um SOC devem incluir o seguinte:

Coleta, correlação e análise de eventos

Monitoramento de segurança

Controle de segurança

Gerenciamento de log

Avaliação de vulnerabilidade

Controle de vulnerabilidades

Inteligência de ameaças

Os appliances de firewall, VPNs e IPS são dispositivos de segurança implantados na infra-estrutura de rede.

Um invasor envia um pedaço de malware como anexo de email para funcionários de uma empresa. Qual é o propósito provável do ataque?

Busca e obtenção de segredos comerciais

O que é guerra cibernética?

É um ataque destinado a pertubar, corromper ou explorar interesses nacionais

Que tipo de malware tem o objetivo principal de se espalhar pela rede?

worm

Qual é o risco potencial ao usar um hotspot sem fio gratuito e aberto em um local público?

O tráfego da rede pode ser sequestrado e as informações roubadas

A pedido dos investidores, uma empresa está procedendo com a atribuição cibernética com um ataque particular que foi conduzido a partir de uma fonte externa. Qual termo de segurança é usado para descrever a pessoa ou dispositivo responsável pelo ataque?

Ator de ameaça

Que nome é dado a um hacker amador?

Hacker inexperiente

O que normalmente motiva os cibercriminosos a atacar redes em comparação com hacktivistas ou hackers patrocinados pelo estado?

Ganho financeiro

O que é um botnet?

Uma rede de computadores infectados que são controlados como um grupo

O que é um hotspot sem fio desonesto?

É um ponto de acesso que parece ser de um negócio legítimo, mas foi realmente criado por alguém sem a permissão do negócio

Qual é a melhor definição de informações de identificação pessoal (PII)?

Dados coletados pelas empresas para distinguir identidades de indivíduos

O que foi usado como arma de guerra cibernética para atacar uma instalação de enriquecimento de urânio no Irã?

Stuxnet

Uma empresa paga uma quantia significativa de dinheiro aos hackers, a fim de recuperar o controle de um servidor de e-mail e dados. Que tipo de ataque de segurança foi usado pelos hackers?

Ramsomware

Quais são as três categorias principais de elementos em um centro de operações de segurança? (Escolha três.)

Pessoas

Processos

Tecnologias

A qual pessoal de um SOC é atribuída a tarefa de procurar ameaças em potencial e implementar ferramentas de detecção de ameaças?

Camada 3 SME

Um agente de ameaça identificou a vulnerabilidade potencial do servidor Web de uma organização e está criando um ataque. O que o ator ameaça fará para construir uma arma de ataque?

* Obtenha uma ferramenta automatizada para entregar a carga útil do malware através da vulnerabilidade

Corresponda a métrica SOC à descrição. (Nem todas as opções são usadas).

tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados - MTTC

período de tempo em que os atores da ameaça têm acesso a uma rede antes de seu acesso ser interrompido – Dwell Time

​tempo médio para identificar que ocorreram incidentes de segurança válidos na rede - MTTD

​​tempo médio necessário para parar e corrigir um incidente de segurança – MTTR

Um SOC está procurando um profissional para preencher uma vaga de emprego. O funcionário deve ter habilidades de nível especializado em rede, endpoint, inteligência contra ameaças e engenharia reversa de malware para procurar ameaças cibernéticas ocultas na rede. Qual trabalho dentro de um SOC requer um profissional com essas habilidades?

Caçador de ameaças

Qual organização é uma organização internacional sem fins lucrativos que oferece a certificação CISSP?

(ISC2)

O termo analista de operações cibernéticas se refere a qual grupo de funcionários em um SOC?

Pessoal de nível 1

Qual trabalho exigiria a verificação de que um alerta representa um verdadeiro incidente de segurança ou um falso positivo?

Analista de alerta

Qual é o benefício de uma organização usar o SOAR como parte do sistema SIEM?

O SOAR automatiza a investigação de incidentes e responde a fluxos de trabalho com base em playbooks.

Quais são as três tecnologias que devem ser incluídas em um sistema de gerenciamento de eventos e informações de segurança SOC? (Escolha três.)

Inteligência de log

Gerenciamento de log

Monitoramento de segurança

Como um sistema de gerenciamento de eventos e informações de segurança (SIEM) em um SOC ajuda o pessoal a lutar contra as ameaças à segurança?

combinando dados de várias tecnologias

Que tipo de arma de guerra cibernética era Stuxnet?

Worm

Um funcionário se conecta sem fio à rede corporativa com um telefone celular. O funcionário configura o telefone celular para atuar como um ponto de acesso sem fio que permite que novos funcionários se conectem à rede corporativa. Que tipo de ameaça à segurança melhor descreve essa situação?

ponto de acesso invasor

Qual ataque cibernético envolve um ataque coordenado de uma botnet de computadores zumbis?

DDos

Quando um usuário liga o PC na quarta-feira, o PC exibe uma mensagem indicando que todos os arquivos do usuário foram bloqueados. Para obter os arquivos não criptografados, o usuário deve enviar um e-mail e incluir uma ID específica no título do e-mail. A mensagem também inclui maneiras de comprar e enviar bitcoins como pagamento para a descriptografia do arquivo. Depois de inspecionar a mensagem, o técnico suspeita que ocorreu uma violação de segurança. Que tipo de malware poderia ser responsável?

Ransomware

Qual exemplo ilustra como o malware pode ser escondido?



Um e-mail é enviado para os funcionários de uma empresa com um anexo que se parece com uma atualização de antivírus, mas na verdade consiste em um spyware.

O que é a Dark Web?

É parte da internet que só pode ser acessado com software especial.

O que caracteriza um ator de ameaça?

* Eles sempre tentam causar algum dano a um indivíduo ou organização.

Uma empresa acaba de ter um incidente de segurança cibernética. O ator da ameaça parecia ter um objetivo de interrupção da rede e parecia usar uma ferramenta comum de hack de segurança que sobrecarregava um determinado servidor com uma grande quantidade de tráfego. Esse tráfego tornou o servidor inoperável. Como um analista certificado de segurança cibernética classificaria esse tipo de ator de ameaças?

Amador

Um grupo de usuários na mesma rede está reclamando de seus computadores rodando lentamente. Depois de investigar, o técnico determina que esses computadores fazem parte de uma rede zumbi. Que tipo de malware é usado para controlar esses computadores?

Botnet

Qual declaração descreve a guerra cibernética?

É um conflito baseado na Internet que envolve a penetração das redes e sistemas de computador de outras nações.

Quais sites um usuário deve evitar ao se conectar a um hotspot sem fio gratuito e aberto?

sites para fazer compras

Quando um usuário faz alterações nas configurações de um sistema Windows, onde essas alterações são armazenadas?

Registro

Tópico 3.2.0 - O registro contém informações sobre aplicativos, usuários, hardware, configurações de rede e tipos de arquivo. O registro também contém uma seção exclusiva para cada usuário, que contém as configurações configuradas por esse usuário específico.

Qual conta de usuário deve ser usada apenas para executar o gerenciamento do sistema e não como a conta para uso regular?

Administrador

Tópico 3.3.0 - A conta de administrador é usada para gerenciar o computador e é muito poderosa. As boas práticas recomendam que ele seja usado somente quando for necessário para evitar a realização acidental de alterações significativas no sistema.

Qual comando é usado para consultar manualmente um servidor DNS para resolver um nome de host específico?

Nslookup

Tópico 3.3.0 - O comando nslookup foi criado para permitir que um usuário consulte manualmente um servidor DNS para resolver um determinado nome de host. O comando ipconfig /displaydns exibe apenas entradas DNS previamente resolvidas. O comando tracert foi criado para examinar o caminho que os pacotes percorrem, à medida que cruzam uma rede e podem resolver um nome de host consultando automaticamente um servidor DNS. O comando net é usado para gerenciar computadores de rede, servidores, impressoras e unidades de rede.

Por motivos de segurança, um administrador de rede precisa garantir que os computadores locais não possam efetuar ping entre si. Quais configurações podem realizar essa tarefa?

Configuração de firewall

Tópico 3.4.0 - As configurações do sistema de arquivos e do cartão inteligente não afetam a operação da rede. As configurações de endereço MAC e a filtragem podem ser usadas para controlar o acesso à rede do dispositivo, mas não podem ser usadas para filtrar diferentes tipos de tráfego de dados.

O que contém informações sobre como as partições de disco rígido são organizadas?

MBR

Tópico 3.2.0 - O MBR contém um pequeno programa que é responsável por localizar e carregar o sistema operacional.

Qual utilitário é usado para mostrar os recursos do sistema consumidos por cada usuário?

Gerenciador de tarefas

Tópico 3.3.0 - O utilitário Gerenciador de Tarefas do Windows inclui uma guia Usuários na qual os recursos do sistema consumidos por cada usuário podem ser exibidos.

Que termo é usado para descrever uma unidade lógica que pode ser formatada para armazenar dados?

Partição

Tópico 3.2.0 - As unidades de disco rígido são organizadas por várias estruturas físicas e lógicas. As partições são porções lógicas do disco que podem ser formatadas para armazenar dados. As partições consistem em trilhas, em setores, e em clusters. As trilhas são anéis concêntricos na superfície do disco. As trilhas são divididas em setores e vários setores são combinados de forma lógica, para formar clusters

Quanta RAM é endereçável por uma versão de 32 bits do Windows?

4GB

Tópico 3.1.0 - Um sistema operacional de 32 bits é capaz de suportar aproximadamente 4 GB de memória. Isso ocorre porque 2^32 é aproximadamente 4 GB.

Qual versão do Windows foi a primeira a introduzir um sistema operacional Windows de 64 bits?

Windows XP

Tópico 3.1.0 - Existem mais de 20 lançamentos e versões do sistema operacional Windows. O lançamento do Windows XP introduziu o processamento de 64 bits para a computação WIndows.

Qual comando net é usado em um PC Windows para estabelecer uma conexão com um diretório compartilhado em um servidor remoto?

Net use

Tópico 3.3.0 - O comando net é um comando muito importante no Windows. Alguns comandos net comuns incluem o seguinte:

net accounts — define os requisitos de senha e logon para usuários

net session — lista ou desconecta sessões entre um computador e outros computadores na rede

net share — cria, remove ou gerencia recursos compartilhados

net start — inicia um serviço de rede ou lista os serviços de rede em execução

net stop – interrompe um serviço de rede

net use — conecta, desconecta e exibe informações sobre recursos de rede compartilhados

net view — mostra uma lista de computadores e dispositivos de rede na rede

Qual é o propósito do comando cd?

Muda o diretório para o diretório raiz

Tópico 3.1.0 - Os comandos da CLI são digitados na janela Prompt de Comando do sistema operacional Windows. O comando cd é usado para alterar o diretório para o diretório raiz do Windows.

O que seria exibido se o comando netstat -abno fosse inserido em um PC com Windows?

Todas as conexões TCP e UDP ativas, seu estado atual e seu ID de processo associado (PID)

Tópico 3.4.0 - Com o parâmetro opcional -abno, o comando netstat exibirá todas as conexões de rede juntamente com os processos em execução associados. Ajuda o usuário a identificar possíveis conexões de malware.

Um incidente de segurança foi arquivado e um empregado acredita que alguém esteve no computador desde que o empregado saiu ontem à noite. O funcionário afirma que o computador foi desligado antes de o funcionário sair para a noite. O computador está funcionando lentamente e os aplicativos estão agindo de forma estranha. Qual ferramenta do Microsoft Windows seria usada pelo analista de segurança para determinar se e quando alguém fez logon no computador após o horário de trabalho?

Visualizador de eventos

Tópico 3.4.0 - Visualizador de eventos é usado para investigar o histórico de eventos de aplicativo, segurança e sistema. Os eventos mostram a data e a hora em que o evento ocorreu junto com a origem do evento. Se um analista de segurança cibernética tiver o endereço do computador Windows alvo ou a data e hora em que ocorreu uma violação de segurança, o analista poderá usar o Visualizador de Eventos para documentar e provar o que ocorreu no computador.

Qual ferramenta do Windows nega seletivamente o tráfego para um computador ou segmento de rede?

Firewall do Windows defender

Qual ferramenta do Windows registra histórico, aplicativos, segurança e eventos do sistema?

Visualizador de eventos

Qual ferramenta ou comando do Windows pode ser usado para procurar conexões TCP de entrada ou saída em um host Windows que não estão autorizadas?

Netstat

Qual ferramenta do Windows fornece informações sobre recursos, como memória, CPU, disco e rede?

Resource monitor

Qual ferramenta do Windows é a proteção interna contra vírus e spyware?

Windows defender

Qual comando ou ferramenta localiza o endereço IP de um servidor a partir de uma URL?

Nslookup

Qual ferramenta do Windows fornece informações sobre aplicativos, processos e serviços em execução no computador?

Gerenciador de tarefas

Qual ferramenta do Windows é o banco de dados que armazena todas as informações sobre hardware, aplicativos, usuários e configurações do sistema?

Registro do Windows

Que tipo de ferramenta é usada por um administrador do Linux para atacar um computador ou rede para encontrar vulnerabilidades?

Pentesting

.1.0 - Pentesting é conhecido como testes de penetração e inclui ferramentas que são usadas para procurar vulnerabilidades em uma rede ou computador atacando-o.

Qual é a vantagem de o Linux ser um sistema operacional de código aberto?

O código-fonte de distribuição Linux pode ser modificado e, em seguida, recompilado

Tópico 4.1.0 - Linux é um sistema operacional de código aberto e qualquer pessoa pode acessar o código-fonte, inspecioná-lo, modificá-lo e recompilá-lo. As distribuições Linux são mantidas por uma comunidade de programadores e são projetadas para serem conectadas a uma rede e não precisam fornecer suporte gratuito.

Qual método pode ser usado para fortalecer um dispositivo?

Força mudanças periódicas de senha

Tópico 4.4.0 - As melhores práticas básicas para o fortalecimento (hardering) de dispositivos são as seguintes:

Garanta a segurança física.

Minimize os pacotes instalados.

Desative serviços não utilizados.

Use SSH e desabilite o login da conta raiz sobre SSH.

Mantenha o sistema atualizado.

Desative a detecção automática USB.

Aplique senhas fortes.

Força mudanças periódicas de senha.

impedir que os usuários reutilizem senhas antigas.

Revise os registros regularmente.

Um administrador de sistema emite o comando ps em um servidor que esteja executando o sistema operacional Linux. Qual é o objetivo desse comando?

Para listar os processos atualmente em execução no sistema

Tópico 4.2.0 - O comando Linux ps é usado para listar os processos atualmente em execução no sistema. Se necessário, esse comando pode ser instruído a exibir processos em execução iniciados pelo usuário atual ou por outros usuários.

Qual código fonte do sistema operacional pode ser baixado e modificado por qualquer pessoa ou empresa?

Linux

Tópico 4.1.0 - Programas de código aberto, como Linux, permitem que o código-fonte seja distribuído e alterado por qualquer pessoa.

Que sistema de arquivos é o sistema de arquivos principal usado pelo Apple em computadores Macintosh atuais?

APFS

Tópico 4.5.0 - O principal sistema de arquivos usado pela Apple em seus últimos computadores Macintosh é o APFS.

Considere o resultado do comando ls -l na saída Linux abaixo. Quais são as permissões de arquivo de grupo atribuídas ao arquivo analyst.txt?

ls –l analyst.txt

-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt

Ler e escrever

Tópico 4.5.0 - As permissões de arquivo são sempre exibidas na ordem Usuário, Grupo e Outro. No exemplo exibido, o arquivo tem as seguintes permissões:

O traço (-) significa que este é um arquivo. Para diretórios, o primeiro traço seria substituído por um\ "d\”.

O primeiro conjunto de caracteres é para permissão de usuário (rwx). O usuário, vendas, que possui o arquivo pode ler, escrever e executar o arquivo.

O segundo conjunto de caracteres é para permissões de grupo (rw-). O grupo, equipe, que possui o arquivo pode ler e gravar no arquivo.

O terceiro conjunto de caracteres é para quaisquer outras permissões de usuário ou grupo (r—). Qualquer outro usuário ou grupo no computador pode apenas ler o arquivo.

No contexto de um sistema operacional Linux, qual comando pode ser usado para exibir a sintaxe e os parâmetros de um comando específico?

man

Tópico 4.2.0 - As funções dos comandos CLI listados de um sistema Linux são as seguintes:

cat- lista o conteúdo de um arquivo

man – exibe a documentação para um comando específico

crontab – gerencia o serviço cron para agendar tarefas do sistema

grep – pesquisa cadeias de caracteres específicas em um arquivo ou outras saídas de comandos

O que é um daemon?

Um processo em segundo plano que é executado sem a necessidade de interação do usuário

Tópico 4.4.0 - Um daemon no Linux é um processo em segundo plano que é executado sem a necessidade de interação do usuário. Um administrador de rede pode visualizar arquivos de log para ver informações sobre daemons em execução no servidor Linux.

Qual comando do Linux pode ser usado para exibir o nome do diretório de trabalho atual?

pwd

Tópico 4.2.0 - Um dos comandos mais importantes no Linux é o comando pwd , que significa diretório de trabalho de impressão. Ele mostra aos usuários o caminho físico para o diretório em que estão trabalhando.

Um autor está carregando um documento de um capítulo de um computador pessoal para um servidor de arquivos de uma editora. Que função desempenha o computador pessoal neste modelo de rede?

Cliente

Tópico 4.3.0 - No modelo de rede cliente / servidor, um dispositivo de rede assume a função de servidor para fornecer um serviço específico, como transferência e armazenamento de arquivos. O dispositivo que requisita o serviço desempenha a função de cliente. No modelo de rede cliente/servidor, um servidor dedicado não precisa necessariamente ser usado, mas se houver um, o modelo de rede em uso é o modelo cliente/servidor. Ao contrário de um modelo de rede peer-to-peer que não tem um servidor dedicado.

Um técnico capturou pacotes em uma rede que está com lentidão ao acessar a Internet. Qual número de porta o técnico deve procurar no material capturado para localizar os pacotes HTTP?

80

Tópico 4.3.0 - HTTP usa a porta TCP 80 e HTTPS usa a porta TCP 443. HTTP e HTTPS são protocolos comumente usados para acessar páginas da Web.

Um administrador de sistema emite o comando apt-get upgrade em um sistema operacional Linux. Qual é o objetivo desse comando?

Cada aplicativo instalado se atualizará para a versão mais recente

Tópico 4.7.0 - Quando o comando apt-get upgrade é emitido em um terminal Linux, todos os aplicativos instalados tentarão atualizar para a versão mais recente disponível.

Por que um rootkit seria usado por um hacker?

Para obter acesso a um dispositivo sem ser detectado

Tópico 4.7.0 - Os hackers usam rootkits para evitar a detecção, bem como ocultar qualquer software instalado pelo hacker.

Por que um administrador de rede escolheria o Linux como sistema operacional no Security Operations Center (SOC)?

O administrador tem mais controle sobre o sistema operacional

Quais são os dois métodos que podem ser usados ​​para proteger um dispositivo de computação? (Escolha dois.)

Aplique o mecanismo de histórico de senha.\*

Garanta a segurança física

Qual comando do Linux pode ser usado para exibir o nome do diretório de trabalho atual?

Pwd

Considere o resultado do ls -lcomando na saída do Linux abaixo. Quais são as permissões de arquivo atribuídas ao usuário de vendas para o analyst.txtarquivo

ler, escrever, executar

Um sistema Linux inicializa na GUI por padrão, então qual aplicativo um administrador de rede pode usar para acessar o ambiente CLI

Emulador de terminal

Qual usuário pode substituir as permissões de arquivo em um computador Linux

usuário root

Que tipo de ferramenta permite aos administradores observar e compreender cada detalhe de uma transação de rede

software de captura de pacotes

Por que o Kali Linux é uma escolha popular para testar a segurança da rede de uma organização?

É uma distribuição de segurança Linux de código aberto que contém muitas ferramentas de penetração.\*

Exibe o nome do diretório de trabalho atual: pwd

executa um comando como outro usuário: sudo

modifica as permissões do arquivo: chmod

desliga o sistema: Vazio

lista os processos que estão em execução no momento: ps

Quais são as duas vantagens do sistema de arquivos NTFS em comparação com o FAT32? (Escolha dois.)

NTFS suporta arquivos maiores.\*

O NTFS oferece mais recursos de segurança.\*

Um usuário de PC emite o comando netstat sem nenhuma opção. O que é exibido como resultado deste comando?

Uma lista de todas as conexõs TCP ativas estabelecidas.

Quais são os dois comandos que podem ser usados ​​para verificar se a resolução de nomes DNS está funcionando corretamente em um PC com Windows? (Escolha dois.)

Nslookup cisco.com

Ping cisco.com

Combine a sequência de inicialização do Windows 10 após o carregamento do gerenciador de inicialização (bootmgr.exe).

Etapa um: o carregador de inicialização do Windows Winload.exe é carregado

Etapa dois: Ntosknl.exe e hal.dll são carregados

Etapa três: Winload.exe lê o registro, escolhe um perfil de hardware e carrega os drivers de dispositivo.

Etapa quatro: Ntoskrnl.exe assume o processo.

Etapa cinco: Winlogon.exe é carregado e executa o processo de logon.

Um técnico instalou um utilitário de terceiros usado para gerenciar um computador com Windows 7. No entanto, o utilitário não é iniciado automaticamente sempre que o computador é iniciado. O que o técnico pode fazer para resolver esse problema?

Altere o tipo de inicialização do utilitário para Automático em Serviços.\*

Qual afirmação descreve a função do protocolo Server Message Block (SMB)?

É usado para compartilhar recursos de rede.\*

Um usuário cria um arquivo com extensão .ps1 no Windows. Que tipo de arquivo é?

Script do PowerShell

Qual é o processo de dividir um grande fluxo de dados em partes menores antes da transmissão?

segmentação

Qual é a PDU associada à camada de transporte?

segmento

Qual camada de pilha de protocolo encapsula dados em quadros?

Enlace de dados

Qual é o nome do processo de adição de informações de protocolo aos dados à medida que ele move para baixo a pilha de protocolos?

Encapsulamento

Um host está transmitindo um broadcast. Qual host ou hosts o receberão?

Todos os hosts na mesma rede

Tópico 5.2.0 - Um broadcast é entregue a cada host que possui um endereço IP na mesma rede.

Qual afirmativa descreve uma característica da computação em nuvem?

Aplicações podem ser acessadas pela internet por usuários individuais ou empresas usando qualquer dispositivo, em qualquer parte do mundo

Tópico 5.1.0 - A computação em nuvem permite aos usuários acessar aplicativos, fazer backup e armazenar arquivos e realizar tarefas sem a necessidade de software ou servidores adicionais. Os usuários da nuvem acessam os recursos em tempo real, através de serviços de assinatura ou pagamento por uso, usando apenas um navegador web.

Um administrador de rede pode executar ping com êxito no servidor em www.cisco.com, mas não pode executar o ping no servidor web da empresa localizado em um ISP em outra cidade. Que ferramenta ou comando podem ajudar a identificar o roteador específico em que o pacote foi perdido ou atrasado?

traceroute

Tópico 5.1.0 - O comando traceroute fornece informações de conectividade sobre o caminho que um pacote segue para chegar ao destino e sobre cada roteador (salto) ao longo do caminho. Ele também indica o tempo que um pacote leva para chegar da origem em cada salto e vice-versa.

Qual camada do modelo OSI contém protocolos para comunicação processo a processo?

Aplicação

Tópico 5.2.0 - A camada de aplicação do modelo OSI é responsável pela comunicação entre os processos. Exemplos de protocolos na camada de aplicação são DHCP, DNS e HTTP.

Em qual camada OSI é um número de porta de destino adicionado a uma PDU durante o processo de encapsulamento?

Camada de transporte

Tópico 5.3.0 - A camada de transporte usa endereços de protocolo na forma de números de porta para identificar aplicativos de rede que devem lidar com dados de cliente e servidor.

Qual processo envolve colocar uma PDU dentro de outra PDU?

Encapsulamento

Tópico 5.3.0 - Quando uma mensagem é colocada dentro de outra mensagem, isso é conhecido como encapsulamento. Em redes, o encapsulamento ocorre quando uma unidade de dados de protocolo é transportada dentro do campo de dados da próxima unidade de dados de protocolo inferior.

Qual afirmação descreve com precisão um processo de encapsulamento TCP / IP quando um PC está enviando dados para a rede?

Os segmentos são enviados da camada de transporte para a camada de rede

Tópico 5.3.0 - Quando os dados estão viajando do PC para a rede, a camada de transporte envia segmentos para a camada de rede. A camada de rede envia pacotes para a camada de acesso à rede, que cria quadros e os converte em bits. Os bits são liberados para a mídia da rede.

Um cliente Web está recebendo uma resposta para uma página da Web de um servidor Web. Do ponto de vista do cliente, qual é a ordem correta da pilha de protocolo que é usada para decodificar a transmissão recebida?

Ethernet, IP, TCP, HTTP

Tópico 5.3.0-1. O HTTP controla a maneira como um servidor da web e um cliente interagem. 2. O TCP gerencia conversas individuais entre servidores da web e clientes. 3. IP é responsável pela entrega através do melhor caminho para o destino. 4. Ethernet pega o pacote do IP e formata-o para transmissão.

Como a BYOD (Bring Your Own Device) muda a maneira como as empresas implementam as redes?

BYOD significa flexibilidade em onde e como os usuários acessam os recursos da rede

Tópico 5.1.0 - Um ambiente BYOD exige que uma organização acomode uma variedade de dispositivos e métodos de acesso. Dispositivos pessoais, que não estão sob o controle da empresa, podem ser aceitos e, portanto, segurança é um fator essencial. Os custos de hardware no local serão reduzidos, permitindo que a empresa priorize a disponibilização de ferramentas de colaboração e outros softwares para usuários BYOD.

Na comunicação entre computadores, qual é o objetivo da codificação de mensagens?

Converter informações para o formato adequado para a transmissão

Tópico 5.2.0 - Antes de uma mensagem ser enviada através de uma rede, ela deve primeiro ser codificada. Codificação é o processo de conversão de dados da mensagem em outro formato adequado a transmissão pelo meio físico. Cada bit da mensagem é codificado em um padrão de sons, de ondas de luz ou de impulsos elétricos, dependendo do meio físico de rede em que os bits são transmitidos. O host destino recebe e decodifica os sinais para interpretar a mensagem.

Qual afirmação é verdadeira sobre os modelos TCP/IP e OSI?​

A camada e transporte TCP/IP e a camada 4 OSI fornecem serviços e funções semelhantes

Tópico 5.2.0 - A camada de rede do TCP / IP fornece a mesma função que a camada de rede OSI. A camada de transporte dos modelos TCP / IP e OSI fornece a mesma função. A camada de aplicação TCP / IP inclui as mesmas funções das camadas OSI 5, 6 e 7.

Que método pode ser usado por dois computadores para garantir que os pacotes não sejam descartados porque muitos dados estão sendo enviados muito rapidamente?

Controle de fluxo

Tópico 5.2.0 - Para que dois computadores possam se comunicar de forma eficaz, deve haver um mecanismo que permita que a origem e o destino definam o tempo de transmissão e recebimento dos dados. O controle de fluxo permite isso, garantindo que os dados não sejam enviados muito rápido para serem recebidos corretamente.

Qual camada OSI envia segmentos para serem encapsulados em um pacote IPv4 ou IPv6?

Camada de transporte

Qual camada é responsável por pegar um pacote IP e prepará-lo para transmissão pelo meio de comunicação?

Camada de enlace de dados

Qual é o termo para dividir um pacote IP ao encaminhá-lo de uma mídia para outra mídia com uma MTU menor?

Fragmentação

Qual método de entrega não garante que o pacote seja entregue totalmente sem erros?

Melhor esforço

Quais são os dois campos mais comumente referenciados em um cabeçalho de pacote IPv4 que indicam de onde o pacote está vindo e para onde ele está indo? (Escolha duas.)

Endereço IP de origem

Endereço IP de destino

Qual instrução está correta sobre campos de cabeçalho de pacote IPv4?

Os endereços ipv4 de origem e destino permanecem os mesmos durante a viagem de origem para o destino

Qual campo é usado para detectar corrupção no cabeçalho IPv4?

Soma de verificação do cabeçalho

Qual campo inclui valores comuns como ICMP (1), TCP (6) e UDP (17)?

Protocolos

O que é indicado por um ping bem-sucedido para o endereço IPv6: :1?

O ip está instalado corretamente no host

Tópico 7.2.0 - O Endereço IPv6 ::1 é o Endereço de Loopback. Um ping bem-sucedido para esse endereço significa que a pilha TCP/IP está instalada corretamente. Isso não significa que quaisquer endereços estão configurados corretamente.

Um usuário se queixa de que a estação de trabalho não pode acessar a rede. O técnico de rede pede ao usuário para emitir o ping 127.0.0.1comando. Qual é o propósito de usar este comando?

Para verificar se a pilha TCP/IP está operacional

Tópico 7.2.0 - O ping 127.0.0.1comando é usado para verificar a operação apropriada da pilha de protocolos TCP/IP da camada de rede para a camada física - e vice-versa. Esta operação deste comando não coloca um sinal na mídia de rede.

Qual é o procedimento usado no ICMPv6 em situações nas quais um host precisa verificar a exclusividade de um endereço IPv6 antes de configurá-lo na interface?

DAD

Tópico 7.1.0 - Antes que um host IPv6 possa habilitar e usar um endereço IPv6 atribuído, o host deve verificar se o endereço é exclusivo na rede. Para verificar que nenhum outro host está usando o endereço IPv6, o host realiza o processo de Detecção de endereço duplicado (DAD), ao enviar uma mensagem de Solicitação de vizinho (NS) ao endereço IPv6.

Um administrador de rede consegue fazer ping com êxito no servidor em www.cisco.com, mas não consegue fazer ping no servidor da Web da empresa localizado em um ISP em outra cidade. Que ferramenta ou comando podem ajudar a identificar o roteador específico em que o pacote foi perdido ou atrasado?

traceroute

Tópico 7.2.0 - O comando traceroute fornece informações de conectividade sobre o caminho que um pacote segue para chegar ao destino e sobre cada roteador (salto) ao longo do caminho. Ele também indica o tempo que um pacote leva para chegar da origem em cada salto e vice-versa.

Um usuário executa um traceroute sobre IPv6. Em que momento um roteador no caminho para o dispositivo de destino descartaria o pacote?

Quando o valor do campo limite de salto chegar a zero

Tópico 7.2.0 - Quando um traceroute é executado, o valor no campo Hop Limit de um pacote IPv6 determina quantos saltos de roteador o pacote pode viajar. Uma vez que o campo Limite de Hop atinge um valor de zero, ele não poderá mais ser encaminhado e o roteador de recebimento soltará o pacote.

Qual mensagem ICMPv6 é enviada quando o campo de limite de salto IPv6 de um pacote é diminuído para zero e o pacote não pode ser encaminhado?

Tempo excedido

Tópico 7.1.0 - ICMPv6 usa o campo de limite de salto no cabeçalho do pacote IPv6 para determinar se o pacote expirou. Se o campo limite de salto atingir zero, um roteador enviará uma mensagem de tempo excedido de volta para a origem indicando que o roteador não pode encaminhar o pacote.

Qual mensagem é enviada por um host para verificar a exclusividade de um endereço IPv6 antes de usar esse endereço?

Solicitação de vizinho

Tópico 7.1.0 - No IPv6, a detecção de endereço duplicado (DAD) é usada no lugar do ARP. Um host IPv6 executa DAD enviando uma mensagem de solicitação de vizinho (NS) para seu próprio endereço IPv6 para garantir a exclusividade do endereço antes de usá-lo.

Qual protocolo é usado para pingtestar a conectividade entre hosts de rede?

ICMP

Tópico 7.1.0 - O Internet Control Message Protocol (ICMP) é usado para pingtestar a conectividade entre hosts de rede. O Protocolo de resolução de endereços (ARP) é usado para mapear endereços IP para endereços MAC. O protocolo DHCP (Dynamic Host Configuration Protocol) é usado para atribuir dinamicamente endereços IP aos hosts de rede. O protocolo de controle de transmissão (TCP) é considerado um protocolo confiável que segmenta os dados da camada de aplicação em segmentos para transmissão.

Um usuário emite umping 2001:db8:3040:114::88 comando e recebe uma resposta que inclui um código de 3. O que esse código representa?

Porta inacessível

Tópico 7.1.0 -

Quando um host ou um gateway recebe um pacote que não pode entregar, ele pode usar uma mensagem ICMP de destino inalcançável para notificar à origem que o destino ou o serviço está inalcançável. A mensagem conterá um código que indica por que não foi possível entregar o pacote. Estes são alguns dos códigos de destino inacessível para ICMPv4:

0 : net unreachable

1 : host unreachable

2 : protocol unreachable

3 : port unreachable

Um usuário emite um comando ping 192.168.219.8 e recebe uma resposta que inclui um código de 0. O que esse código representa?

Rede inacessível

Tópico 7.1.0 -

Quando um host ou um gateway recebe um pacote que não pode entregar, ele pode usar uma mensagem ICMP de destino inalcançável para notificar à origem que o destino ou o serviço está inalcançável. A mensagem conterá um código que indica por que não foi possível entregar o pacote. Estes são alguns dos códigos de destino inacessível para ICMPv4:

0 : net unreachable

1 : host unreachable

2 : protocol unreachable

3 : port unreachable

O que caracteriza um utilitário traceroute?

Ele identifica os roteadores no caminho de um host de origem para um host de destino

Tópico 7.2.0 - Traceroute é um utilitário que gera uma lista de saltos (ou roteadores) ao longo do caminho de um host de origem para o host de destino.

Por que um gerente precisaria usar o tracert comando?

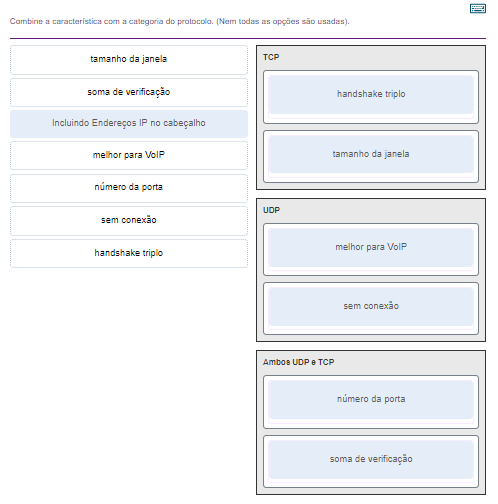
Para exibir uma lista das interfaces do lado do roteador entre o dispositivo de origem e o dispositivo de destino

Tópico 7.2.0 - Tracert é um utilitário que gera uma lista de saltos que foram alcançados com sucesso ao longo do caminho. Essa lista pode dar informações importantes para a verificação e a solução de problemas.Se os dados chegarem ao destino, o rastreamento listará a interface de cada roteador no caminho entre os hosts. Caso ocorra falha nos dados em algum salto ao longo do caminho, o endereço do último roteador que respondeu ao rastreamento poderá fornecer uma indicação de onde está o problema ou das restrições de segurança que foram encontradas.

Qual protocolo oferece suporte à configuração automática de endereço sem estado (SLAAC) para atribuição dinâmica de endereços IPv6 a um host?

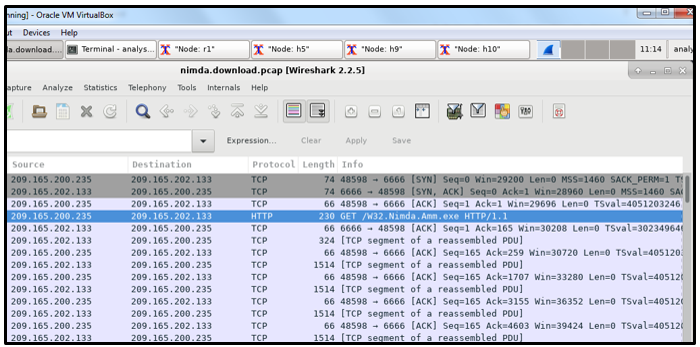
ICMPv6

Tópico 7.1.0 - SLAAC usa mensagens ICMPv6 ao atribuir dinamicamente um endereço IPv6 a um host.DHCPv6 é um método alternativo de atribuição de endereços IPv6 a um host.O ARPv6 não existe. O Neighbour Discovery Protocol (NDP) fornece a funcionalidade do ARP para redes IPv6.UDP é o protocolo da camada de transporte usado porDHCPv6.



Como a varredura de rede ajuda a avaliar a segurança das operações?

Consulte a figura. Um analista de segurança de rede está examinando dados capturados usando Wireshark. Os quadros capturados indicam que um host está baixando malware de um servidor. Qual porta de origem é usada pelo host para solicitar o download?



49598

Quais são as três responsabilidades da camada de transporte? (Escolha três.)

identificando os aplicativos e serviços no cliente e servidor que devem lidar com os dados transmitidos

atender aos requisitos de confiabilidade das aplicações, se houver

multiplexar vários fluxos de comunicação de muitos usuários ou aplicativos na mesma rede

Qual é o resultado de um ataque de envenenamento por ARP?

As informações do cliente são roubadas.

Um analista de segurança cibernética acredita que um invasor está falsificando o endereço MAC do gateway padrão para executar um ataque man-in-the-middle. Qual comando o analista deve usar para exibir o endereço MAC que um host está usando para acessar o gateway padrão?

Arp –a

Um usuário envia uma solicitação HTTP para um servidor Web em uma rede remota. Durante o encapsulamento da solicitação, quais informações são adicionadas ao campo de endereço de um quadro para indicar o destino?

o endereço MAC do gateway padrão

Que tipo de informação contém uma tabela ARP?

Endereço IP para mapeamentos de endereço MAC

Um administrador de rede está testando a conectividade de rede emitindo o comando ping em um roteador. Qual símbolo será exibido para indicar que um tempo expirou durante a espera de uma mensagem de resposta de eco ICMP?

Ponto (.)

Um usuário está executando um comando tracert para um dispositivo remoto. Em que ponto um roteador, que está no caminho para o dispositivo destino, para de encaminhar o pacote?

quando o valor no campo TTL chega a zero

Qual mecanismo é usado por um roteador para impedir que um pacote IPv4 recebido viaje infinitamente em uma rede?

Ele decrementa o valor do campo TTL em 1 e se o resultado for 0, descarta o pacote e envia uma mensagem Time Exceeded para o host de origem.

Um usuário que não pode se conectar ao servidor de arquivos entra em contato com o help desk. O técnico do help desk solicita que o usuário faça ping no endereço IP do gateway padrão configurado na estação de trabalho. Qual é o propósito deste comando ping ?

testar se o host é capaz de acessar hosts em outras redes

Em qual camada OSI é um endereço MAC de origem adicionado a uma PDU durante o processo de encapsulamento?

Camada de enlace de dados

O que é feito com um pacote IP antes de ser transmitido por um meio físico?

É encapsulado por um quadro da camada 2

Que PDU é processada quando um host está desencapsulando uma mensagem na camada de transporte do modelo TCP/IP?

Segmento

Que tipo de transmissão é usada para transmitir um único fluxo de vídeo, como uma videoconferência baseada na web, para um número selecionado de usuários?

Multicast

O que é uma descrição de uma transferência de zona DNS?

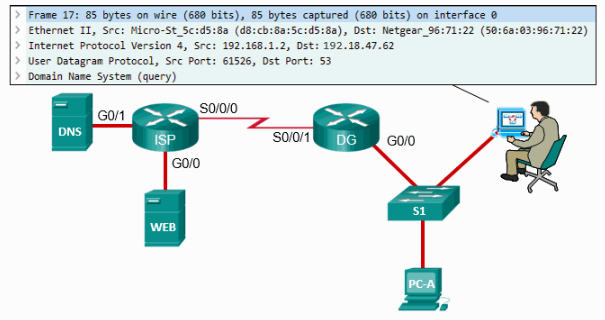
transferir blocos de dados DNS de um servidor DNS para outro servidor

Como um DHCPDISCOVER é transmitido em uma rede para chegar a um servidor DHCP?

Uma mensagem DHCPDISCOVER é enviada com o endereço IP de difusão como o endereço de destino.

Qual serviço de rede usa o protocolo WHOIS?

DNS



Consulte a figura. Um analista de segurança cibernética está visualizando pacotes capturados encaminhados no switch S1. Qual dispositivo tem o endereço MAC 50:6 a: 03:96:71:22?

Roteador DG

Qual protocolo é um protocolo de compartilhamento de arquivos cliente/servidor e também um protocolo de solicitação/resposta?

SMB

Quais são os três intervalos de endereços IP que são reservados para uso interno privado? (Escolha três.)

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

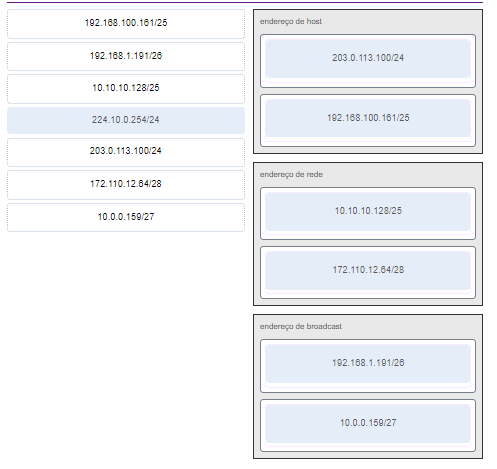
Qual é a forma descompactada completa do endereço IPv6 2001:420:59:0:1::a/64?

2001:0420:0059:0000:0001:0000:0000:000a

Quais são os dois tamanhos (mínimo e máximo) de um quadro Ethernet? (Escolha duas.)

64 a 1518

Corresponder cada endereço IPv4 à categoria de endereço apropriada. (Nem todas as opções são usadas.)



Que ação um switch Ethernet executa quando recebe um quadro com um endereço de origem de Camada 2 desconhecido?

Ele registra o endereço de origem na tabela de endereços do switch

Qual característica descreve um cliente sem fio operando no modo ativo?

Deve conhecer o SSID para se conectar a um AP (Ponto de acesso)

Qual protocolo de roteamento é usado para trocar rotas entre provedores de serviços de Internet?

BGP

Em qual local de memória a tabela de roteamento de um roteador é mantida?

RAM

Pontos de acesso leves encaminham dados entre quais dois dispositivos na rede? (Escolha duas.)

Cliente sem fio

Um controlador de Lan sem fio

O que é uma característica do modo de descoberta passiva de WLAN?

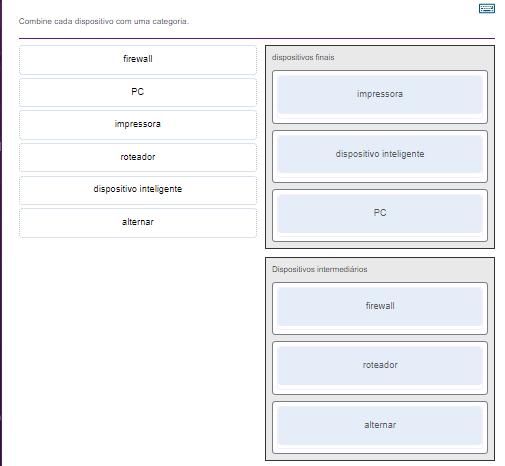
O AP envia periodicamente quadros de beacon contendo o SSID

Quais informações em um pacote de dados um roteador usa para tomar decisões de encaminhamento?

O endereço IP destino

Um roteador Cisco está executando o IOS 15. Quais são os dois tipos de entrada da tabela de roteamento que serão adicionados quando um administrador de rede ativar uma interface e atribuir um endereço IP a ela? (Escolha duas.)

* Interface conectada diretamente
* Interfaces de Rota local



Quais dois protocolos são protocolos de roteamento de estado de link? (Escolha duas.)

* OSPF
* ISIS

Qual é a característica de uma porta roteada configurada em um switch Cisco?

* É atribuído um endereço IP

O que é uma característica de um hub?

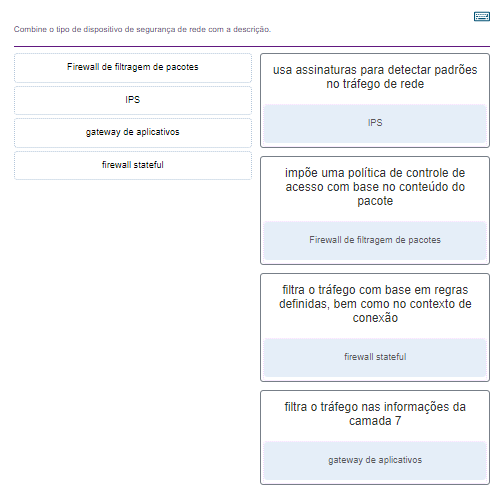
* Regenera os sinais recebios em uma porta fora todas as outros portas

Qual técnica é necessária para garantir uma transferência privada de dados usando uma VPN?

* Criptografia

Quais são as duas desvantagens de usar um IDS? (Escolha duas.)

* O ids não interrompe o trafego mal-intencionado
* O ids requer outros dispositivos para responder aos ataques



Qual componente AAA pode ser estabelecido usando cartões token?

* Autenticação

Quais são as duas afirmativas verdadeiras sobre servidores NTP em uma rede corporativa? (Escolha duas.)

* Os servidores ntp garanem um carimbo de data/hora preciso nas informações de registro e depuração

O que é um sistema de detecção de intrusões baseado em host (HIDS)?

* Ele combina as funcionalidades de aplicativos antimalware com proteção de firewall

Qual recurso do firewall é usado para assegurar que os pacotes recebidos em uma rede são respostas legítimas as requisições iniciadas pelos hosts internos?

* Inspeção de pacotes stateful (SPI)

Quais são os dois dispositivos facilmente encontrados na camada de acesso do modelo de design da LAN corporativa hierárquica? (Escolha duas.)

* Ponto de acesso
* Switch de camada 2

Qual é a função do SNMP?

* Fornece um formato de mensagem para comunicação entre gestores de dispositivos de rede e agentes

Qual é uma vantagem do HIPS que não é fornecida pela IDS?

* O HIPS protege recursos críticos do sistema e monitora os processos do sistema operacional

No processo de coleta de dados, que tipo de dispositivo aguardará tráfego, mas coletará apenas estatísticas de tráfego?

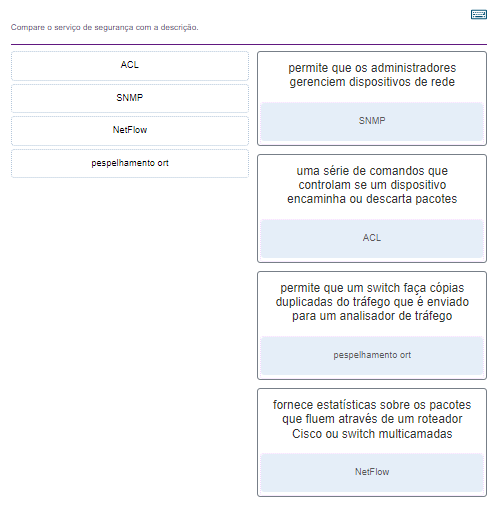
* Coletor do netflow

Qual é a função da camada de distribuição do modelo de projeto de rede de três camadas?

* Agregando conexõs da camada de acesso

Qual é o resultado do uso de dispositivos de segurança que incluem serviços de descriptografia e inspeção HTTPS?

* Os dispositivos introduzem atrasos de processamento e problemas de privacidade.



Módulo 18: Compreender o questionário de defesa

Como a BYOD (Bring Your Own Device) muda a maneira como as empresas implementam as redes?

Byod significa flexibilidade em onde e como os usuários acessam os recursos de rede

Tópico 18.2.0 - Um ambiente BYOD exige que uma organização acomode uma variedade de dispositivos e métodos de acesso. Dispositivos pessoais, que não estão sob o controle da empresa, podem ser aceitos e, portanto, segurança é um fator essencial. Os custos de hardware no local serão reduzidos, permitindo que a empresa priorize a disponibilização de ferramentas de colaboração e outros softwares para usuários BYOD.

Qual dispositivo geralmente é a primeira linha de defesa em uma abordagem em camadas de defesa em profundidade?

Rotador de borda

Tópico 18.1.0 - O roteador de borda conecta uma organização a um provedor de serviços. O roteador de borda tem um conjunto de regras que especificam qual tráfego é permitido ou negado.

Com a evolução das redes sem fronteiras, qual vegetal é agora usado para descrever uma abordagem de defesa em profundidade?

Alcachofra

Tópico 18.1.0 - A alcachofra agora é usada para fornecer uma analogia visual para descrever uma abordagem de segurança de defesa em profundidade. A cebola costumava ser descritiva porque o invasor “descascaria” cada camada dos mecanismos de defesa de rede. Agora, a alcachofra é usada porque uma única pétala ou folha pode ser movida ou removida para revelar informações sensíveis.

Que tipo de política empresarial estabelece as regras de conduta e as responsabilidades dos trabalhadores e dos empregadores?

As partes interessadas

Tópico 18.2.0 - As políticas de negócios definem uma linha de base de uso aceitável. As políticas da empresa estabelecem as regras e a conduta e as responsabilidades dos funcionários e do empregador. As políticas da empresa protegem os direitos dos trabalhadores, bem como os interesses comerciais da empresa.

Um administrador está preocupado em restringir quais aplicativos e usos de rede são aceitáveis para a organização. Qual componente de política de segurança o administrador usa para resolver essas preocupações?

Política de uso aceitável

Tópico 18.2.0 - A política de uso aceitável (AUP) identifica quais aplicativos de rede e usos são aceitáveis para uma organização.

Qual componente de uma política de segurança define explicitamente o tipo de tráfego permitido em uma rede e quais usuários podem ou não fazer?

Políticas de usos aceitáveis

Tópico 18.2.0 - As políticas de segurança especificam requisitos e fornecem uma linha de base para organizações. As políticas de segurança podem incluir o seguinte:

Políticas de identificação e autenticação que especificam indivíduos autorizados que têm acesso aos recursos de rede e procedimentos de verificação

Políticas de senha que garantem que os requisitos mínimos sejam atendidos e métodos de autenticação estão sendo aplicados e atualizados

Políticas de acesso remoto que identificam como os usuários remotos podem acessar uma rede e ao que eles têm permissão para se conectar

Políticas de uso aceitáveis que identificam aplicativos de rede e uso de rede que são permitidos na organização

Que dispositivo seria usado como a terceira linha de defesa em uma abordagem de defesa em profundidade?

Roteador interno

Tópico 18.1.0 - Em uma abordagem de defesa em profundidade, o roteador de borda formaria a primeira linha de defesa. O firewall seria a segunda linha de defesa seguida pelo roteador interno que compõem a terceira linha de defesa.

A laptop inside a house connects to a cloud. On the opposite side of the cloud a building connects.

Consulte a figura. A política de segurança de uma empresa permite que os funcionários se conectem à intranet do escritório de suas casas. Qual tipo de política de segurança é isso?

Acesso remoto

Tópico 18.2.0 - A seção de política de acesso remoto de uma política de segurança corporativa identifica como usuários remotos podem acessar uma rede e o que é acessível por meio de conectividade remota.

O que é uma característica de uma abordagem de segurança em camadas de defesa profunda?

O facasso de uma salvaguarda não afeta a eficácia as outras salvaguaras

Tópico 18.1.0 - Na abordagem de segurança em camadas de defesa em profundidade, as diferentes camadas trabalham juntas para criar uma arquitetura de segurança na qual a falha de uma salvaguarda não afeta a eficácia das outras salvaguardas.

Qual é uma prática recomendada de segurança BYOD?

Subscrever um serviço de localizador de dispositivos com a funcionalidade de limpeza remota

Tópico 18.2.0 - Uma das melhores práticas para dispositivos BYOD é assinar um serviço de localizador de dispositivos com recurso de apagamento remoto no caso de o dispositivo ser perdido ou roubado.

O que os regulamentos de conformidade de segurança definem?

Quais as organizações são responsáveis pelo fornecimento e a responsabilidade pelo incrumprimento

Tópico 18.2.0 - Os regulamentos de conformidade definem o que as organizações são responsáveis pelo fornecimento e o incumprimento de responsabilidade. Os regulamentos de conformidade que uma organização é obrigada a seguir serão diferentes de uma organização para a próxima, pois os regulamentos dependem do tipo de organização e dos dados que a organização manipula.

Que dispositivo seria usado como uma segunda linha de defesa em uma abordagem de defesa em profundidade?

Firewall

Tópico 18.1.0 - Em uma abordagem de defesa em profundidade, o roteador de borda formaria a primeira linha de defesa. O firewall seria a segunda linha de defesa seguida pelo roteador interno que compõem a terceira linha de defesa.

Quais duas áreas uma pessoa de segurança de TI deve entender para identificar vulnerabilidades em uma rede? (Escolha duas.)

Hardware usado por aplicativos

Aplicativos importantes usados

Tópico 18.1.0 - Para identificar vulnerabilidades de segurança, um especialista em segurança cibernética deve compreender os aplicativos que estão sendo usados e suas vulnerabilidades associadas, bem como o hardware usado.

Qual é o objetivo principal do Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST)?

para permitir que uma variedade de equipes de resposta a incidentes de segurança de computadores colabore, coopere e coordene o compartilhamento de informações, a prevenção de incidentes e as estratégias de reação rápida

Qual organização define identificadores CVE exclusivos para vulnerabilidades de segurança da informação publicamente conhecidas que facilitam o compartilhamento de dados?

Mitre

Qual é o principal objetivo da Plataforma de Compartilhamento de Informações de Malware (MISP)?

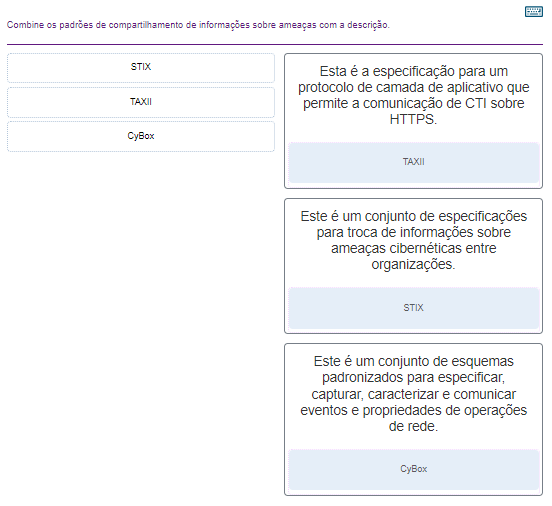
permitir o compartilhamento automatizado de COIs entre pessoas e máquinas usando o STIX e outros formatos de exportação

O que é CyBox?

É um conjunto de esquemas padronizados para especificar, capturar, caracterizar e comunicar eventos e propriedades de operações de rede.

Como o FireEye detecta e evita ataques de dia zero?

abordando todas as etapas de um ciclo de vida de ataque com um motor sem assinatura utilizando análise de ataque stateful



Qual é a função principal do Centro de Segurança da Internet (CIS)?

oferecer avisos e avisos de ameaça cibernética 24 horas-7, identificação de vulnerabilidades e respostas de mitigação e incidentes

Como o AIS aborda uma ameaça recém-descoberta?

ao permitir a troca em tempo real de indicadores de ameaças cibernéticas com os EUA Governo Federal e o setor privado

Qual é o propósito do software de gerenciamento de dispositivos móveis (MDM)?

Ele é usado para implementar políticas de segurança, configuração e configurações de software em dispositivos móveis

Qual é a característica de uma abordagem de segurança de defesa profunda em camadas?

Uma falha de salvaguarda não afeta a eficácia de outras salvaguardas.

Em uma abordagem de defesa em profundidade, quais três opções devem ser identificadas para defender com eficácia uma rede contra ataques? (Escolha três.)

Ativos que precisam de proteção

As vulnerabilidades no sistema

Ameaças aos ativos

Qual é a primeira linha de defesa quando uma organização está usando uma abordagem de defesa profunda para a segurança de rede?

Roteador de borda

Quais duas opções são as práticas recomendadas de segurança que ajudam a reduzir os riscos de BYOD? (Escolha duas.)

Mantenha o sistema operacional e o software atualizados.

Ligue apenas o Wi-Fi ao usar a rede sem fio.

Quais são os três objetivos que uma política de segurança BYOD realiza? (Escolha três.)

Identificar quais funcionários podem trazer seus próprios dispositivos

identificar salvaguardas a serem implementas se um dispositivo estiver comprometido

descrever os direitos de acesso e atividades permitidas ao pessoal de segurança no dispositivo

O que é uma característica da abordagem de segurança de alcachofra, defesa em profundidade?

Os agentes de ameaças não precisam mais descascar cada camada antes de atingir os dados ou o sistema alvo.

Qual é o benefício de uma abordagem de defesa em profundidade?

A eficácia de outras medidas de segurança não é afetada quando um mecanismo de segurança falha.

Quando uma auditoria de segurança é realizada em uma empresa, o auditor relata que os novos usuários têm acesso aos recursos da rede além de suas funções normais de trabalho. Além disso, os usuários que se deslocam para posições diferentes mantêm suas permissões anteriores. Que tipo de violação está ocorrendo?

O menor privilégio

Qual é o princípio por trás do modelo de controle de acesso não discricionário?

Permite que as decisões de acesso sejam baseadas em funções e responsabilidades de um usuário dentro da organização.

**O** modelo de controle de acesso não discricionário usou as funções e responsabilidades do usuário como base para as decisões de acesso.

Qual componente AAA pode ser estabelecido usando cartões token?

Autenticação

Ao projetar uma rede de protótipo para um novo farm de servidores, um designer de rede opta por usar links redundantes para se conectar ao restante da rede. Qual objetivo de negócios será abordado por esta escolha?

Disponibilidade

Que tipo de controle de acesso aplica o controle de acesso mais rigoroso e é comumente usado em aplicações militares ou de missão crítica?

Controle de acesso obrigatório (MAC)

Qual componente do modelo de segurança de confiança zero se concentra no acesso seguro quando uma API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo?

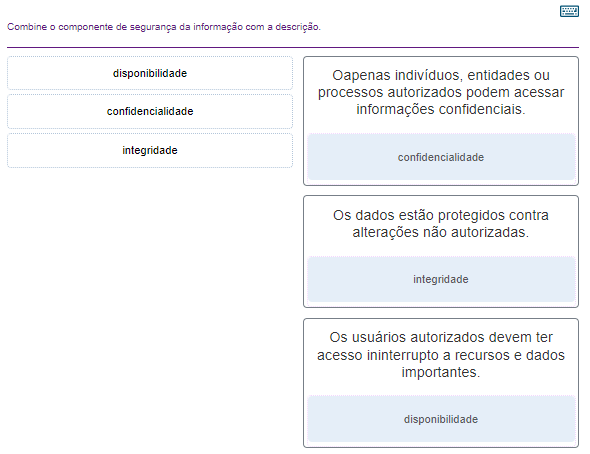
carga de trabalho

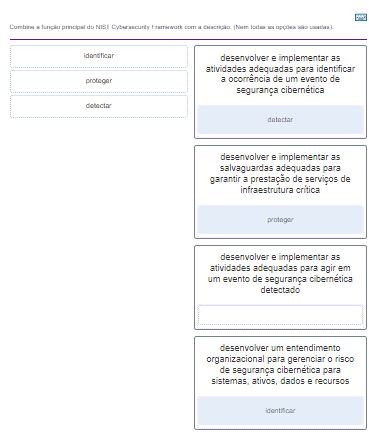
Senhas, frases secretas e PINs são exemplos de qual termo de segurança?

Autenticação

Qual é a finalidade da função de contabilidade de segurança de rede?

para acompanhar as ações de um usuário





Quais são os três resultados do NIST Cybersecurity Framework identificar a função principal? (Escolha três.)

Avaliação de risco

Gerenciamento de ativos

Administração

Um analista de segurança cibernética está realizando uma avaliação CVSS em um ataque em que um link da Web foi enviado a vários funcionários. Uma vez clicado, um ataque interno foi lançado. Qual métrica do CVSS Base Metric Group é usada para documentar que o usuário precisou clicar no link para que o ataque ocorra?

Iteração do usuário

Nas avaliações de segurança de rede, que tipo de teste emprega software para verificar redes internas e servidores voltados para a Internet em busca de vários tipos de vulnerabilidades?

Avaliação de vulnerabilidade

Quais duas classes de métricas estão incluídas no CVSS Base Metric Group? (Escolha duas.)

Métricas de impacto

Explorabiidade

Qual plano de gerenciamento de segurança especifica um componente que envolve o rastreamento da localização e configuração de dispositivos e software em rede em uma empresa?

Gerenciamento de ativos

Em que ordem as etapas do ciclo de vida do gerenciamento de vulnerabilidades são conduzidas?

 **descobrir, priorizar ativos, avaliar, relatar, corrigir, verificar**

Ao abordar um risco identificado, qual estratégia visa parar de realizar as atividades que criam risco?

Prevenção de riscos

O que é uma ação que deve ser executada na etapa de descoberta do ciclo de vida do gerenciamento de vulnerabilidades?

Desenvolve uma base de rede

Uma empresa está desenvolvendo uma política de segurança para comunicação segura. Na troca de mensagens críticas entre uma sede e uma filial, um valor hash só deve ser recalculado com um código predeterminado, garantindo assim a validade da fonte de dados. Qual aspecto das comunicações seguras é abordado?

Autenticação de origem

De que tipo de ataque o uso de HMACs protege?

Man-in-the-Middle

Qual é a diferença entre algoritmos de criptografia simétricos e assimétricos?

Algoritmos de criptografia simétricos usam chaves pré-compartilhadas. Algoritmos de criptografia assimétricos usam chaves diferentes para criptografar e descriptografar dados.

Qual é a finalidade de um certificado digital?

Ele autentica um site e estabelece uma conexão segura para trocar dados confidenciais.

Qual tecnologia tem a função de usar protocolos confiáveis de terceiros para emitir credenciais que são aceitas como uma identidade autorizada?

Certificados PKI

Uma empresa implementa uma política de segurança que garante que um arquivo enviado do escritório da sede para a filial só possa ser aberto com um código predeterminado. Este código é alterado todos os dias. Quais dois algoritmos podem ser usados para alcançar essa tarefa? (Escolha duas.)

AES

3DES

Qual objetivo das comunicações seguras é alcançado com a criptografia de dados?

Confidencialidade

Qual é o propósito do algoritmo DH?

para gerar um segredo compartilhado entre dois hosts que não se comunicaram antes

O que é a lista negra?

Esta é uma lista de aplicativos que pode ditar quais aplicativos do usuário não podem ser executados em um computador.

Um profissional de segurança está fazendo recomendações a uma empresa para melhorar a segurança de terminais. Qual tecnologia de endpoint de segurança seria recomendada como um sistema baseado em agentes para proteger hosts contra malware?

* AS COVAS

Qual declaração descreve o termo iptables?

É um aplicativo de firewall baseado em regras no Linux.

O que a função de telemetria fornece no software de segurança baseado em host?

Ele permite que programas de segurança baseados em host tenham funções de registro abrangentes.

Qual instrução descreve o Cisco Threat Grid Glivebox?

É um produto sandbox para analisar comportamentos de malware.

Qual é a diferença entre um HIDS e um firewall?

Um HIDS monitora os sistemas operacionais em computadores host e processa a atividade do sistema de arquivos. Os firewalls permitem ou negam o tráfego entre o computador e outros sistemas.

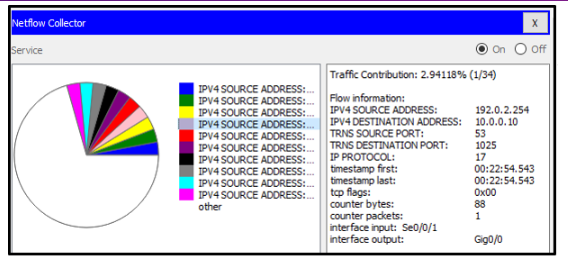
Em um host Windows, qual ferramenta pode ser usada para criar e manter listas negras e listas brancas?

Editor de Política de Grupo

Qual técnica poderia ser usada pelo pessoal de segurança para analisar um arquivo suspeito em um ambiente seguro?

SAndbox

Consulte a figura. Um administrador de rede está exibindo alguma saída no coletor de fluxo de rede. O que pode ser determinado a partir da saída do fluxo de tráfego mostrado?



Esta é uma resposta DNS UDP a uma maquina cliente

Um administrador do sistema executa um utilitário de verificação de arquivos em um PC Windows e observa um arquivo lsass.exe no diretório Arquivos de programas. O que o administrador deve fazer?

Exclua o arquivo porque ele provavelmente é malware

Quais informações podem ser fornecidas pelo utilitário Cisco NetFlow?

Horários de uso de pico e roteamento de tráfego

Qual instrução descreve os dados de sessão nos logs de segurança?

É um regisro de uma conversa entre hosts de rede

Quais duas opções são as abordagens de monitoramento de segurança de rede que usam técnicas analíticas avançadas para analisar dados de telemetria de rede? (Escolha duas.)

NBA e NBAD

Quais duas funções são fornecidas pela camada de rede? (Escolha duas.)

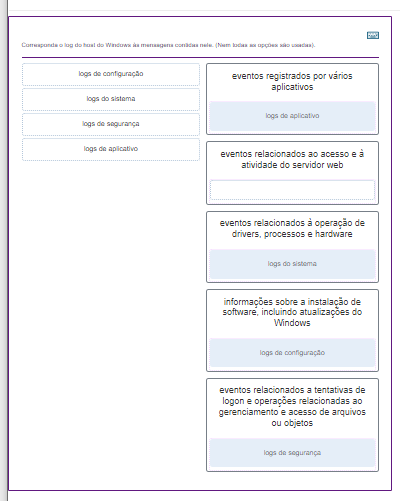
* fornecer aos dispositivos finais um identificador de rede exclusivo
* direcionar pacotes de dados para os hosts destino em outras redes

Qual instrução descreve um Cisco Web Security Appliance (WSA)?

Funciona como um proxy web

Qual appliance Cisco pode ser usado para filtrar o conteúdo do tráfego de rede para relatar e negar tráfego com base na reputação do servidor Web?

WSA



Em um sistema Cisco AVC, em qual módulo o NetFlow é implantado?

Coleta de métricas

O que indica se o carimbo de data/hora na seção HEADER de uma mensagem syslog é precedido por um símbolo de ponto ou asterisco?

Há um problema associado ao NTP

Qual função é fornecida pelo aplicativo Sguil?

Isso toma os alertas gerados por Snort legíveis e pesquisáveis

Quais duas ferramentas têm uma interface GUI e podem ser usadas para visualizar e analisar capturas completas de pacotes? (Escolha duas.)

Wireshark e Móulo de análise de rede cisco prime

Qual tipo de mensagem ICMP deve ser interrompida na entrada?

echo

Que tipo de ataque é realizado por agentes de ameaça contra uma rede para determinar quais endereços IP, protocolos e portas são permitidos pelas ACLs?

reconhecimento

Quais duas tecnologias são usadas principalmente em redes ponto a ponto? (Escolha duas.)

Bitcoin e Bittorent

Qual técnica é necessária para garantir uma transferência privada de dados usando uma VPN?

Criptografia

O que é o Tor?

Uma plataforma de software e rede de hosts P2Pque funcionam como roteadores de internet

Como o IMAP pode ser uma ameaça à segurança para uma empresa?

Um email pode ser usado para trazer malware para um host

Qual tecnologia seria usada para criar os logs do servidor gerados por dispositivos de rede e revisados por uma pessoa de rede de nível básico que trabalha no turno noturno em um data center?

syslog

Que técnica um ator ameaçador usaria para disfarçar vestígios de uma exploração em curso?

Informaçõs de tempo corrompidos atacandoa infraestrutura NTP

Quais são os dois protocolos de camada de aplicação que gerenciam a troca de mensagens entre um cliente com um navegador da Web e um servidor da Web remoto? (Escolha duas.)

HTTP/HTTPS

Por que a tecnologia HTTPS adiciona complexidade ao monitoramento de segurança de rede?

HTTPS oculta o tráfego de dados por meio de criptografia de ponta a ponta

Qual método é usado por algum malware para transferir arquivos de hosts infectados para um host de ator de ameaça?

Tuneis ICMP

Qual abordagem se destina a evitar explorações que direcionam o syslog?

Use syslog-ng

Qual protocolo é explorado por cibercriminosos que criam iFrames maliciosos?

HTTP

Qual HIDS está integrado ao Security Onion e usa regras para detectar alterações nos parâmetros operacionais baseados em host causadas por malware através de chamadas do sistema?

OSSEC

Qual é o propósito para a normalização dos dados?

Para simplificar a pesquisa de eventos correlacionados

Qual é o objetivo da redução de dados no que diz respeito ao NSM?

Para diminuir a quantidade de dados NSM a serem tratados

Que tipo de eventos devem ser atribuídos a categorias em Sguil?

Positivo real

Qual termo é usado para descrever o processo de conversão de entradas de log em um formato comum?

Normalização

Como o valor de hash dos arquivos é útil em investigações de segurança de rede?

Ele ajuda a identificar assinaturas de malware

Qual ferramenta é um sistema integrado de detecção de intrusões baseado em host Security Onion?

OSSEC

Qual ferramenta incluída no Security Onion fornece uma interface visual para os dados do NSM?

Squert

Qual elemento de meta-característica no Modelo Diamond descreve as informações obtidas pelo adversário?

resultados

Qual é o objetivo do agente da ameaça em estabelecer um canal de comunicação bidirecional entre o sistema alvo e uma infraestrutura CNC?

Para permitir que o agente de ameaça emita comandos para o software que está instalado no destino

Um agente de ameaça coleta informações de servidores Web de uma organização e pesquisa informações de contato do funcionário. As informações coletadas são usadas para pesquisar informações pessoais na Internet. A que fase de ataque essas atividades pertencem de acordo com o modelo Cyber Kill Chain?

reconhecimento

O que é definido no SOP de uma capacidade de resposta a incidentes de segurança de computador (CSIRC)?

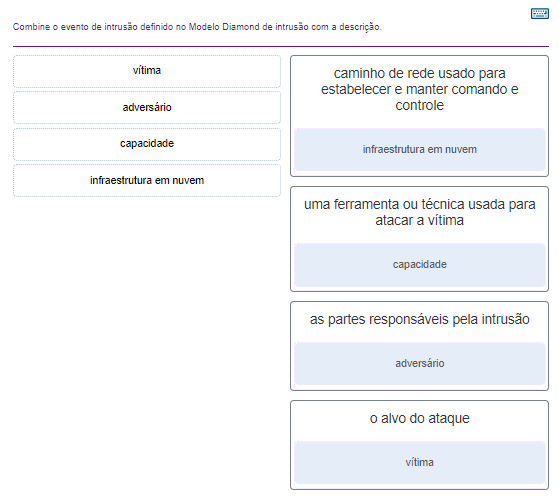
Os procedimentos que são seguidos durante uma resposta a incidentes

Em que etapa do processo de resposta a incidentes do NIST o CSIRT realiza uma análise para determinar quais redes, sistemas ou aplicativos são afetados; quem ou o que originou o incidente e como o incidente está ocorrendo?

escopo

De acordo com os padrões do NIST, qual participante da resposta a incidentes é responsável por coordenar uma resposta a incidentes com outras partes interessadas para minimizar os danos de um incidente?

Gerenciamento de wan



Em que fase do ciclo de vida de resposta a incidentes do NIST são coletadas evidências que podem ajudar as investigações subsequentes por parte das autoridades?

Contenção, erradicação e recuperação

Quais duas fontes compartilhadas de informação estão incluídas no framework MITRE ATT&CK? (Escolha duas.)

Táticas, técnicas e procedimentos do atacante

Mapeando os passos em um ataque para uma matriz de táticas generalizadas

A qual pessoal em um SOC é atribuída a tarefa de verificar se um alerta disparado pelo software de monitoramento representa um verdadeiro incidente de segurança?

Pessoal de nível 1

Qual classificação indica que um alerta é verificado como um incidente de segurança real?

Positivo real

O que é indicado por um ID de assinatura Snort que está abaixo de 3464?

O sid foi criado pelo sourcefire e distribuído sob um acordo gpl

Que informações estão contidas na seção de opções de uma regra Snort?

Texto descrevendo o evento

Um agente de ameaça violou com êxito o firewall de rede sem ser detectado pelo sistema IDS. Que condição descreve a falta de alerta?

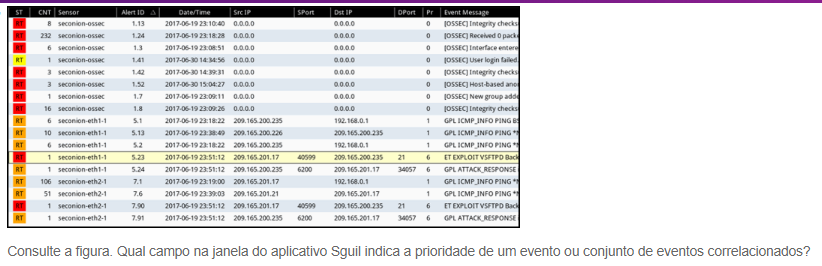
Falso negativo

Depois que uma ferramenta de monitoramento de segurança identifica um anexo de malware entrando na rede, qual é o benefício de realizar uma análise retrospectiva?

Uma análise retrospectiva pode ajuar a rastrear o comportamento do malware a partir do ponto de identificação

Um administrador de rede está tentando baixar um arquivo válido de um servidor interno. No entanto, o processo aciona um alerta em uma ferramenta NMS. Qual condição descreve este alerta?

Falso positivo



st

O que é indicado por uma verdadeira classificação de alerta de segurança negativa?

O tráfego normal é corretamente ignorado e alertas errôneos não estão sendo emitidos

**1. Quando o relatório em tempo real de eventos de segurança de várias fontes está sendo recebido, qual função no SIEM fornece captura e processamento de dados em um formato comum?**

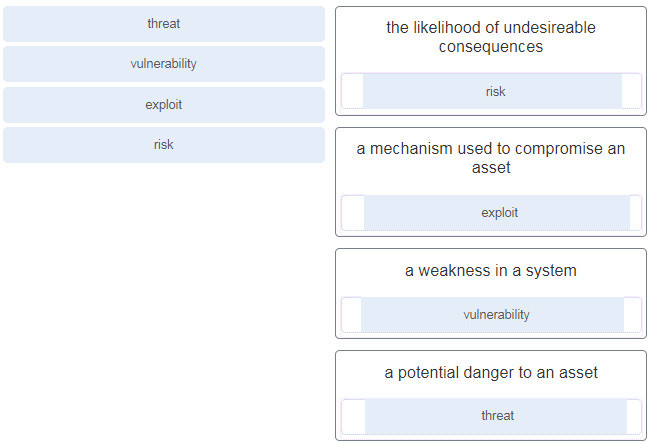
* coleção de log
* **A normalização**
* a agregação
* A conformidade

**2. Qual é o valor dos hashes de arquivos para investigações de segurança de rede?**

* Eles garantem a disponibilidade de dados.
* Eles garantem o não-repúdio.
* Eles oferecem confidencialidade.
* **Eles podem servir como assinaturas de malware.**

**3. Qual tecnologia é um sistema SIEM de código aberto?**

* StealthWatch (Verida)
* **ELK (A)**
* Splunk (pebê)
* Wireshark (a)

**4. Combine o conceito de segurança com a descrição.**   


**5. Quais são os dois componentes importantes de uma infraestrutura de chave pública (PKI) usada na segurança de rede? (Escolha dois.)**

* sistema de prevenção de intrusão
* **certificados digitais**
* Algoritmos de criptografia simétrica
* **Autoridade de certificação**
* geração de chave pré-compartilhada

**Uma** infraestrutura de chave pública usa certificados digitais e autoridades de certificação para gerenciar a distribuição de chaves assimétricas. Os certificados PKI são informação pública. A autoridade de certificação PKI (CA) é um terceiro confiável que emite o certificado. A CA tem seu próprio certificado (certificado auto-assinado) que contém a chave pública da CA.

**6. Quais são os três algoritmos projetados para gerar e verificar assinaturas digitais? (Escolha três.)**

* 3DES em
* IKE (IKE)
* **DSA (A.)**
* AES em
* **O ECDSA**
* **RSA em**

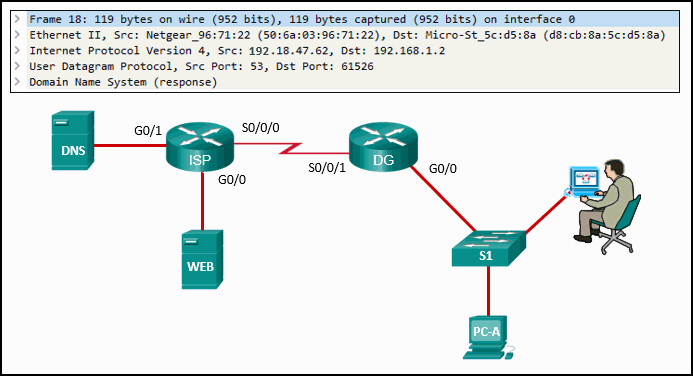
**Existem** três algoritmos de Padrão de Assinatura Digital (DSS) que são usados para gerar e verificar assinaturas digitais:   
Algoritmo de Assinatura Digital (DSA)   
Rivest-Shamir Adelman Algoritmo (RSA)   
Algoritmo de Assinatura Digital da Curva Elíptica (ECDSA)

**7. Qual seção de uma política de segurança é usada para especificar que apenas indivíduos autorizados devem ter acesso a dados corporativos?**

* Declaração de autoridade
* **Política de identificação e autenticação**
* política de acesso ao campus
* Política de acesso à Internet
* Declaração de âmbito
* Política de uso aceitável

**A** seção de política de identificação e autenticação da política de segurança normalmente especifica pessoas autorizadas que podem ter acesso a recursos de rede e procedimentos de verificação de identidade.

**8 - O que se refere. Consulte a exposição. Um analista de segurança cibernética está vendo pacotes capturados encaminhados no switch S1. Qual dispositivo tem o endereço MAC d8:cb:8a:5c:d5:8a?**



* **PC-A**
* Servidor de DNS
* Servidor web
* router DG
* router ISP

**Explicação:** A captura do Wireshark é uma resposta DNS do servidor DNS para PC-A. Como o pacote foi capturado na LAN em que o PC está, o roteador DG teria encapsulado o pacote de resposta do roteador ISP em um quadro Ethernet endereçado ao PC-A e encaminhado o quadro com o endereço MAC do PC-A como destino.

**9. Que tipo de mensagem é enviada por um cliente DHCPv4 solicitando um endereço IP?**

* **Mensagem de transmissão** **DHCPDISCOVER**
* Mensagem unicast DHCPDISCOVER
* Mensagem unicast de DHCPOFFER
* Mensagem unicast DHCPACK

**Quando** o cliente DHCPv4 solicita um endereço IP, ele envia uma mensagem de transmissão DHCPDISCOVER buscando um servidor DHCPv4 na rede.

**10. Coloque a prioridade de coleta de evidências da maioria volátil para menos volátil, conforme definido pelas diretrizes do IETF.**   


**11. Quais dois protocolos estão associados à camada de transporte? (Escolha dois.)**

* ICMP (PIMP)
* IP
* **UDP (PID)**
* PPP (PIP)
* **TCP ()**

**O** TCP e o UDP residem na camada de transporte nos modelos OSI e TCP/IP.

**12 - O que se é. Um administrador de rede está criando um perfil de rede para gerar uma linha de base de rede. O que está incluído no elemento de espaço de endereço de ativo crítico?**

* o tempo entre o estabelecimento de um fluxo de dados e sua terminação
* os daemons TCP e UDP e portas que podem ser abertas no servidor
* **os endereços IP ou a localização lógica dos sistemas ou dados essenciais**
* a lista de processos TCP ou UDP disponíveis para aceitar dados

**Explanation:**Um perfil de rede deve incluir alguns elementos importantes, como o seguinte:   
Taxa total – a quantidade de dados que passam de uma determinada fonte para um determinado destino em um determinado período de tempo   
Sessão duratio n – o tempo entre o estabelecimento de um fluxo de dados e sua terminação   
Portas usadas – uma lista de processos TCP ou UDP que estão disponíveis para aceitar dados   
Espaço crítico de endereço de ativo – os endereços IP ou a localização lógica de sistemas ou dados essenciais

**13 - O que se (com um and). Quais são as três métricas de impacto contidas no Grupo Métrica Base do CVSS 3.0? (Escolha três.)**

* **a confidencialidade**
* Nível de remediação
* **Integridade**
* vector de ataque
* Explorar
* **Disponibilidade**

**Explicação:**   
O Common Vulnerability Scoring System (CVSS) é uma estrutura aberta neutra em relação ao fornecedor, padrão da indústria, para pesar os riscos de uma vulnerabilidade usando uma variedade de métricas. O CVSS usa três grupos de métricas para avaliar a vulnerabilidade, o Grupo de Métrica Base, o Grupo Métrica Temporal e o Grupo Métrico Ambiental. O Grupo Base Métrico tem duas classes de métricas (exploração e impacto). As métricas de impacto estão enraizadas nas seguintes áreas: confidencialidade, integridade e disponibilidade.

**14. O que é uma característica do DNS?**

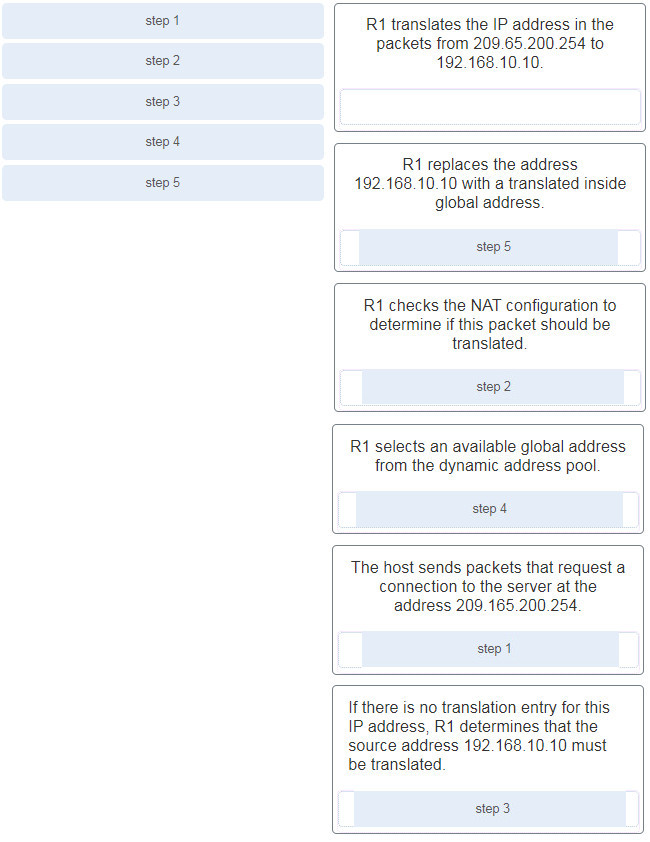
* **Os servidores DNS podem armazenar em cache consultas recentes para reduzir o tráfego de consulta DNS.**
* Todos os servidores DNS devem manter mapeamentos para toda a estrutura DNS.
* Os servidores DNS são programados para enviar solicitações de tradução de nomes que não estejam dentro de sua zona.
* O DNS depende de uma topologia hub-and-spoke com servidores centralizados.

**Explicação:** DNS usa uma hierarquia para servidores descentralizados para executar a resolução de nomes. Os servidores DNS mantêm apenas registros para sua zona e podem armazenar em cache consultas recentes para que futuras consultas não produzam tráfego DNS excessivo.

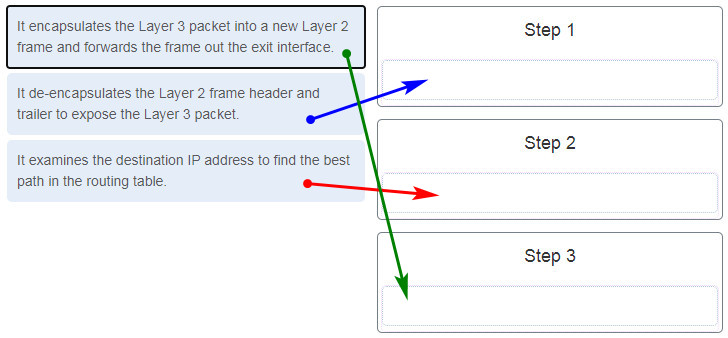
**15. Quais são as duas diferenças entre HTTP e HTTP/2? (Escolha dois.)**

* **O HTTP/2 usa um cabeçalho comprimido para reduzir os requisitos de largura de banda.**
* **O HTTP/2 usa multiplexing para suportar vários fluxos e aumentar a eficiência.**
* O HTTP/2 usa códigos de status diferentes do que o HTTP para melhorar o desempenho.
* HTTP/2 emite solicitações usando um formato de texto, enquanto HTTP usa comandos binários.
* O HTTP tem um formato de cabeçalho diferente do que o HTTP/2 tem.

**O** objetivo do HTTP/2 é melhorar o desempenho do HTTP, abordando os problemas de latência do HTTP. Isso é realizado usando recursos como multiplexação, push do servidor, código binário e compressão de cabeçalho.

**16. Combine as etapas com as ações envolvidas quando um host interno com endereço IP 192.168.10.10 tenta enviar um pacote para um servidor externo no endereço IP 209.165.200.254 em um roteador R1 que está executando NAT dinâmico. (Nem todas as opções são usadas.)**   


**Explicação:** A tradução dos endereços IP de 209.65.200.254 a 192.168.10.10 será realizada quando a resposta voltar do servidor.

**17 - Sim. Um roteador recebeu um pacote destinado a uma rede que está na tabela de roteamento. Quais etapas o roteador executa para enviar esse pacote em seu caminho? Corresponder a etapa à tarefa realizada pelo roteador.**   


**18. Quais são duas características compartilhadas do IDS e do IPS? (Escolha dois.)**

* Ambos têm um impacto mínimo no desempenho da rede.​
* **Ambos são implantados como sensores.**
* Ambos analisam cópias do tráfego de rede.
* **Ambos usam assinaturas para detectar tráfego malicioso.**
* Ambos dependem de um dispositivo de rede adicional para responder ao tráfego malicioso.

**Explicação:** Tanto o IDS quanto o IPS são implantados como sensores e usam assinaturas para detectar tráfego malicioso. O IDS analisa cópias do tráfego de rede, o que resulta em um impacto mínimo no desempenho da rede. O IDS também depende de um IPS para impedir o tráfego malicioso. ​​

**19. Qual declaração descreve uma política de segurança típica para uma configuração de firewall DMZ?**

* **O tráfego que se origina da interface DMZ é seletivamente permitido para a interface externa.**
* O tráfego de retorno do interior associado ao tráfego proveniente do exterior é permitido atravessar da interface interna para a interface externa.
* O tráfego de retorno do exterior associado ao tráfego proveniente do interior é permitido atravessar da interface externa para a interface DMZ.
* O tráfego que se origina da interface interna é geralmente bloqueado total ou muito seletivamente permitido para a interface externa.
* O tráfego que se origina da interface externa é permitido atravessar o firewall para a interface interna com poucas ou nenhumas restrições.

**Explicação:**   
Com um design de firewall de três interfaces com conexões internas, externas e DMZ, as configurações típicas incluem o seguinte:   
O tráfego proveniente de DMZ destinado à rede interna é normalmente bloqueado.   
O tráfego proveniente da DMZ destinado a redes externas é normalmente permitido com base em quais serviços estão sendo usados na DMZ.   
O tráfego proveniente da rede interna destinado a partir da DMZ é normalmente inspecionado e autorizado a retornar.   
O tráfego proveniente de redes externas (a rede pública) é normalmente permitido na DMZ apenas para serviços específicos.

**20 anos. Após reclamações dos usuários, um técnico identifica que o servidor web da faculdade está funcionando muito lentamente. Uma verificação do servidor revela que há um número excepcionalmente grande de solicitações TCP provenientes de vários locais na Internet. Qual é a origem do problema?**

* O servidor está infectado com um vírus.
* **Um ataque DDoS está em andamento.**
* Não há largura de banda suficiente para se conectar ao servidor.
* Há um ataque de repetição em andamento.

**Explicação:** A fonte do problema não pode ser um vírus porque nesta situação o servidor é passivo e na extremidade receptora do ataque. Um ataque de repetição usa dados interceptados e gravados em uma tentativa de obter acesso a um servidor não autorizado. Este tipo de ataque não envolve vários computadores. O problema não é a largura de banda disponível, mas o número de conexões TCP que ocorrem. Receber um grande número de conexões de vários locais é o principal sintoma de um ataque distribuído de negação de serviço que usa botnets ou computadores zumbis.

**21 - Quais duas declarações descrevem os ataques de acesso? (Escolha dois.)**

* **Os ataques de senha podem ser implementados pelo uso de métodos de ataque de força bruta, cavalos de Tróia ou sniffers de pacotes.**
* Para detectar serviços de escuta, os ataques de varredura de porta verificam um intervalo de números de porta TCP ou UDP em um host.
* Os ataques de redirecionamento de porta usam uma placa de adaptador de rede no modo promíscuo para capturar todos os pacotes de rede que são enviados através de uma LAN.
* Os ataques de exploração de confiança geralmente envolvem o uso de um laptop para atuar como um ponto de acesso desonesto para capturar e copiar todo o tráfego de rede em um local público, como um hotspot sem fio.
* **Os ataques de estouro do buffer gravam dados além da memória de buffer alocada para substituir dados válidos ou para explorar sistemas para executar códigos maliciosos.**

**Um** ataque de acesso tenta obter acesso a um recurso usando uma conta sequestrada ou outros meios. Os cinco tipos de ataques de acesso incluem o seguinte:   
senha – um dicionário é usado para tentativas de login repetidas   
exploração de confiança – utiliza privilégios concedidos para aceder a material não autorizado   
Redirecionamento de porta – usa um host interno comprometido para passar o tráfego através de um firewall   
man-in-the-middle – um dispositivo não autorizado posicionado entre dois dispositivos legítimos, a fim de redirecionar ou capturar o tráfego   
buffer overflow – muitos dados enviados para um local de memória que já contém dados

**22 - Sim. Quais duas ações podem ser tomadas ao configurar o Windows Firewall? (Escolha dois.)**

* Ligue a triagem do porto.
* **Abra manualmente as portas necessárias para aplicações específicas.**
* **Permitir que um firewall de software diferente controle o acesso.**
* Habilite a autenticação de endereço MAC.
* Faça uma reversão.

**Quando** um firewall de software diferente é instalado, o Firewall do Windows deve ser desativado através do painel de controle do Windows Firewall. Quando o Firewall do Windows está ativado, portas específicas podem ser ativadas que são necessárias para aplicativos específicos.

**23 - Qual declaração descreve o estado das contas de administrador e de convidados depois que um usuário instala a versão da área de trabalho do Windows em um novo computador?**

* Por padrão, a conta de convidado está ativada, mas a conta de administrador está desativada.
* Por predefinição, tanto o administrador como as contas de convidado estão activadas.
* **Por predefinição, as contas de administrador e de convidado estão desativadas.**
* Por predefinição, a conta de administrador está activada, mas a conta de convidado está desactivada.

**Quando** um usuário instala a versão de desktop do Windows, duas contas de usuário locais são criadas automaticamente durante o processo, administrador e convidado. Ambas as contas estão desativadas por padrão.

**24. Qual é o objetivo de entrar no comando nslookup cisco.com em um PC com Windows?**

* **para verificar se o serviço DNS está em execução**
* para se conectar ao servidor Cisco
* para testar se o servidor Cisco está acessível
* para descobrir o tempo de transmissão necessário para chegar ao servidor Cisco

**Explicação:** O nslookupO comando consulta servidores DNS para descobrir o endereço IP ou os endereços associados ao nome de domínio cisco.com. Um resultado bem-sucedido indica que a configuração de DNS no PC é funcional e também indica o endereço IP para o nome de domínio que está sendo exibido. O comando não tenta conectar diretamente ao host Cisco real.

**25 - Como o ID do evento é atribuído no Sguil?**

* Todos os eventos da série de eventos correlacionados recebem o mesmo ID do evento.
* Somente o primeiro evento da série de eventos correlacionados é atribuído um ID exclusivo.
* Todos os eventos da série de eventos correlacionados recebem o mesmo ID do grupo de eventos.
* **Cada evento na série de eventos correlacionados é atribuído um ID exclusivo.**

**Explicação:** Em Sguil, cada evento recebe um ID de evento exclusivo, mas apenas o primeiro ID do evento na série de eventos correlacionados é exibido na guia RealTime.

**26 - Sim. Quais são os dois tipos de tráfego de rede de protocolos que geram muito tráfego de rotina? (Escolha dois.)**

* **routing atualiza o tráfego**
* Tráfego de auditoria de segurança do Windows
* Tráfego de IPsec
* **Tráfego do STP**
* Tráfego de SSL

**Explicação:** Para reduzir a enorme quantidade de dados coletados para que os analistas de segurança cibernética possam se concentrar em ameaças críticas, alguns dados menos importantes ou menos relevantes podem ser eliminados dos conjuntos de dados. Por exemplo, o tráfego de gerenciamento de rede de roteamento, como atualizações de roteamento e tráfego STP, pode ser eliminado.

**27 - Sim. Quais são dois elementos que formam o valor PRI em uma mensagem syslog? (Escolha dois.)**

* **Facilidade**
* carimbo de data/hora
* **gravidade**
* cabeçalho
* nome de host

**O** PRI em uma mensagem syslog consiste em dois elementos, a facilidade e a gravidade da mensagem.

**28 - Quais três informações são encontradas nos dados da sessão? (Escolha três.)**

* Endereço IP de gateway padrão
* **números de porta de origem e de destino**
* **Protocolo de transporte de camada 4**
* Endereços MAC de origem e destino
* nome de usuário
* **Endereços IP de origem e destino**

**Os** dados de sessão incluem informações de identificação, como endereços IP de origem e destino, números de portas de origem e destino e o protocolo Layer 4 em uso. Os dados de sessão não incluem o nome de usuário, os endereços MAC de origem e destino e um endereço IP de gateway padrão.

**29 - 29 - Reais. Que tipo de mensagem ICMP pode ser usada por agentes de ameaças para realizar ataques de reconhecimento e varredura de rede?**

* Resposta da máscara do ICMP
* Descoberta do roteador ICMP
* **ICMP inacessível**
* Redirecionamentos do ICMP

**Explicação:** As mensagens comuns de ICMP de interesse para os agentes de ameaças incluem:   
Pedido de eco ICMP e resposta de eco: usado para realizar a verificação do host e ataques DoS   
ICMP inacessível: usado para realizar reconhecimento de rede e ataques de varredura   
Resposta da máscara ICMP: usada para mapear uma rede IP interna   
Redirecionamentos ICMP: usado para atrair um host de destino para enviar todo o tráfego através de um dispositivo comprometido e criar um ataque man-in-the-middle   
Descoberta do roteador ICMP: usada para injetar entradas de rota falsas na tabela de roteamento de um host de destino

**30. Uma inundação de pacotes com endereços IP de origem inválida solicita uma conexão na rede. O servidor está ocupado tentando responder, resultando em solicitações válidas sendo ignoradas. Que tipo de ataque ocorreu?**

* Sequestro de sessão TCP
* **Inundante do TCP SYN**
* Redefinir TCP
* Inundante de UDP

**Explicação:** O ataque TCP SYN Flood explora o hands-way TCP de três vias. O agente de ameaças envia continuamente pacotes de solicitação de sessão TCP SYN com um endereço IP de origem falsificado aleatoriamente para um destino pretendido. O dispositivo de destino responde com um pacote TCP SYN-ACK para o endereço IP falsificado e aguarda um pacote TCP ACK. Essas respostas nunca chegam. Eventualmente, o host de destino é sobrecarregado com conexões TCP semi-abertas e nega serviços TCP.

**31 - Um invasor está redirecionando o tráfego para um gateway padrão falso na tentativa de interceptar o tráfego de dados de uma rede comuída. Que tipo de ataque poderia conseguir isso?**

* Túneis de DNS
* Inundante do TCP SYN
* **DHCP spoofing**
* Envenenamento do cache ARP

**Explicação:** Em ataques de falsificação de DHCP, um agente de ameaça configura um servidor DHCP falso na rede para emitir endereços DHCP para clientes com o objetivo de forçar os clientes a usar um gateway padrão falso ou inválido. Um ataque man-in-the-middle pode ser criado definindo o endereço de gateway padrão para o endereço IP do agente de ameaças.

**32 - Sim. Qual é o objetivo mais comum de envenenamento por otimização de mecanismos de pesquisa (SEO)?**

* **aumentar o tráfego da web para sites maliciosos**
* para construir uma botnet de zumbis
* para enganar alguém para instalar malware ou divulgar informações pessoais
* para sobrecarregar um dispositivo de rede com pacotes maliciosamente formados

**Um** usuário mal-intencionado pode criar um SEO para que um site malicioso apareça mais alto nos resultados de pesquisa. O site malicioso geralmente contém malware ou é usado para obter informações através de técnicas de engenharia social.

**33. Os usuários relatam que um arquivo de banco de dados no servidor principal não pode ser acessado. Um administrador de banco de dados verifica o problema e percebe que o arquivo de banco de dados agora está criptografado. A organização recebe um e-mail ameaçador exigindo pagamento para a descriptografia do arquivo de banco de dados. Que tipo de ataque a organização experimentou?**

* ataque man-in-the-middle
* Ataque do DoS
* **ransomware**
* Cavalo de Tróia

**Um** especialista em segurança cibernética precisa estar familiarizado com as características dos diferentes tipos de malware e ataques que ameaçam uma organização.

**34 - Sim. Ao lidar com uma ameaça de segurança e usar o modelo Cyber Kill Chain, quais duas abordagens uma organização pode usar para ajudar a bloquear possíveis explorações em um sistema? (Escolha dois.)**

* Coletar e-mail e web logs para reconstrução forense.
* Realize análise completa de malware.
* **Treine desenvolvedores web para proteger o código.**
* Construa detecções para o comportamento de armadores conhecidos.
* **Realizar testes regulares de varredura e penetração de vulnerabilidades.**

**Os** alvos de exploração mais comuns, uma vez que uma arma é entregue, são aplicações, vulnerabilidades do sistema operacional e contas de usuário. Entre outras medidas, como verificação regular de vulnerabilidades e testes de penetração, treinar desenvolvedores web na segurança de código pode ajudar a bloquear possíveis explorações em sistemas.

**35. Como os profissionais de TI corporativos podem lidar com ameaças cibernéticas baseadas em DNS?**

* Limite o número de navegadores abertos simultaneamente ou guias do navegador.
* **Monitore os logs do servidor de proxy DNS e procure consultas DNS incomuns.**
* Use dispositivos IPS/IDS para verificar o tráfego corporativo interno.
* Limite o número de consultas DNS permitidas na organização.

**Explicação:** consultas DNS para nomes de domínio gerados aleatoriamente ou subdomínios DNS de aparência aleatória extremamente longos devem ser consideradas suspeitas. Os ciberanalistas podem fazer o seguinte para ataques baseados em DNS:   
Analise os registros DNS.   
Use um serviço DNS passivo para bloquear solicitações para suspeita de CnC e explorar domínios.

**36 ('). Como o uso do HTTPS complica o monitoramento de segurança de rede?**

* **O HTTPS adiciona complexidade aos pacotes capturados.**
* O HTTPS não pode proteger os visitantes de um site fornecido pela empresa.
* O tráfego do navegador da Web é direcionado para servidores infectados.
* O HTTPS pode ser usado para se infiltrar em consultas DNS.

**Explicação:**   
O HTTPS adiciona sobrecarga extra ao pacote formado por HTTP. O HTTPS criptografa usando a camada de soquete segura (SSL). Mesmo que alguns dispositivos possam realizar descriptografia e inspeção SSL, isso pode apresentar problemas de processamento e privacidade. O HTTPS adiciona complexidade às capturas de pacotes devido à mensagem adicional envolvida no estabelecimento de uma conexão de dados criptografada.

**37 - Sim. Qual é a responsabilidade do departamento de recursos humanos ao lidar com um incidente de segurança?**

* Coordenar a resposta a incidentes com outras partes interessadas e minimizar os danos do incidente.
* Realizar ações para minimizar a eficácia do ataque e preservar evidências.
* **Aplicar medidas disciplinares se um incidente for causado por um funcionário.**
* Revise as políticas, planos e procedimentos de incidentes para violações de diretrizes locais ou federais.

**O** departamento de recursos humanos pode ser chamado a realizar medidas disciplinares se um incidente for causado por um funcionário.

**38 - O que se é! Como um sistema de gerenciamento de informações e eventos de segurança (SIEM) em um SOC ajuda o pessoal a combater ameaças à segurança?**

* integrando todos os dispositivos de segurança e aparelhos em uma organização
* Analisando os dados de registro em tempo real
* **Combinando dados de múltiplas tecnologias**
* Implementando dinamicamente regras de firewall

**Explanation:**Um sistema de gerenciamento de informações e eventos de segurança (SIEM) combina dados de várias fontes para ajudar o pessoal do SOC a coletar e filtrar dados, detectar e classificar ameaças, analisar e investigar ameaças e gerenciar recursos para implementar medidas preventivas.

**39. Em que camada OSI é um endereço IP de origem adicionado a um PDU durante o processo de encapsulamento?**

* **camada de rede**
* camada de transporte
* camada de link de dados
* camada de aplicação

**40. Qual é o objetivo do CSMA/CA?**

* para evitar loops
* para isolar o tráfego
* para filtrar o tráfego
* **para evitar colisões**

**Explanation:**CSMA/CA significa acesso múltiplo sentido do sensor de portador com a prevenção de colisão. É um mecanismo usado em redes sem fio para evitar que colisões de pacotes ocorram.

**41. Por que o DHCP é preferido para uso em redes grandes?**

* Os hosts em grandes redes exigem mais configurações de endereçamento IP do que hosts em pequenas redes.
* Impedi o compartilhamento de arquivos protegidos por direitos autorais.
* **É uma maneira mais eficiente de gerenciar endereços IP do que a atribuição de endereços estáticos.**
* As grandes redes enviam mais solicitações de domínio para resolução de endereços IP do que redes menores.
* O DHCP usa um protocolo de camada de transporte confiável.

**Explicação:** A atribuição de endereço IP estático requer que o pessoal configure cada host de rede com endereços manualmente. Grandes redes podem mudar com frequência e ter muito mais hosts para configurar do que pequenas redes. O DHCP fornece um meio muito mais eficiente de configurar e gerenciar endereços IP em redes grandes do que a atribuição de endereços estáticos.

**42 - O que se passa com que se é com o que dizer. Qual fase do ciclo de vida da resposta a incidentes do NIST inclui monitoramento contínuo pelo CSIRT para identificar e validar rapidamente um incidente?**

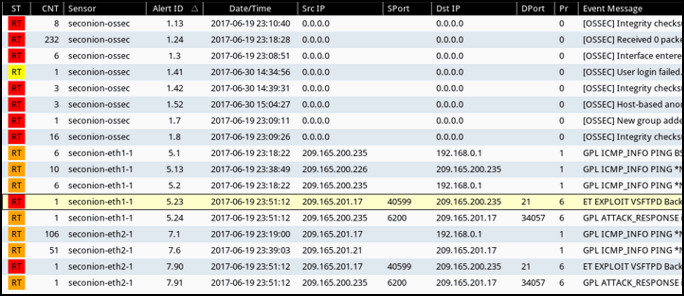
* Atividades de pós-incidente
* **Detecção e análise**
* contenção, erradicação e recuperação
* preparação

**Explicação:** Está na fase de detecção e análise do ciclo de vida da resposta a incidentes do NIST que o CSIRT identifica e valida incidentes por meio de monitoramento contínuo. O NIST define quatro etapas do ciclo de vida da resposta a incidentes.

**43 - Quais são dois problemas que podem ser causados por um grande número de mensagens de solicitação e resposta ARP? (Escolha dois.)**

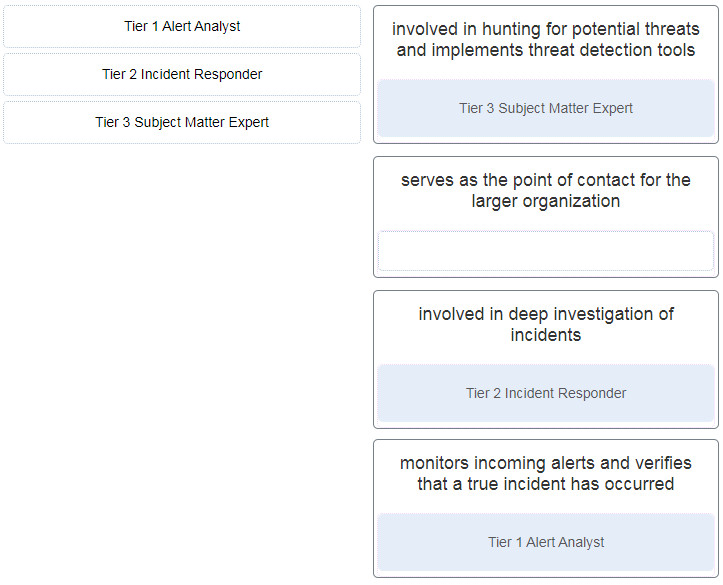
* **Todas as mensagens de solicitação ARP devem ser processadas por todos os nós na rede local.**
* Um grande número de mensagens de solicitação e resposta ARP pode retardar o processo de comutação, levando o switch a fazer muitas alterações em sua tabela MAC.
* A rede pode ficar sobrecarregada porque as mensagens de resposta do ARP têm uma carga útil muito grande devido ao endereço MAC de 48 bits e ao endereço IP de 32 bits que eles contêm.
* **A solicitação ARP é enviada como uma transmissão e inundará toda a sub-rede.**
* Os interruptores ficam sobrecarregados porque concentram todo o tráfego das sub-redes conectadas.

**Explicação:** **solicitações ARP são enviadas como transmissões:**   
(1) Todos os nós os receberão, e eles serão processados por software, interrompendo a CPU.   
(2) O interruptor para a frente (inundações) Transição da camada 2 para todas as portas.   
Uma opção não altera sua tabela MAC com base em mensagens de solicitação ou resposta ARP. O interruptor preenche a tabela MAC usando o endereço MAC de origem de todos os quadros. A carga útil ARP é muito pequena e não sobrecarrega o interruptor.

**44. Consulte a exposição. Qual campo na janela de aplicação Sguil indica a prioridade de um evento ou conjunto de eventos correlacionados?**   


* **ST (ST)**
* Alerta de identificação
* Pr em P
* CNT (CNT)

**Explicação:** A janela de aplicação Sguil tem vários campos disponíveis que fornecem informações sobre um evento. O campo ST dá o status de um evento que inclui uma prioridade codificada por cores de amarelo claro a vermelho para indicar quatro níveis de prioridade.

**45. Combine os títulos de trabalho com posições de pessoal SOC. (Nem todas as opções são usadas.)**   


* Analista de alerta de nível 1 **—** monitora os alertas de entrada e verifica se um incidente verdadeiro ocorreu
* Respondente de Incidente do Tier 2 **–** envolvido em investigação profunda de incidente
* Especialista em matéria de assunto de nível 3 **–** envolvido na caça de possíveis threads e implementa ferramentas de detecção de rosqueas
* (não usar) **– servir** como ponto de contato para o grande organitazion

**46 - Sim. Se o gateway padrão estiver configurado incorretamente no host, qual é o impacto nas comunicações?**

* O host não pode se comunicar na rede local.
* **O host pode se comunicar com outros hosts na rede local, mas não consegue se comunicar com hosts em redes remotas.**
* O host pode se comunicar com outros hosts em redes remotas, mas não consegue se comunicar com hosts na rede local.
* Não há impacto nas comunicações.

**Um** gateway padrão é necessário apenas para se comunicar com dispositivos onanother network. A ausência de um gateway padrão não afeta a conectividade entre dispositivos na mesma rede local

**47. Quando um protocolo sem conexão está em uso em uma camada inferior do modelo OSI, como os dados ausentes são detectados e retransmitidos, se necessário?**

* Os reconhecimentos sem conexão são usados para solicitar retransmissão.
* **Os protocolos orientados a conexão de camada superior acompanham os dados recebidos e podem solicitar a retransmissão dos protocolos de nível superior no host de envio.**
* Os protocolos IP da camada de rede gerenciam as sessões de comunicação se os serviços de transporte orientados a conexão não estiverem disponíveis.
* O processo de entrega de melhor esforço garante que todos os pacotes enviados são recebidos.

**Quando** os protocolos sem conexão estão em uso em uma camada inferior do modelo OSI, os protocolos de nível superior podem precisar trabalhar juntos nos hosts de envio e recebimento para contabilizar e retransmitir dados perdidos. Em alguns casos, isso não é necessário, porque para algumas aplicações uma certa quantidade de perda de dados é tolerável.

**48 - O que se é com o que é. O que é a notação de comprimento de prefixo para a máscara de sub-rede 255.255.255.224?**

* /25 em (em (
* /26 (em (em
* **/ 27 em (em 2**
* /28 em (em 2

**O** formato binário para 255.255.255.25224 é 1111111.111111.1111.111111.11.11.11.11100000. O comprimento do prefixo é o número de 1s consecutivos na máscara de sub-rede. Portanto, o comprimento do prefixo é /27.

**49. Qual ferramenta de monitoramento de rede salva quadros de rede capturados em arquivos PCAP?**

* NetFlow (AO)
* **Wireshark (a)**
* SNMP (V)
* SIEM (em (Reuters

**O** Wireshark é um analisador de protocolo de rede usado para capturar o tráfego de rede. O tráfego capturado pelo Wireshark é salvo em arquivos PCAP e inclui informações de interface e timestamps.

**50. Qual é o mecanismo TCP usado na prevenção de congestionamentos?**

* hands-way de aperto de mão
* par de soquete
* um aperto de mão de mão de duas vias
* **janela de deslizamento**

**O** TCP usa o Windows para tentar gerenciar a taxa de transmissão para o fluxo máximo que a rede e o dispositivo de destino podem suportar, minimizando a perda e retransmissões. Quando sobrecarregado com dados, o destino pode enviar uma solicitação para reduzir a janela. Esta prevenção de congestionamento é chamada janelas deslizantes.

**51 -O que é a Internet?**

* É uma rede baseada na tecnologia Ethernet.
* Ele fornece acesso à rede para dispositivos móveis.
* **Fornece conexões através de redes globais interconectadas.**
* É uma rede privada para uma organização com conexões LAN e WAN.

**A** Internet fornece conexões globais que permitem que dispositivos em rede (estações de trabalho e dispositivos móveis) com diferentes tecnologias de rede, como Ethernet, DSL/cabo e conexões seriais, se comuniquem. Uma rede privada para uma organização com conexões LAN e WAN é uma intranet.

Qual é o protocolo usado pelo comando traceroute para enviar e receber solicitações de eco e respostas de eco?

* ICMP

**52. Qual protocolo é usado pelo comando traceroute para enviar e receber ecólicas e eco-replies?**

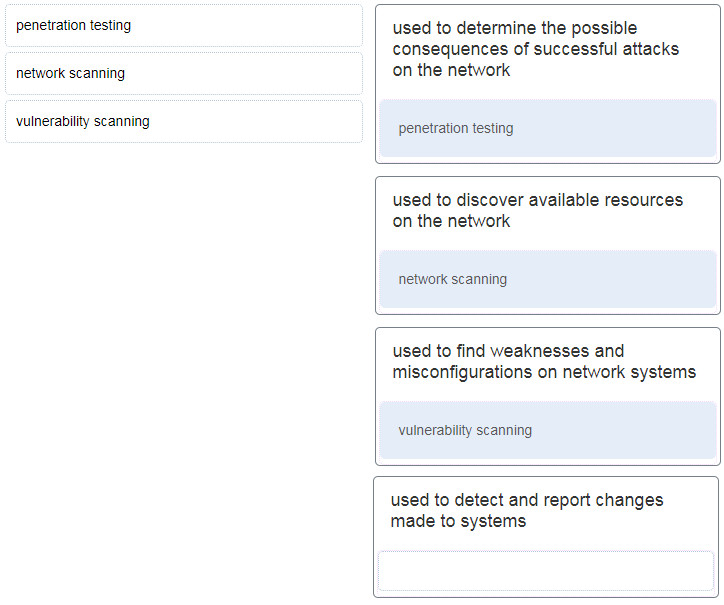
* SNMP (V)
* **ICMP (PIMP)**
* Telnet (A)
* TCP ()

**Explicação:** Traceroute usa o ICMP (Internet Control Message Protocol) para enviar e receber mensagens de solicitação de eco e eco-reply.

**53 - Sim. Quais são duas mensagens ICMPv6 que não estão presentes no ICMP para IPv4? (Escolha dois.)**

* **Solicitação de Vizinho**
* Destino inalcancável
* Confirmação do anfitrião
* O tempo excedido
* **Anúncio do roteador**
* Redirecionamento de rota

**O** ICMPv6 inclui quatro novos tipos de mensagens: Anúncio de roteadores, anúncio de vizinhos, solicitação de roteador e solicitação de vizinho.

**54. Combine a técnica de teste de segurança de rede com a forma como ela é usada para testar a segurança da rede. (Nem todas as opções são usadas.)**   


**55 - Sim. Quais são duas ferramentas de monitoramento que capturam o tráfego de rede e o encaminham para dispositivos de monitoramento de rede? (Escolha dois.)**

* **SPAN**
* **torneiras de rede**
* SNMP (V)
* SIEM (em (Reuters
* Wireshark (a)

**Uma** torneira **de** rede é usada para capturar o tráfego para monitorar a rede. O toque é tipicamente um dispositivo de divisão passiva implementado em linha na rede e encaminha todo o tráfego, incluindo erros de camada física para um dispositivo de análise. O SPAN é uma tecnologia de espelhamento de porta suportada em switches Cisco que permite que o switch copie quadros e os encaminhone para um dispositivo de análise.

**56 - O que se é com o que é. Qual ferramenta de monitoramento de rede está na categoria de analisadores de protocolo de rede?**

* SNMP (V)
* SPAN (p. S
* **Wireshark (a)**
* SIEM (em (Reuters

**O** Wireshark é um analisador de protocolo de rede usado para capturar o tráfego de rede. O tráfego capturado pelo Wireshark é salvo em arquivos PCAP e inclui informações de interface e timestamps.

**57. Com base na saída de comando mostrada, quais permissões ou permissões de arquivo foram atribuídas ao outro grupo de usuários para o arquivo data.txt?**

ls –l data.txt

-rwxrw-r--- staff de vendas 1028 28 15:50 data.txt

* Acesso total
* Leia, escreva
* **Leia**
* ler, escrever, executar

**Explicação:** As permissões de arquivo são sempre exibidas no usuário, grupo e outra ordem. No exemplo exibido, o arquivo tem as seguintes permissões:   
O traço ( – ) significa que este é um arquivo. Para os diretórios, o primeiro traço seria substituído por um “d”.   
O primeiro conjunto de caracteres é para permissão do usuário (rwx). O usuário, vendas, quem possui o arquivo pode ler, escrever e executar o arquivo.   
O segundo conjunto de caracteres é para permissões de grupo (rw-). O grupo, a equipe, que possui o arquivo pode ler e gravar no arquivo.   
O terceiro conjunto de caracteres é para qualquer outro usuário ou permissão de grupo (r-). Qualquer outro usuário ou grupo no computador só pode ler o arquivo.

**58 anos. Quais são os três benefícios de usar links simbólicos sobre links duros no Linux? (Escolha três.)**

* **Eles podem se vincular a um diretório.**
* Eles podem ser comprimidos.
* Links simbólicos podem ser exportados.
* Eles podem ser criptografados.
* **Eles podem ligar para um arquivo em um sistema de arquivos diferente.**
* **Eles podem mostrar a localização do arquivo original.**

**No** Linux, um link difícil é outro arquivo que aponta para o mesmo local que o arquivo original. Um soft link (também chamado de link simbólico ou um link simbólico) é um link para outro nome do sistema de arquivos. Os links rígidos são limitados ao sistema de arquivos em que são criados e não podem ser vinculados a um diretório; os links suaves não se limitam ao mesmo sistema de arquivos e podem ser vinculados a um diretório. Para ver a localização do arquivo original para um link simbólico, use o comando ls –l.

**59. Que dois tipos de informações pessoais podem ser vendidas na dark web por cibercriminosos? (Escolha dois.)**

* Cidade de residência
* **Fotos do Facebook**
* O nome de um banco
* Nome de um animal de estimação
* **Endereço de rua**

**Informações** de identificação pessoal (PII) são qualquer informação que possa ser usada para identificar positivamente um indivíduo. Exemplos de PII incluem o seguinte:   
Nome   
Número de segurança social   
Na data de nascimento   
Números de cartão de crédito   
Números de conta bancária   
Informações do Facebook   
Informações de endereço (rua, e-mail, números de telefone).

**60 anos. Quais são os três serviços oferecidos pela FireEye? (Escolha três.)**

* **Bloqueia ataques em toda a web**
* Cria regras de firewall dinamicamente
* **Identificar e parar o malware latente em arquivos**
* sujeita todo o tráfego para análise de inspeção profunda de pacotes
* implanta conjuntos de regras de detecção de incidentes para ferramentas de segurança de rede
* **Identificar e interromper vetores de ameaças de e-mail**

**A** FireEye é uma empresa de segurança que usa uma abordagem em três frentes que combina inteligência de segurança, experiência em segurança e tecnologia. A FireEye oferece o SIEM e o SOAR com a Helix Security Platform, que usam análise comportamental e detecção avançada de ameaças.

**61 - O que se é. Após a contenção, qual é o primeiro passo para erradicar um ataque?**

* Mude todas as senhas.
* Patch todas as vulnerabilidades.
* Realizar reuniões sobre as lições aprendidas.
* **Identifique todos os hosts que precisam de remediação.**

**Uma** vez que um ataque é contido, o próximo passo é identificar todos os hosts que precisarão de remediação para que os efeitos do ataque possam ser eliminados.

**62 - O que se é com o que é. Qual atividade é normalmente realizada por um agente de ameaças na fase de instalação da Cyber Kill Chain?**

* **Instale um web shell no servidor web de destino para acesso persistente.**
* Colha endereços de e-mail de contas de usuário.
* Abra um canal de comunicação bidirecional para a infraestrutura CnC.
* Obtenha uma ferramenta automatizada para entregar a carga útil de malware.

**Na** fase de instalação da Cyber Kill Chain, o agente de ameaças estabelece uma porta dos fundos para o sistema para permitir o acesso contínuo ao alvo.

Qual é o objetivo de um ataque na fase de instalação da Cyber Kill Chain?

**63 - O que se é dada. Um especialista em segurança de rede é encarregado de implementar uma medida de segurança que monitora o status dos arquivos críticos no data center e envia um alerta imediato se algum arquivo for modificado. Qual aspecto das comunicações seguras é abordado por esta medida de segurança?**

* Autenticação de origem
* **integridade dos dados**
* não repúdio
* Confidencialidade dos dados

**Explicação:** As comunicações seguras consistem em quatro elementos:   
Confidencialidade de dados – garante que apenas usuários autorizados possam ler a mensagem   
Integridade dos dados – garante que a mensagem não foi alterada   
Autenticação de origem – garante que a mensagem não é uma falsificação e realmente vem de quem ela afirma   
Não-repúdio de dados – garante que o remetente não pode repudiar, ou refutar, a validade de uma mensagem enviada

**64. Um administrador de rede está configurando um servidor AAA para gerenciar a autenticação TACACS +. Quais são os dois atributos da autenticação TACACS+? (Escolha dois.)**

* Porta TCP 40
* **criptografia para todas as comunicações**
* Processo único para autenticação e autorização
* Porto UDP 1645
* criptografia para apenas a senha de um usuário
* **processos separados para autenticação e autorização**

**Explicação:** A autenticação TACACS+ inclui os seguintes atributos:   
Separa processos de autenticação e autorização   
Criptografa todas as comunicações, não apenas senhas   
Utiliza a porta TCP 49

**65. Na tentativa de evitar ataques de rede, os analistas cibernéticos compartilham atributos identificáveis únicos de ataques conhecidos com colegas. Quais são os três tipos de atributos ou indicadores de compromisso que são úteis para compartilhar? (Escolha três.)**

* **Endereços IP dos servidores de ataque**
* **alterações feitas no software de sistema final**
* netbios nomes de firewalls comprometidos
* **características dos arquivos de malware**
* BIOS de sistemas de ataque
* ID do sistema de sistemas comprometidos

**Muitos** ataques de rede podem ser evitados compartilhando informações sobre indicadores de comprometimento (IOC). Cada ataque tem atributos identificáveis únicos. Indicadores de compromisso são a evidência de que um ataque ocorreu. Os COIs podem estar identificando recursos de arquivos de malware, endereços IP de servidores que são usados no ataque, nomes de arquivos e alterações características feitas no software do sistema de ponta.

**66. Quais dois tipos de mensagens são usadas no lugar da ARP para resolução de endereços no IPv6? (Escolha dois.)**

* anycast
* broadcast
* **Solicitação de vizinho**
* resposta de eco
* Pedido de eco
* **Anúncio de vizinhos**

**O** IPv6 não usa o ARP. Em vez disso, a descoberta de vizinhos ICMPv6 é usada enviando solicitações de vizinhos e mensagens de publicidade de vizinhos.

**67 anos. O que é indicado por uma verdadeira classificação de alerta de segurança negativa?**

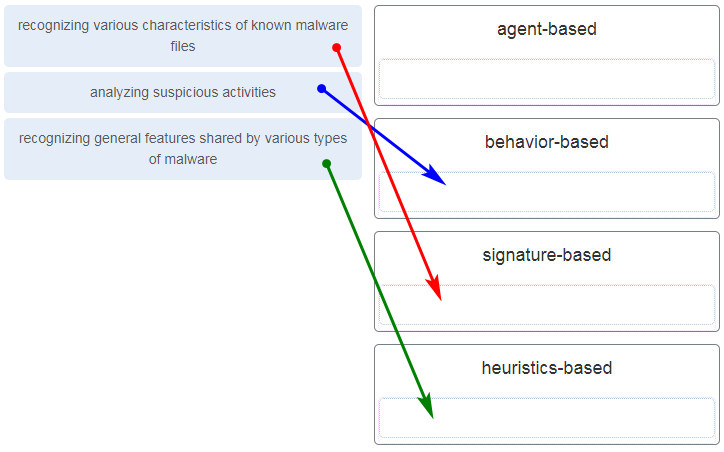
* Um alerta é verificado como um incidente de segurança real.
* Um alerta é emitido incorretamente e não indica um incidente de segurança real.
* **O tráfego normal é corretamente ignorado e alertas errôneos não estão sendo emitidos.**
* Os exploras não estão sendo detectados pelos sistemas de segurança que estão em vigor.

**As** classificações negativas verdadeiras são desejáveis porque indicam que o tráfego normal não está sendo identificado corretamente como tráfego malicioso por medidas de segurança.

**68 - Qual declaração descreve a abordagem de detecção de intrusão baseada em anomalias?**

* Ele compara o arquivo de definição de antivírus a um repositório baseado na nuvem para atualizações mais recentes.
* **Ele compara o comportamento de um host a uma linha de base estabelecida para identificar possíveis intrusões.**
* Ele compara as assinaturas do tráfego de entrada com um banco de dados de intrusão conhecido.
* Ele compara as operações de um host com uma política de segurança bem definida.

**Explicação:** Com uma abordagem de detecção de intrusão baseada em anomalias, uma linha de base de comportamentos do hospedeiro é estabelecida primeiro. O comportamento do hospedeiro é verificado em relação à linha de base para detectar desvios significativos, o que pode indicar possíveis intrusões.

**69. Combine a descrição com a abordagem antimalware. (Nem todas as opções são usadas.)**   


**Explicação:**Os programas de antimalware podem detectar vírus usando três abordagens diferentes:

* **Baseado em assinatura** – ao reconhecer várias características de arquivos de malware conhecidos
* **Baseado em heurística** – ao reconhecer recursos gerais compartilhados por vários tipos de malware
* **Baseado no comportamento** – através da análise de atividades suspeitas

Que tipo de evidência sustenta uma afirmação baseada em evidências previamente obtidas?

Provas corroborantes

Um host está transmitindo um broadcast. Qual host ou hosts o receberão?

Todos os hosts na mesma rede

Tópico 5.2.0 - Um broadcast é entregue a cada host que possui um endereço IP na mesma rede.

Qual afirmativa descreve uma característica da computação em nuvem?

Aplicaçõs podem ser acessadas pela internet por usuários individuais ou empresas usando auqlaqur dispositivo, em qualquer parte do mundo

Tópico 5.1.0 - A computação em nuvem permite aos usuários acessar aplicativos, fazer backup e armazenar arquivos e realizar tarefas sem a necessidade de software ou servidores adicionais. Os usuários da nuvem acessam os recursos em tempo real, através de serviços de assinatura ou pagamento por uso, usando apenas um navegador web.

Um administrador de rede pode executar ping com êxito no servidor em www.cisco.com, mas não pode executar o ping no servidor web da empresa localizado em um ISP em outra cidade. Que ferramenta ou comando podem ajudar a identificar o roteador específico em que o pacote foi perdido ou atrasado?

traceroute

Tópico 5.1.0 - O comando traceroute fornece informações de conectividade sobre o caminho que um pacote segue para chegar ao destino e sobre cada roteador (salto) ao longo do caminho. Ele também indica o tempo que um pacote leva para chegar da origem em cada salto e vice-versa.

Qual camada do modelo OSI contém protocolos para comunicação processo a processo?

aplicação

Tópico 5.2.0 - A camada de aplicação do modelo OSI é responsável pela comunicação entre os processos. Exemplos de protocolos na camada de aplicação são DHCP, DNS e HTTP.

Em qual camada OSI é um número de porta de destino adicionado a uma PDU durante o processo de encapsulamento?

Camada de transporte

Tópico 5.3.0 - A camada de transporte usa endereços de protocolo na forma de números de porta para identificar aplicativos de rede que devem lidar com dados de cliente e servidor.

Qual processo envolve colocar uma PDU dentro de outra PDU?

encapsulamento

Tópico 5.3.0 - Quando uma mensagem é colocada dentro de outra mensagem, isso é conhecido como encapsulamento. Em redes, o encapsulamento ocorre quando uma unidade de dados de protocolo é transportada dentro do campo de dados da próxima unidade de dados de protocolo inferior.

Qual afirmação descreve com precisão um processo de encapsulamento TCP / IP quando um PC está enviando dados para a rede?

Os segmentos são enviados da camada de transporte para a camada de rede

Tópico 5.3.0 - Quando os dados estão viajando do PC para a rede, a camada de transporte envia segmentos para a camada de rede. A camada de rede envia pacotes para a camada de acesso à rede, que cria quadros e os converte em bits. Os bits são liberados para a mídia da rede.

Um cliente Web está recebendo uma resposta para uma página da Web de um servidor Web. Do ponto de vista do cliente, qual é a ordem correta da pilha de protocolo que é usada para decodificar a transmissão recebida?

Ethernet, IP, TCP, HTTP

Tópico 5.3.0-1. O HTTP controla a maneira como um servidor da web e um cliente interagem. 2. O TCP gerencia conversas individuais entre servidores da web e clientes. 3. IP é responsável pela entrega através do melhor caminho para o destino. 4. Ethernet pega o pacote do IP e formata-o para transmissão.

Como a BYOD (Bring Your Own Device) muda a maneira como as empresas implementam as redes?

BYOD significa flexibilidade em onde e como os usuários acessam os recursos da rede

Tópico 5.1.0 - Um ambiente BYOD exige que uma organização acomode uma variedade de dispositivos e métodos de acesso. Dispositivos pessoais, que não estão sob o controle da empresa, podem ser aceitos e, portanto, segurança é um fator essencial. Os custos de hardware no local serão reduzidos, permitindo que a empresa priorize a disponibilização de ferramentas de colaboração e outros softwares para usuários BYOD.

Na comunicação entre computadores, qual é o objetivo da codificação de mensagens?

Converter informações para o formato adequado para a transmissão

Tópico 5.2.0 - Antes de uma mensagem ser enviada através de uma rede, ela deve primeiro ser codificada. Codificação é o processo de conversão de dados da mensagem em outro formato adequado a transmissão pelo meio físico. Cada bit da mensagem é codificado em um padrão de sons, de ondas de luz ou de impulsos elétricos, dependendo do meio físico de rede em que os bits são transmitidos. O host destino recebe e decodifica os sinais para interpretar a mensagem.

Qual afirmação é verdadeira sobre os modelos TCP/IP e OSI?​

A camada de transporte TCP/IP e a camada 4 OSI fornecem serviços e funções semelhantes.

Tópico 5.2.0 - A camada de rede do TCP / IP fornece a mesma função que a camada de rede OSI. A camada de transporte dos modelos TCP / IP e OSI fornece a mesma função. A camada de aplicação TCP / IP inclui as mesmas funções das camadas OSI 5, 6 e 7.

Que método pode ser usado por dois computadores para garantir que os pacotes não sejam descartados porque muitos dados estão sendo enviados muito rapidamente?

Controle de fluxo

Tópico 5.2.0 - Para que dois computadores possam se comunicar de forma eficaz, deve haver um mecanismo que permita que a origem e o destino definam o tempo de transmissão e recebimento dos dados. O controle de fluxo permite isso, garantindo que os dados não sejam enviados muito rápido para serem recebidos corretamente.

**1. A definição de incidentes de segurança informática e elemento de termos relacionados é em que parte do plano de resposta a incidentes?**

* **A política**
* Plano
* o procedimento

**2. O elemento estratégia e metas é em que parte do plano de resposta a incidentes?**

* **Plano**
* o procedimento
* A política

**3. A estrutura organizacional e definição de papéis, responsabilidades e níveis de autoridade é em qual parte do plano de resposta a incidentes?**

* **A política**
* Plano
* o procedimento

**4. As classificações de priorização e gravidade do elemento incidentes é em qual parte do plano de resposta a incidentes?**

* **A política**
* Plano
* o procedimento

**5. Qual é o dois netOs comandos estão associados ao compartilhamento de recursos de rede? (Escolha dois.)**

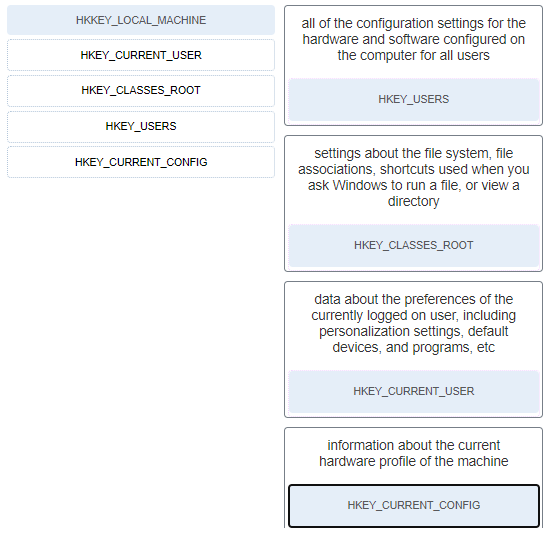
* Início líquido
* contas de rede
* quota-parte líquida
* uso líquido
* paragem líquida

**Explicação:**

O que é netO comando é um comando muito importante. Alguns comuns netOs comandos incluem estes:

* net accounts– define os requisitos de senha e logon para usuários
* net session– listar ou desconecta sessões entre um computador e outros computadores na rede
* net sharecria, remove ou gerencia recursos compartilhados
* net startIniciar um serviço de rede ou listas executando serviços de rede
* net stop– interrompe um serviço de rede
* net useConecta, desconecta e exibe informações sobre recursos de rede compartilhada
* net viewMostra uma lista de computadores e dispositivos de rede na rede

**6. Combine a chave do Registro do Windows 10 com sua descrição. (Nem todas as opções são usadas)**



Qual formato de PDU é usado quando os bits são recebidos dos meios físicos de rede pela placa de rede de um host?

**7. Qual formato PDU é usado quando bits são recebidos do meio de rede pela NIC de um host?**

* Segment
* arquivo do arquivo
* Pacote de embalagem
* quadro

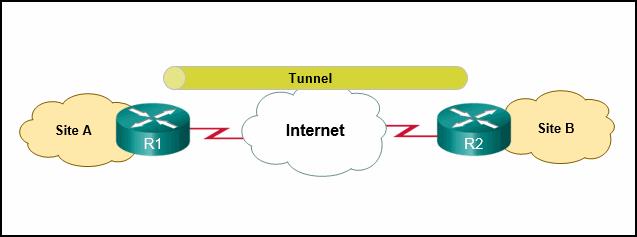
**Quando** recebidos na camada física de um host, os bits são formatados em um quadro na camada de link de dados. Um pacote é o PDU na camada de rede. Um segmento é o PDU na camada de transporte. Um arquivo é uma estrutura de dados que pode ser usada na camada de aplicativo.

**8 - O que se é. Um usuário está executando um tracert para um dispositivo remoto. Em que ponto um roteador, que está no caminho para o dispositivo de destino, pararia de encaminhar o pacote?**

* quando o roteador recebe uma mensagem ICMP Time Exceeded
* quando os valores das mensagens Echo Request e Echo Responderem chegarem a zero
* Quando o valor de RTT chega a zero
* quando o valor no campo TTL atinge zero
* quando o anfitrião responde com uma mensagem ICMP Echo Responder

**Quando** um roteador recebe um pacote traceroute, o valor no campo TTL é decrementado por 1. Quando o valor no campo atinge zero, o roteador receptor não encaminhará o pacote e enviará uma mensagem ICMP Time Exceeded de volta para a fonte.

**9. Consulte a exposição. Qual solução pode fornecer uma VPN entre o site A e o site B para suportar o encapsulamento de qualquer protocolo Layer 3 entre as redes internas em cada site?**



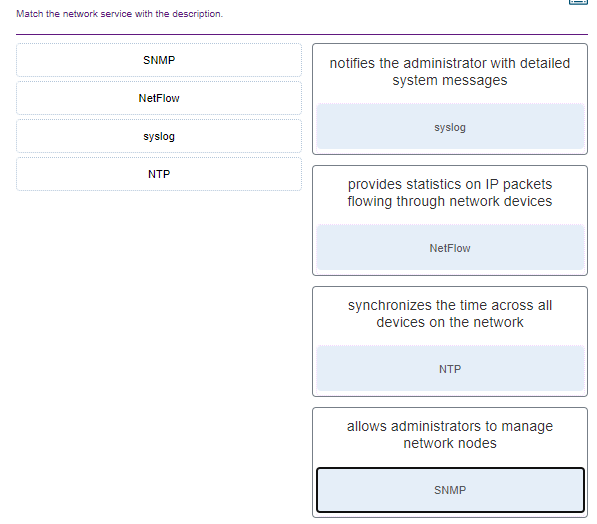
* um túnel de IPsec
* Cisco SSL VPN (es)
* um túnel GRE
* um túnel de acesso remoto

**Um** túnel de encapsulamento de roteamento genérico (GRE) é uma solução de tunelamento de VPN não segura, local-a-site, capaz de encapsular qualquer protocolo Layer 3 entre vários sites através de um trabalho de internet IP.

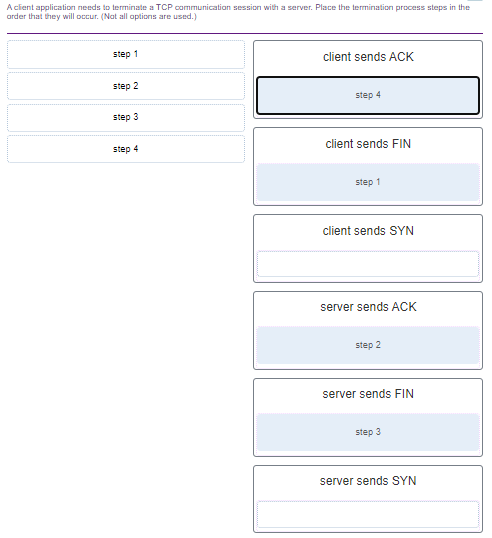
**10. Para que finalidade um administrador de rede usaria a ferramenta Nmap?**

* proteção dos endereços IP privados dos hosts internos
* Identificação de anomalias de rede específicas
* coleta e análise de alertas e logs de segurança
* Detecção e identificação de portos abertos

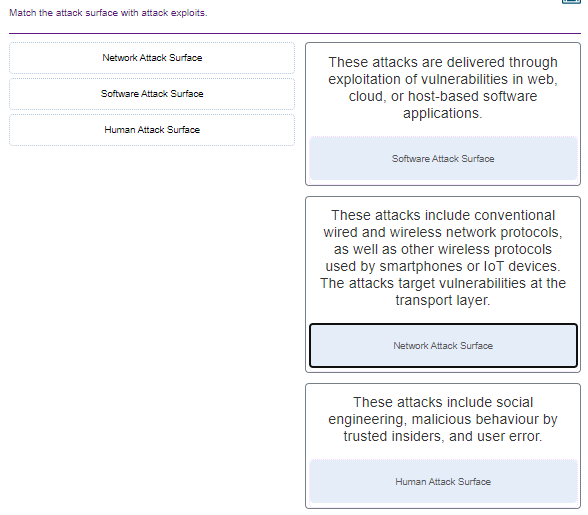
**11. Combine o serviço de rede com a descrição.**



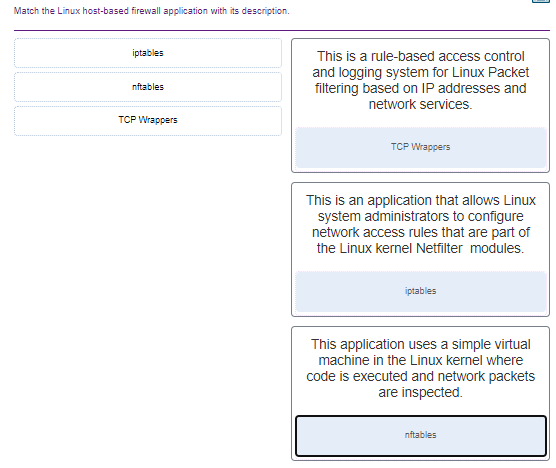
**12 - O que se é preciso falar com isso. Um aplicativo cliente precisa encerrar uma sessão de comunicação TCP com um servidor. Coloque as etapas do processo de rescisão na ordem em que elas ocorrerão. (Nat todas as opções são usadas.)**



**13. Combine a superfície de ataque com exploits de ataque.**



**14. Combine o aplicativo de firewall baseado em host Linux com sua descrição.**

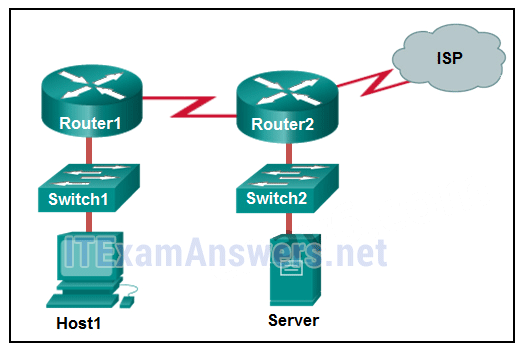


**Qual ataque à rede busca criar um DoS para clientes ao evitar que possam eles obtenham um aluguel de DHCP?**

**15. Que ataque de rede procura criar um DoS para os clientes, impedindo-os de obter um contrato de arrendamento DHCP?**

* **DHCP de fome (privação DHCP)**
* O endereço IP spoofing
* DHCP spoofing
* Ataque da mesa do CAM

**Explicação:** Os ataques de fome do DCHP são lançados por um invasor com a intenção de criar um DoS para clientes DHCP. Para atingir esse objetivo, o invasor usa uma ferramenta que envia muitas mensagens DHCPDISCOVER para arrendar todo o pool de endereços IP disponíveis, negando-os a hosts legítimos.

**16. Consulte a exposição. Se o Host1 fosse transferir um arquivo para o servidor, quais camadas do modelo TCP/IP seriam usadas?**   


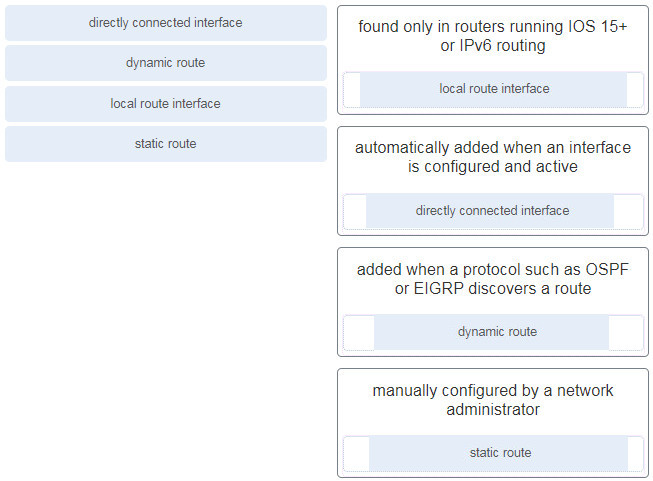
* somente as camadas de aplicação e Internet
* **camadas de aplicação, transporte, Internet e acesso à rede**
* apenas camadas de acesso à Internet e à rede
* apenas aplicação, transporte, rede, link de dados e camadas físicas
* apenas camadas de aplicativos, Internet e acesso à rede
* aplicação, sessão, transporte, rede, link de dados e camadas físicas

**O** modelo TCP/IP contém as camadas de aplicativo, transporte, internet e acesso à rede. Uma transferência de arquivo usa o protocolo de camada de aplicativo FTP. Os dados se moveriam da camada de aplicativo através de todas as camadas do modelo e da rede para o servidor de arquivos.

**17 - Sim. Uma empresa tem um servidor de arquivos que compartilha uma pasta chamada Public. A política de segurança de rede especifica que a pasta pública é atribuída apenas os direitos de leitura para qualquer pessoa que possa fazer login no servidor enquanto os direitos de edição são atribuídos apenas ao grupo de administração da rede. Qual componente é abordado na estrutura de serviço de rede AAA?**

* Automação
* Autenticação
* **A autorização**
* contabilidade

**Depois que** um usuário é autenticado com sucesso (logged no servidor), a autorização é o processo de determinar quais recursos de rede o usuário pode acessar e quais operações (como ler ou editar) o usuário pode executar.

**18. Combine o tipo de entrada da tabela de roteamento de rede de destino com uma definição.**   


**19. Uma pessoa que vem a um café pela primeira vez quer obter acesso sem fio à Internet usando um laptop. Qual é o primeiro passo que o cliente sem fio fará para se comunicar através da rede usando um quadro de gerenciamento sem fio?**

* Associar-se à AP
* Autenticar para a AP
* **Descubra a AP**
* Concordo com a AP na carga útil

**Explicação:**Para que os dispositivos sem fio se comuniquem em uma rede sem fio, os quadros de gerenciamento são usados para concluir um processo de três estágios:

Descubra o AP   
Autenticar com o AP   
Associar-se à AP

Quais são os estágios concluídos por um dispositivo sem fio antes de poder se comunicar através de uma rede LAN sem fio?

* Descubra o AP , Autenticar com o AP , Associar-se à AP

**20 anos. Foi atribuído um dispositivo o endereço IPv6 de 2001:0db8:cafe:4500:1000:00d8:0058:00ab/64. Qual é o identificador de rede do dispositivo?**

* 2001:0db8:café: 4500:1000
* 2001:0db8:café:4500:1000:00d8:0058:00ab
* 1000:00d8:0058:00ab
* **2001:0db8:café: 4500**
* Em 2001

**Explicação:** O endereço tem um comprimento de prefixo de /64. Assim, os primeiros 64 bits representam a parte da rede, enquanto os últimos 64 bits representam a parte do host do endereço IPv6.

**21 - Sim. Um administrador quer criar quatro sub-redes a partir do endereço de rede 192.168.1.0/24. Qual é o endereço de rede e máscara de sub-rede da segunda sub-rede utilizável?**

**sub-rede 192.168.1.64   
máscara de sub-rede 255.255.255.192**

sub-rede 192.168.1.64   
máscara de sub-rede 255.255.255.240

sub-rede 192.168.1.32   
máscara de sub-rede 255.255.255.240

sub-rede 192.168.1.128   
máscara de sub-rede 255.255.255.192

sub-rede 192.168.1.8   
máscara de sub-rede 255.255.255.224

**22 - Sim. Que termo descreve um conjunto de ferramentas de software projetadas para aumentar os privilégios de um usuário ou para conceder acesso ao usuário a partes do sistema operacional que normalmente não devem ser permitidas?**

* Compilador
* **rootkit**
* gerenciador de pacotes
* Teste de penetração

**Explanation:** Um rootkit é usado por um invasor para proteger um backdoor para um computador comprometido, conceder acesso a partes do sistema operacional normalmente não permitidas ou aumentar os privilégios de um usuário.

**23 - Sim. O pessoal de segurança de TI de uma organização percebe que o servidor web implantado na DMZ é frequentemente alvo de agentes de ameaças. A decisão é tomada para implementar um sistema de gerenciamento de patches para gerenciar o servidor. Qual método de estratégia de gerenciamento de riscos está sendo usado para responder ao risco identificado?**

* partilha de riscos
* Evitar o risco
* **Redução de risco**
* retenção de risco

**Explicação:**Existem quatro estratégias potenciais para responder aos riscos que foram identificados:

**Evitar riscos** – Pare de realizar as atividades que criam riscos.

**Redução de riscos** – Diminua o risco tomando medidas para reduzir a vulnerabilidade.

**Compartilhamento de risco** – Mude um pouco do risco para outras partes.

**Retenção de riscos** – Aceite o risco e suas consequências.

**24. Quais são as duas características do método SLAAC para configuração de endereços IPv6? (Escolha dois.)**

* **O gateway padrão de um cliente IPv6 em uma LAN será o endereço link-local da interface do roteador conectada à LAN.**
* Este método stateful de adquirir um endereço IPv6 requer pelo menos um servidor DHCPv6.
* Os clientes enviam mensagens de anúncio do roteador para os roteadores para solicitar o endereçamento IPv6.
* **O endereçamento IPv6 é atribuído dinamicamente aos clientes através do uso de ICMPv6.**
* As mensagens de solicitação de roteador são enviadas pelo roteador para oferecer endereçamento IPv6 aos clientes.

**25 - Sim. Um técnico percebe que um aplicativo não está respondendo a comandos e que o computador parece responder lentamente quando os aplicativos são abertos. Qual é a melhor ferramenta administrativa para forçar a liberação de recursos do sistema a partir da aplicação não responsiva?**

* Visualizador do evento
* Restauração do sistema
* Adicionar ou remover programas
* **Gerente de tarefas**

**Explicação:** Use a guia Desempenho do Gerenciador de Tarefas para ver uma representação visual da utilização da CPU e da RAM. Isso é útil para determinar se mais memória é necessária. Use a guia Aplicativos para interromper um aplicativo que não está respondendo.

**26 - Sim. Como os dados estatísticos podem ser usados para descrever ou prever o comportamento da rede?**

* **Comparando o comportamento normal da rede com o comportamento atual da rede**
* Gravando conversas entre os endpoints da rede
* por listar os resultados das atividades de navegação no site do usuário
* Exibindo mensagens de alerta geradas pelo Snort

**Os** dados estatísticos são criados através da análise de outras formas de dados de rede. As características estatísticas do comportamento normal da rede podem ser comparadas ao tráfego de rede atual, em um esforço para detectar anomalias. Conclusões resultantes da análise podem ser usadas para descrever ou prever o comportamento da rede.

**27 - Sim. Qual métrica no Grupo Métrico Base CVSS é usado com um vetor de ataque?**

* **A proximidade do agente de ameaça à vulnerabilidade**
* a presença ou ausência do requisito de interação do usuário para que uma exploração seja bem-sucedida
* a determinação se a autoridade inicial muda para uma segunda autoridade durante a exploração
* o número de componentes, software, hardware ou redes que estão fora do controle do invasor e que devem estar presentes para que uma vulnerabilidade seja explorada com sucesso

**Essa** é uma métrica que reflete a proximidade do agente de ameaças ao componente vulnerável. Quanto mais remoto o agente de ameaças é para o componente, maior a gravidade. Atores de ameaças próximos à sua rede ou dentro da sua rede são mais fáceis de detectar e mitigar.

**Qual função principal do NIST Cybersecurity Framework está preocupada com o desenvolvimento e a implementação de salvaguardas que garantam a prestação de serviços críticos de infraestrutura?**

**28 - O que se refere. Qual função central do NIST Cybersecurity Framework está preocupada com o desenvolvimento e implementação de salvaguardas que garantem a prestação de serviços de infraestrutura crítica?**

* Responder
* Detectar
* Identificar a
* Recupera- se:
* **Proteger a**

**29 - 29 - Sim. Qual é uma diferença entre os modelos de rede cliente-servidor e peer-to-peer?**

* Somente no modelo cliente-servidor podem ocorrer transferências de arquivos.
* Uma transferência de dados que usa um dispositivo que serve em uma função de cliente requer que um servidor dedicado esteja presente.
* Uma rede peer-to-peer transfere dados mais rapidamente do que uma transferência usando uma rede cliente-servidor.
* **Cada dispositivo em uma rede peer-to-peer pode funcionar como um cliente ou um servidor.**

**30. Qual declaração é correta sobre os protocolos de rede?**

* **Eles definem como as mensagens são trocadas entre a origem e o destino.**
* Todos funcionam na camada de acesso à rede de TCP/IP.
* Eles só são necessários para a troca de mensagens entre dispositivos em redes remotas.
* Os protocolos de rede definem o tipo de hardware que é usado e como ele é montado em racks.

**31 - Sim. - Sim. Que abordagem pode ajudar a bloquear possíveis métodos de entrega de malware, conforme descrito no modelo Cyber Kill Chain, em um servidor web com sede na Internet?**

* Construa detecções para o comportamento de malware conhecido.
* Colete arquivos de malware e metadados para análise futura.
* Audite o servidor web para determinar forensemente a origem da exploração.
* **Analise o caminho de armazenamento da infraestrutura usado para arquivos.**

**Um** agente de ameaças pode enviar a arma através de interfaces da web para o servidor de destino, seja em uploads de arquivos ou solicitações codificadas na web. Ao analisar o caminho de armazenamento da infraestrutura usado para arquivos, medidas de segurança podem ser implementadas para monitorar e detectar entregas de malware por meio desses métodos.

**32 - Sim. Qual elemento meta-recurso no Modelo Diamante classifica o tipo geral de evento de intrusão?**

* Fase de fase
* **Os resultados**
* Metodologia
* Direção

**33. Qual comando do Linux é usado para gerenciar processos?**

* chrootkit (a)
* ls (es)
* grep (remirpe
* **Mata matar**

**Explicação:** O comando kill é usado para parar, reiniciar ou pausar um processo. O comando chrootkit é usado para verificar o computador para rootkits, um conjunto de ferramentas de software que podem aumentar o nível de privilégio de um usuário ou conceder acesso a partes do software normalmente não permitidos. O comando grep é usado para procurar um arquivo ou texto dentro de um arquivo. O comando ls é usado para listar arquivos, diretórios e informações de arquivo.

**34 - Sim. Que ferramenta pode ser usada em um sistema Cisco AVC para analisar e apresentar os dados de análise do aplicativo em relatórios de painel?**

* NetFlow (AO)
* NBAR2 (
* **Prime (')**
* IPFIX (IPO)

**Explanation:**Um sistema de gerenciamento e relatórios, como o Cisco Prime, pode ser usado para analisar e apresentar os dados da análise do aplicativo em relatórios de painel para uso pelo pessoal de monitoramento de rede.

**35. Qual registro do Windows Event Viewer inclui eventos relacionados à operação de drivers, processos e hardware?**

* **logs do sistema**
* registos de aplicações
* Logs de segurança
* Logs de configuração

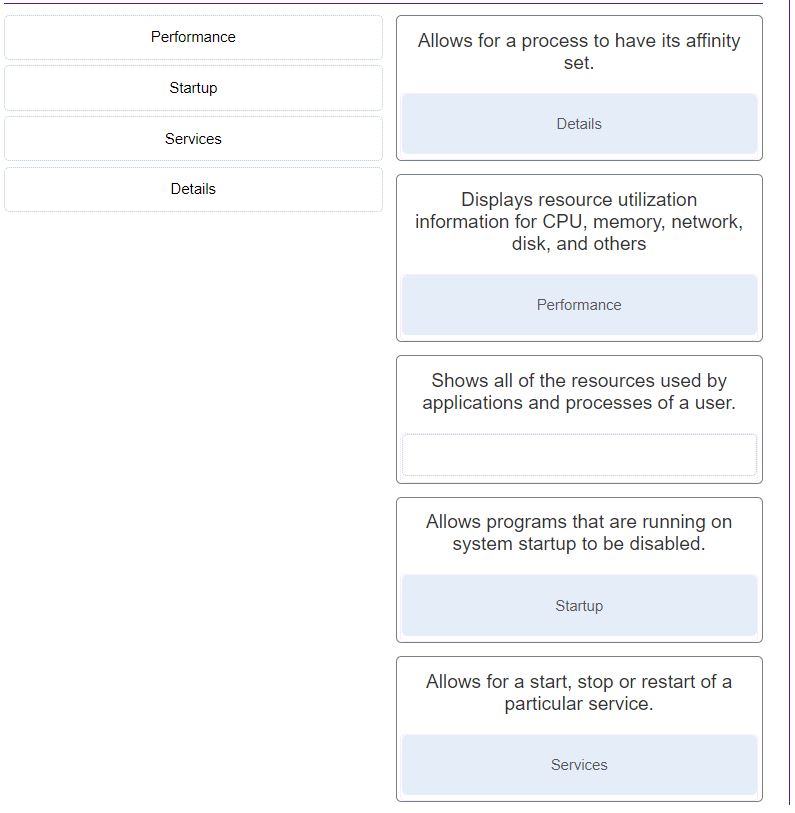
Por padrão, o Windows mantém quatro tipos de logs de host:

* **Logs de aplicativos –** eventos registrados por vários aplicativos
* **Logs do sistema –** eventos sobre a operação de drivers, processos e hardware
* **Registros de configuração –** informações sobre a instalação de software, incluindo atualizações do Windows
* **Registros de segurança –** eventos relacionados à segurança, como tentativas de logon e operações relacionadas ao gerenciamento e acesso de arquivos ou objetos

**36 (em inglês). Qual método é usado para tornar os dados não legíveis para usuários não autorizados?**

* **Criptografar os dados.**
* Fragmento dos dados.
* Adicione um checksum ao final dos dados.
* Atribua-o um nome de usuário e uma senha.

**Os** dados de rede podem ser criptografados usando vários aplicativos de criptografia para que os dados sejam tornados não legíveis para usuários não autorizados. Os usuários autorizados têm o aplicativo de criptografia para que os dados possam ser não criptografados.

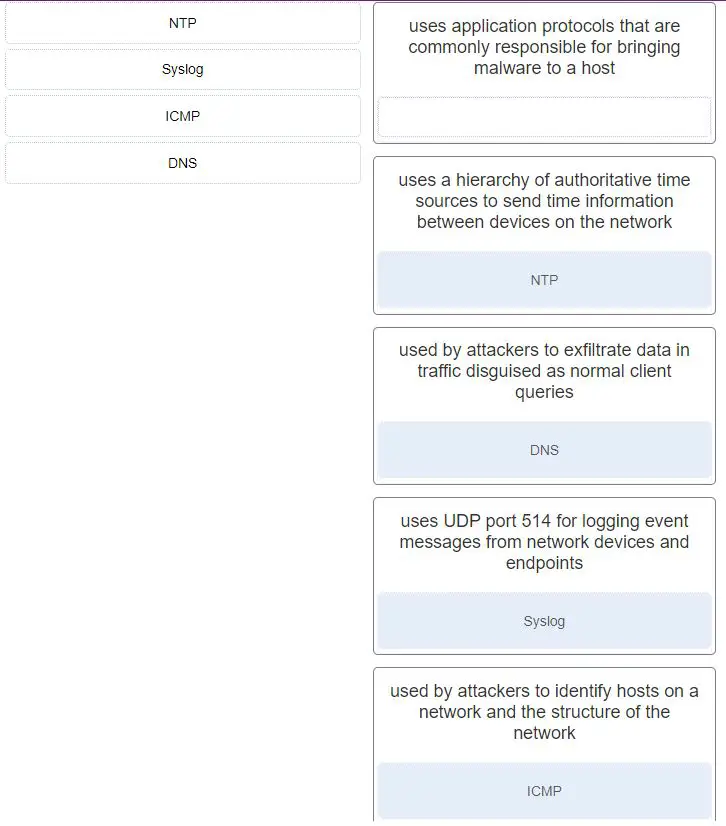
**37. Combine as guias do Gerenciador de Tarefas do Windows 10 às suas funções. (Nem todas as opções são usadas.)**   


**38 - O que se fala em: 38. Para sistemas de rede, qual sistema de gestão aborda o inventário e controle de configurações de hardware e software?**

* Gestão de ativos
* Gestão de vulnerabilidades
* gestão de riscos
* **gestão de configuração**

**Explicação:** O gerenciamento de configuração aborda o inventário e o controle de configurações de hardware e software de sistemas de rede.

**38 anos. Combine a tecnologia ou protocolo de rede comum com a descrição. (Nem todas as opções são usadas.)**



**40. Quais são as três principais funções fornecidas pela Ceia de Segurança? (Escolha três.)**

* planejamento de continuidade de negócios
* **captura completa de pacotes**
* **análise de alerta**
* **Detecção de intrusão**
* gerenciamento de dispositivos de segurança
* Contenção de ameaças

**O** Security Onion é um conjunto de ferramentas de monitoramento de segurança de rede (NSM) para avaliar alertas de segurança cibernética. Para os analistas de segurança cibernética, o Security Onion fornece sistemas completos de detecção de intrusão baseados em rede e host e ferramentas de análise de alerta.

**41. Em termos NAT, que tipo de endereço se refere ao endereço IPv4 globalmente rotível de um host de destino na Internet?**

* **For fora do mundo**
* dentro do mundo global
* For fora do local
* dentro do local

**De acordo com** a perspectiva de um dispositivo NAT, os endereços globais internos são usados por usuários externos para alcançar hosts internos. Dentro dos endereços locais são os endereços atribuídos a hosts internos. Endereços globais externos são os endereços de destinos na rede externa. Os endereços locais externos são os endereços privados reais dos hosts de destino atrás de outros dispositivos NAT.

**42 - O que se passa com que se fala em 42. Quais dois campos ou recursos a Ethernet examina para determinar se um quadro recebido é passado para a camada de enlace de dados ou descartado pela NIC? (Escolha dois.)**

* CEF em
* Endereço MAC de origem
* **tamanho mínimo do quadro**
* Auto-MDIX
* **Sequência de verificação de quadros**

**43 - Sim. - Sim. Que tipo de dados seriam considerados um exemplo de dados voláteis?**

* cache do navegador web
* **Registos de memória**
* Arquivos de log
* ficheiros de temperatura

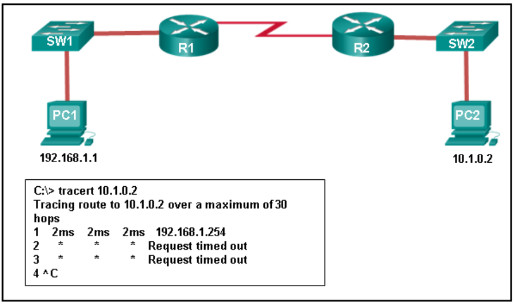
**Explicação:** Os dados voláteis são dados armazenados na memória, como registros, cache e RAM, ou são dados que existem em trânsito. A memória volátil é perdida quando o computador perde energia.

**44. Qual é o principal objetivo das explorações por um agente de ameaça através da arma entregue a um alvo durante a fase de exploração da Cyber Kill Chain?**

* Inicie um ataque de DoS.
* Envie uma mensagem de volta para um CnC controlado pelo agente de ameaças.
* **Quebre a vulnerabilidade e ganhe o controle do alvo.**
* Estabeleça uma porta traseira para o sistema.

**Após** a entrega da arma, o agente de ameaça a usa para quebrar a vulnerabilidade e ganhar o controle do alvo. O agente de ameaça usará um exploit que ganha o efeito desejado, faz isso silenciosamente e evita detecções. Estabelecer uma porta traseira no sistema alvo é a fase de instalação.

**45. Consulte a exposição. Um administrador está tentando solucionar problemas de conectividade entre PC1 e PC2 e usa o comando tracert do PC1 para fazê-lo. Com base na saída exibida, onde o administrador deve começar a solucionar problemas?**

CyberOps Associate 1.0 Exame final

* **R1 em IR**
* PC2 em
* SW2 (G)
* R2 em IR
* SW1 (S: SW

**Explicação:** Tracert é usado para rastrear o caminho que um pacote leva. A única resposta bem-sucedida foi do primeiro dispositivo ao longo do caminho na mesma LAN que o host de envio. O primeiro dispositivo é o gateway padrão no roteador R1. O administrador deve, portanto, começar a solucionar problemas no R1.

**46 - Sim. Para quais três ferramentas de segurança o Cisco Talos mantém os conjuntos de regras de detecção de incidentes de segurança? (Escolha três.)**

* **Snort (su-t**
* NetStumbler (em of the
* Socat (tratos)
* **SpamCop em**
* **ClamAV (Emblema)**

**47. Qual firewall baseado em host usa uma abordagem de três perfis para configurar a funcionalidade de firewall?**

* **Firewall do Windows**
* iptables (esufláveis)
* TCP Wrapper em
* nftables em

**O** Windows Firewall usa uma abordagem baseada em perfil para configurar a funcionalidade de firewall. Ele usa três perfis, público, privado e domínio, para definir funções de firewall.

**48 - O que se é com o que é. Quando um usuário visita um site de loja on-line que usa HTTPS, o navegador do usuário consulta a CA para uma CRL. Qual é o propósito desta pergunta?**

* **verificar a validade do certificado digital**
* para solicitar o certificado digital auto-assinado da CA
* para verificar o comprimento da chave usada para o certificado digital
* para negociar a melhor criptografia para usar

**Um** certificado digital deve ser revogado se for inválido. As CAs mantêm uma lista de revogação de certificados (CRL), uma lista de números de série de certificados revogados que foram invalidados. O navegador do usuário consultará a CRL para verificar a validade de um certificado.

**49. Qual etapa do Ciclo de Vida do Gerenciamento de Vulnerabilidade determina um perfil de risco de linha de base para eliminar riscos baseados em criticidade de ativos, ameaça de vulnerabilidade e classificação de ativos?**

* Descobri- se
* **avaliar a**
* Priorizar os ativos
* Verificam o que

**Explicação:**Os passos no Ciclo de Vida de Gestão de Vulnerabilidades incluem:

* Descubra – inventariar todos os ativos em toda a rede e identificar detalhes do host, incluindo sistemas operacionais e serviços abertos, para identificar vulnerabilidades
* Priorizar ativos – categorizar ativos em grupos ou unidades de negócios e atribuir um valor comercial a grupos de ativos com base em sua criticidade às operações comerciais
* Avaliar – determinar um perfil de risco de linha de base para eliminar riscos com base na criticidade dos ativos, ameaças de vulnerabilidade e classificação de ativos
* Relatório – meça o nível de risco comercial associado aos ativos de acordo com as políticas de segurança. Documente um plano de segurança, monitore atividades suspeitas e descreva vulnerabilidades conhecidas.
* Remediação – priorize de acordo com o risco de negócios e corrija vulnerabilidades em ordem de risco
* Verificar – verificar se as ameaças foram eliminadas através de auditorias de acompanhamento

**50. Qual sistema de gerenciamento implementa sistemas que rastreiam a localização e a configuração de dispositivos e software em rede em uma empresa?**

* **Gestão de ativos**
* Gestão de vulnerabilidades
* gestão de riscos
* gestão de configuração

**O** gerenciamento de ativos envolve a implementação de sistemas que rastreiam a localização e a configuração de dispositivos e software em rede em uma empresa.

**51 - O que se é. Um administrador de rede está revisando alertas do servidor devido a relatórios de lentidão da rede. O administrador confirma que um alerta era um incidente de segurança real. Qual é a classificação de alerta de segurança deste tipo de cenário?**

* Falsa negativa
* **verdadeiro positivo**
* Verdadeiro negativo
* falso positivo

**52. Qual protocolo de camada de aplicação é usado para fornecer serviços de compartilhamento de arquivos e impressão para aplicativos da Microsoft?**

* SMTP (PT)
* O HTTP
* **SMB**
* DHCP em

**Explanation:**SMB é usado em redes da Microsoft para compartilhamento de arquivos e serviços de impressão. O sistema operacional Linux fornece um método de compartilhamento de recursos com redes da Microsoft usando uma versão do SMB chamada SAMB.

**53 - Sim. Qual dispositivo em uma abordagem de defesa em profundidade nega conexões iniciadas de redes não confiáveis a redes internas, mas permite que usuários internos dentro de uma organização se conectem a redes não confiáveis?**

* interruptor da camada de acesso
* **Firewall**
* router interno
* IPS

**Um** firewall é tipicamente uma segunda linha de defesa em uma abordagem de defesa em camadas para a segurança de rede. O firewall normalmente se conecta a um roteador de borda que se conecta ao provedor de serviços. O firewall rastreia as conexões iniciadas dentro da empresa e nega o início de conexões de redes não confiáveis externas que vão para redes internas confiáveis.

Quais são os dois possíveis problemas de rede que podem ocorrer pela operação ARP? (Escolha duas.)

**54. Quais são dois potenciais problemas de rede que podem resultar da operação ARP? (Escolha dois.)**

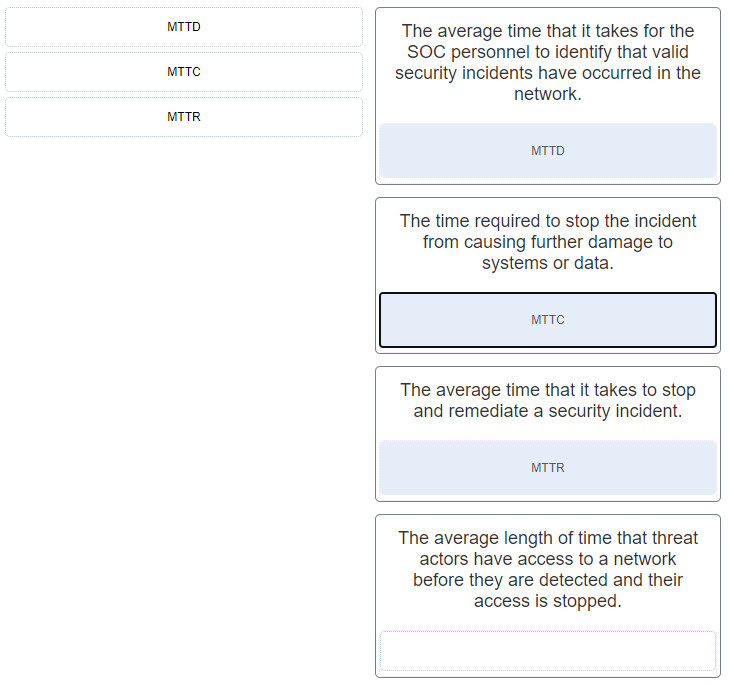
* Um grande número de transmissões de solicitação ARP pode fazer com que a tabela de endereços MAC do host transborde e impeça a comunicação do host na rede.
* Em grandes redes com baixa largura de banda, várias transmissões de ARP podem causar atrasos na comunicação de dados.
* **Os invasores de rede podem manipular mapeamentos de endereço MAC e endereço IP em mensagens ARP com a intenção de interceptar o tráfego de rede.**
* Várias respostas ARP resultam na tabela de endereços MAC do switch contendo entradas que correspondem aos endereços MAC dos hosts que estão conectados à porta de switch relevante.
* Configurar manualmente associações estáticas de ARP poderia facilitar a intoxicação por ARP ou a paródia de endereço MAC.

**55 - Sim. Quais são os três procedimentos do Sguil fornecidos aos analistas de segurança para tratar alertas? (Escolha três.)**

* **Escale um alerta incerto.**
* Correlacionar alertas semelhantes em uma única linha.
* **Categorize verdadeiros positivos.**
* Pivot para outras fontes e ferramentas de informação.
* Construa consultas usando Query Builder.
* **Expira falsos positivos.**

**Explicação:**Sguil é uma ferramenta para endereçar alertas. Três tarefas podem ser concluídas em Sguil para gerenciar alertas:

* Alertas que foram encontrados para ser falsos positivos podem ser expirados.
* Um alerta pode ser escalado se o analista de segurança cibernética não tiver certeza de como lidar com isso.
* Eventos que foram identificados como verdadeiros positivos podem ser categorizados.

**56 (em inglês). Combine a métrica SOC com a descrição. (Não se aplicam todas as opções.)**   


**57. Quais são os dois serviços fornecidos pela ferramenta NetFlow? (Escolha dois.)**

* Configuração do QoS
* **cobrança de rede baseada em uso**
* análise de log
* Monitorização da lista de acessos
* **Monitoramento de rede**

**O** NetFlow fornece eficientemente um conjunto importante de serviços para aplicativos IP, incluindo contabilidade de tráfego de rede, faturamento de rede baseado em uso, planejamento de rede, segurança, recursos de monitoramento de negação de serviço e monitoramento de rede.

**58 anos. Quais são as duas características de um vírus? (Escolha dois.)**

* Um vírus normalmente requer ativação do usuário final.
* Um vírus pode estar dormente e depois ativar em uma hora ou data específica.
* Um vírus se replica explora independentemente vulnerabilidades em redes.
* Um vírus tem uma vulnerabilidade proputista, um mecanismo de propagação e uma carga útil.
* Um vírus fornece ao invasor dados sensíveis, como senhas

**O** tipo de interação do usuário final necessária para iniciar um vírus é normalmente abrir um aplicativo, abrir uma página da Web ou ligar no computador. Uma vez ativado, um vírus pode infectar outros arquivos localizados no computador ou outros computadores na mesma rede.

**59. O que é uma característica de um cavalo de Tróia no que se refere à segurança da rede?**

* Demasiada informação é destinada a um bloco de memória particular, fazendo com que áreas de memória adicionais sejam afetadas.
* Quantidades extremas de dados são enviadas para uma interface de dispositivo de rede específica.
* Um dicionário eletrônico é usado para obter uma senha para ser usada para se infiltrar em um dispositivo de rede chave.
* O malware está contido em um programa executável aparentemente legítimo.

**Um** cavalo de Tróia realiza operações maliciosas sob o disfarce de um programa legítimo. Os ataques de negação de serviço enviam quantidades extremas de dados para uma interface de host ou dispositivo de rede específica. Ataques de senha usam dicionários eletrônicos na tentativa de aprender senhas. Os ataques de estouro do buffer de buffers de memória enviando muitas informações para um host para tornar o sistema inoperante.

**60 anos. Que técnica é usada em ataques de engenharia social?**

* enviar lixo por e-mail
* buffer overflow
* phishing
* man-in-the-middle

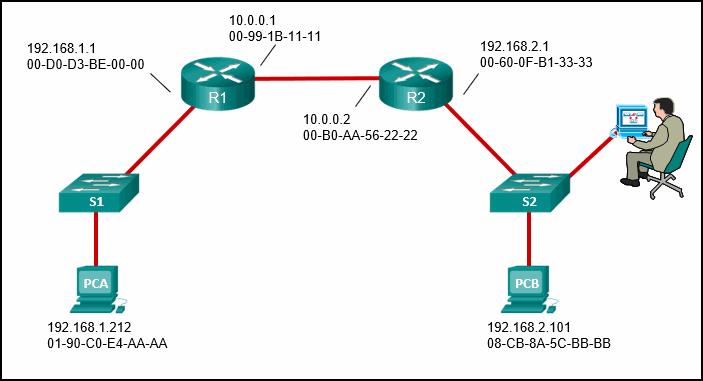
**Um** agente de ameaças envia e-mails fraudulentos que é disfarçado como sendo de uma fonte legítima e confiável para enganar o destinatário para instalar malware em seu dispositivo ou para compartilhar informações pessoais ou financeiras.

**61 - O que se é. Qual é o objetivo de implementar VLANs em uma rede?**

* Eles podem separar o tráfego do usuário.
* Eles evitam os loops da camada 2.
* Eliminam colisões de rede.
* Eles permitem que os switches encaminhem pacotes Layer 3 sem um roteador.

**As** VLANs são usadas em uma rede para separar o tráfego do usuário com base em fatores como função, equipe do projeto ou aplicativo, sem levar em conta a localização física do usuário ou dispositivo.

**62 - O que se refere ao seu nome. Consulte a exposição. Um analista de segurança cibernética está visualizando pacotes encaminhados pelo switch S2. Quais endereços identificarão quadros contendo dados enviados do PCA para o PCB?**



Endereço de Julho de Propriedade de Endereço: 192.168.2.1   
Endereço: 00-60-0F-B1-33-33   
Dst IP: 192.168.2.101   
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212   
Src MAC: 01-90-C0-E4-AA-AA   
Dst IP: 192.168.2.101   
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212   
Endereço: 00-60-0F-B1-33-33   
Dst IP: 192.168.2.101   
Dst MAC: 08-CB-8A-5C-BB-BB

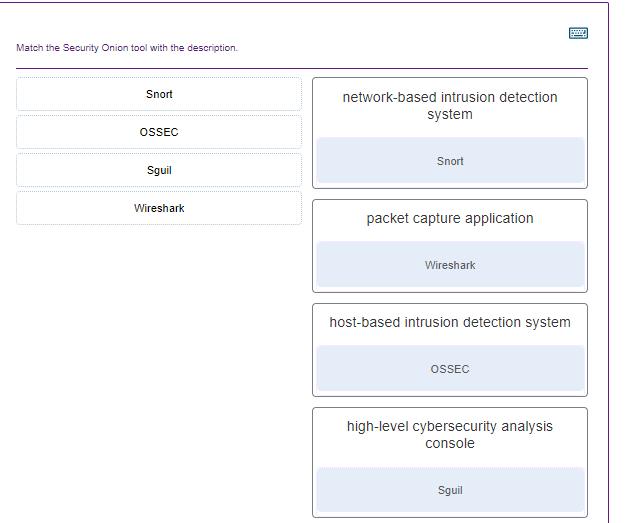
Src IP: 192.168.1.212   
Endereço: 00-60-0F-B1-33-33   
Dst IP: 192.168.2.101   
Dst MAC: 00-D0-D3-BE-00-00

**Quando** uma mensagem enviada do PCA para o PCB atinge o roteador R2, alguns campos de cabeçalho de quadro serão reescritos pelo R2 antes de encaminhar para alternar para alternar S2. Os quadros conterão o endereço MAC de origem do roteador R2 e o endereço MAC de destino do PCB. Os quadros manterão o endereçamento IPv4 original aplicado pelo PCA, que é o endereço IPv4 do PCA como o endereço de origem e o endereço IPv4 do PCB como destino.

**63 - O que se fala em matéria de ímpro que se o inserviram. Um analista de segurança cibernética precisa coletar dados de alerta. Quais são as três ferramentas de detecção para executar essa tarefa na arquitetura Security Onion? (Escolha três.)**

* CapME (é)
* Wazuh (Wazur)
* Kibana (Ianbana
* Zeek (é de Ze
* Sguil (guil)
* Wireshark (a)

**64. Combine a ferramenta de cebola de segurança com a descrição.**

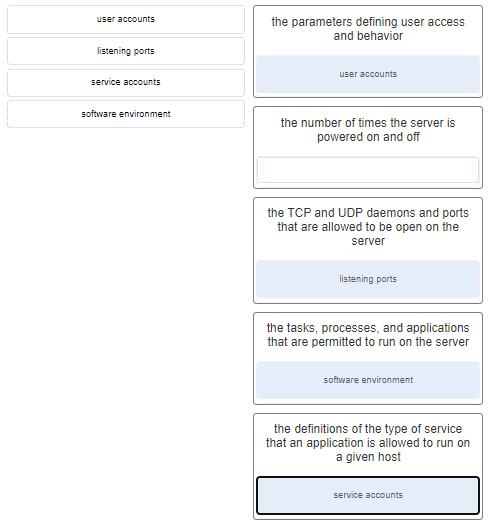


**65. Em avaliações de segurança de rede, que tipo de teste é usado para avaliar o risco representado por vulnerabilidades a uma organização específica, incluindo a avaliação da probabilidade de ataques e o impacto de explorações bem-sucedidas na organização?**

* varredura de porta
* análise de risco
* Teste de penetração
* avaliação da vulnerabilidade

Corresponda o elemento de perfil do servidor à descrição. (Nem todas as opções são usadas).

**66. Corresponder ao elemento perfil do servidor com a descrição. (Nem todas as opções são usadas.)**



**Explicação:** Os elementos de um perfil de servidor incluem o seguinte:Ouening ports – os daemons TCP e UDP e portas que podem ser abertas no servidor   
Contas de usuário – os parâmetros que definem o acesso e o comportamento do usuário   
Contas de serviço – as definições do tipo de serviço que um aplicativo pode executar em um determinado host   
Ambiente de software – as tarefas, processos e aplicativos que podem ser executados no servidor

**67 anos. Ao abordar um risco identificado, qual estratégia visa transferir parte do risco para outras partes?**

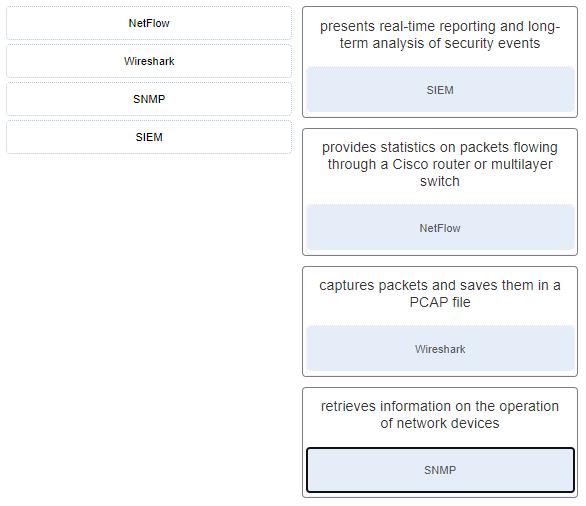
* Evitar o risco
* partilha de riscos
* retenção de risco
* Redução de risco

**68 - O que se encontra em Inglês. O que é um toque de rede?**

* Uma tecnologia usada para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança
* uma tecnologia Cisco que fornece estatísticas sobre pacotes que fluem através de um roteador ou switch multicamada
* um recurso suportado em switches Cisco que permite ao switch copiar quadros e encaminhá-los para um dispositivo de análise
* um dispositivo passivo que encaminha todos os erros de tráfego e camada física para um dispositivo de análise

**Uma** torneira **de** rede é usada para capturar o tráfego para monitorar a rede. O toque é tipicamente um dispositivo de divisão passiva implementado em linha na rede e encaminha todo o tráfego, incluindo erros de camada física, para um dispositivo de análise.

**69 - O que se quer dizer. Combine a ferramenta de monitoramento com a definição.**



**70. Se um SOC tem uma meta de 99,999% de tempo de atividade, quantos minutos de inatividade por ano seriam considerados dentro de sua meta?**

* Aproximadamente 5 minutos por ano.
* Aproximadamente 10 minutos por ano
* Aproximadamente 20 minutos por ano.
* Aproximadamente 30 minutos por ano.

**Explicação:** Dentro de um ano, há 365 dias x 24 horas por dia x 60 minutos por hora de 525.600 minutos. Com a meta de tempo de atividade 99,999% do tempo, o tempo de inatividade precisa ser controlado abaixo de 525.600 x (1-0.99999) x 5,256 minutos por ano.

**71 - O que se é com o que dizer. O servidor HTTP respondeu a uma solicitação de cliente com um código de status 200. O que indica esse código de status?**

* A solicitação é entendida pelo servidor, mas o recurso não será atendido.
* O pedido foi concluído com sucesso.
* O servidor não conseguiu encontrar o recurso solicitado, possivelmente por causa de um URL incorreto.
* O pedido foi aceite para processamento, mas o processamento não está concluído.

**72. Qual é uma vantagem para as pequenas organizações de adotar o IMAP em vez de POP?**

* O POP só permite que o cliente armazene mensagens de forma centralizada, enquanto o IMAP permite o armazenamento distribuído.
* IMAP envia e recupera e-mail, mas POP só recupera e-mail.
* Quando o usuário se conecta a um servidor POP, as cópias das mensagens são mantidas no servidor de e-mail por um curto período de tempo, mas o IMAP as mantém por um longo tempo.
* As mensagens são mantidas nos servidores de e-mail até que sejam excluídas manualmente do cliente de e-mail.

**Explanation:**IMAP e POP são protocolos que são usados para recuperar mensagens de e-mail. A vantagem de usar IMAP em vez de POP é que quando o usuário se conecta a um servidor compatível com IMAP, cópias das mensagens são baixadas para o aplicativo cliente. O IMAP armazena as mensagens de email no servidor até que o usuário exclua manualmente essas mensagens.

**73. Que ferramenta de segurança de depuração pode ser usada por chapéus pretos para fazer engenharia reversa de arquivos binários ao escrever explorações?**

* WinDbg (Diances)
* Ovelha de fogo
* Skipfish (esto)
* A A IDA (A

**74 anos. Quais são as três características de um sistema de gestão da segurança da informação? (Escolha três.)**

* Envolve a implementação de sistemas que rastreiam a localização e a configuração de dispositivos e softwares em rede em uma empresa.
* **É uma abordagem sistemática e multifacetada para a cibersegurança.**
* Ele aborda o inventário e controle de configurações de hardware e software de sistemas.
* **Consiste em um conjunto de práticas que são sistematicamente aplicadas para garantir a melhoria contínua da segurança da informação.**
* **Consiste em uma estrutura de gerenciamento através da qual uma organização identifica, analisa e aborda os riscos de segurança da informação.**
* É baseado na aplicação de servidores e dispositivos de segurança.

**Explicação:**Um Sistema de Gerenciamento de Segurança da Informação (ISMS) consiste em uma estrutura de gerenciamento através da qual uma organização identifica, analisa e aborda os riscos de segurança da informação. Os SGSIS não são baseados em servidores ou dispositivos de segurança. Em vez disso, um SGSI consiste em um conjunto de práticas que são sistematicamente aplicadas por uma organização para garantir a melhoria contínua da segurança da informação. Os SGSIS fornecem modelos conceituais que orientam as organizações no planejamento, implementação, governo e avaliação de programas de segurança da informação.

Os SGSIS são uma extensão natural do uso de modelos de negócios populares, como o Gerenciamento de Qualidade Total (TQM) e os Objetivos de Controle para a Informação e Tecnologias Relacionadas (COBIT), no campo da segurança cibernética.

Um SGSI é uma abordagem sistemática e multifacetada para a segurança cibernética. A abordagem inclui pessoas, processos, tecnologias e culturas em que interagem em um processo de gestão de riscos.

**75 anos. Quais são as três tecnologias que devem ser incluídas em um sistema de gerenciamento de informações e eventos de segurança SOC? (Escolha três.)**

* **coleta de eventos, correlação e análise**
* **Monitoramento de segurança**
* Autenticação do usuário
* Serviço de procuração
* prevenção de intrusão
* **Inteligência de ameaças**

**Explicação:** As tecnologias em um SOC devem incluir o seguinte:   
Coleta de eventos, correlação e análise   
? Monitoramento de segurança   
? Controle de segurança   
? Gestão de logs   
- Avaliação de vulnerabilidade   
- Rastreamento de vulnerabilidades   
? Inteligência de ameaça   
Servidor proxy, VPN e IPS são dispositivos de segurança implantados na infraestrutura de rede.

**76 - Sim. Que parte do URL, http://www.cisco.com/index.html, representa o domínio DNS de nível superior?**

* http (chata)
* www (com a
* **.com dobr**
* índice

**Explicação:** Os componentes do URL http://www.cisco.com/index.htm são os seguintes:   
http ? protocolo   
www - parte do nome do servidor   
cisco - parte do nome de domínio   
index ? nome do arquivo   
com ? o domínio de nível superior

**77. O que melhor descreve a ameaça à segurança de falsificar?**

* enviar e-mails em massa para indivíduos, listas ou domínios com a intenção de impedir que os usuários acessem o e-mail
* **enviar quantidades anormalmente grandes de dados para um servidor remoto para impedir o acesso do usuário aos serviços do servidor**
* interceptar o tráfego entre dois hosts ou inserir informações falsas no tráfego entre dois hosts
* fazer com que os dados pareçam vir de uma fonte que não é a fonte real

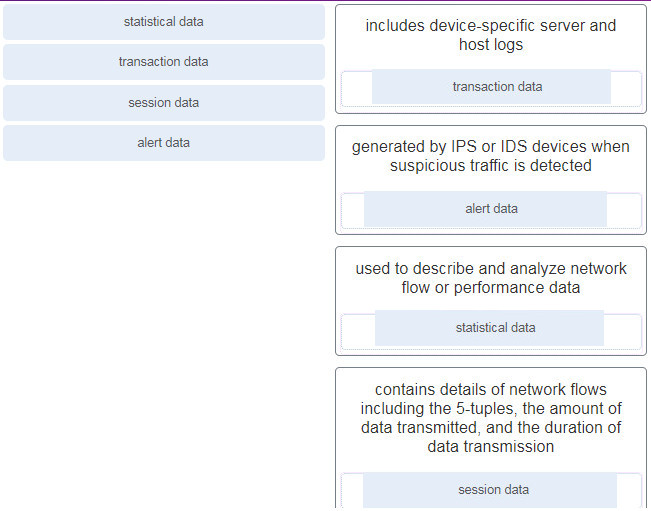
**78 anos. Uma empresa recém-criada tem quinze computadores com Windows 10 que precisam ser instalados antes que a empresa possa abrir para negócios. Qual é uma prática recomendada que o técnico deve implementar ao configurar o Firewall do Windows?**

* O técnico deve remover todas as regras de firewall padrão e negar seletivamente o tráfego de chegar à rede da empresa.
* **Após a implementação de software de segurança de terceiros para a empresa, o técnico deve verificar se o Firewall do Windows está desativado.**
* O técnico deve criar instruções para usuários corporativos sobre como permitir um aplicativo através do Firewall WIndows usando a conta Administrador.
* O técnico deve habilitar o Firewall do Windows para tráfego de entrada e instalar outro software de firewall para controle de tráfego de saída.

**Explicação: desabilite** apenas o Windows Firewall se outro software de firewall estiver instalado. Use o Firewall do Windows (Windows 7 ou 8) ou o Painel de Controle do Windows Defender (Windows 10) para ativar ou desativar o Firewall do Windows.

**79 - Em relação a isto que se fala em 79. Qual declaração define a diferença entre dados de sessão e dados de transação em logs?**

* Os dados de sessão analisam o tráfego de rede e prevê o comportamento da rede, enquanto os dados da transação registram as sessões de rede.
* Os dados de sessão são usados para fazer previsões sobre comportamentos de rede, enquanto os dados de transação são usados para detectar anomalias de rede.
* **Os dados de sessão registram uma conversa entre hosts, enquanto os dados da transação se concentram no resultado de sessões de rede.**
* Os dados de sessão mostram o resultado de uma sessão de rede, enquanto os dados da transação são em resposta ao tráfego de ameaças à rede.

**80 anos. Combine o tipo de dados de monitoramento de rede com a descrição.**   


**81 anos. Qual dispositivo suporta o uso do SPAN para permitir o monitoramento de atividades maliciosas?**

* **Interruptor do Cisco Catalyst**
* Outros produtos Cisco IronPort
* Cisco NAC (Ao)
* Agente de segurança da Cisco

**82 anos. Qual termo é usado para descrever consultas automatizadas que são úteis para adicionar eficiência ao fluxo de trabalho de operações cibernéticas?**

* Cadeia de ciber-matte
* **Livro de reprodução**
* Cadeia de custódia
* rootkit

**Um** manual é uma consulta automatizada que pode adicionar eficiência ao fluxo de trabalho de operações cibernéticas.

**83 - Sim. Quando as ACLs são configuradas para bloquear a paródia de endereço IP e os ataques de inundação do DoS, qual mensagem ICMP deve ser permitida tanto de entrada quanto de ida?**

* resposta de eco
* inacessíveis
* quera de origem
* **Eco**

**84 anos de existência. Depois que uma ferramenta de monitoramento de segurança identifica um anexo de malware entrando na rede, qual é o benefício de realizar uma análise retrospectiva?**

* Ele pode identificar como o malware entrou originalmente na rede.
* **Uma análise retrospectiva pode ajudar a rastrear o comportamento do malware a partir do ponto de identificação.**
* Pode calcular a probabilidade de um incidente futuro.
* Pode determinar qual host de rede foi afetado pela primeira vez.

**O** monitoramento de segurança geral pode identificar quando um anexo de malware entra em uma rede e qual host é infectado pela primeira vez. A análise retrospectiva dá o próximo passo e é o rastreamento do comportamento do malware a partir desse ponto.

**85 anos. Quais dois tipos de dados seriam classificados como informações pessoalmente identificáveis (PII)? (Escolha dois.)**

* leitura do termostato da casa
* Número médio de bovinos por região
* **Número de identificação do veículo**
* uso de emergência hospitalar por região
* **Fotografias do Facebook**

**86 (em inglês). Um técnico de help desk percebe um aumento do número de chamadas relacionadas ao desempenho dos computadores localizados na fábrica. O técnico acredita que as botnets estão causando o problema. Quais são os dois propósitos das botnets? (Escolha dois.)**

* **para transmitir vírus ou spam para computadores na mesma rede**
* para gravar todos e quaisquer teclas
* **para atacar outros computadores**
* para reter o acesso a um computador ou arquivos até que o dinheiro tenha sido pago
* para ter acesso à parte restrita do sistema operacional

**Explanation:** Botnets podem ser usados para realizar ataques DDoS, obter dados ou transmitir malware para outros dispositivos na rede.

**87 - O que se fala em: 87. Quais duas afirmações descrevem o uso de algoritmos assimétricos? (Escolha dois.)**

* As chaves públicas e privadas podem ser usadas de forma intercambiável.
* **Se uma chave pública for usada para criptografar os dados, uma chave privada deve ser usada para descriptografar os dados.**
* Se uma chave pública for usada para criptografar os dados, uma chave pública deve ser usada para descriptografar os dados.
* **Se uma chave privada for usada para criptografar os dados, uma chave pública deve ser usada para descriptografar os dados.**
* Se uma chave privada for usada para criptografar os dados, uma chave privada deve ser usada para descriptografar os dados.

**Explicação:** Algoritmos assimétricos usam duas chaves: uma chave pública e uma chave privada. Ambas as chaves são capazes do processo de criptografia, mas a chave correspondente complementar é necessária para a descriptografia. Se uma chave pública criptografar os dados, a chave privada correspondente descriptografa os dados. O contrário também é verdade. Se uma chave privada criptografar os dados, a chave pública correspondente descriptografa os dados.

**88 - Sim. Quais são os três serviços de segurança fornecidos pelas assinaturas digitais? (Escolha três.)**

* **Fornece confidencialidade de dados assinados digitalmente**
* Os dados de garantias não foram alterados em trânsito
* fornece não-repúdio usando funções HMAC
* **Fornece a encriptação de dados**
* **Autenticada a fonte**
* Autenticada o destino

**89 anos. Quais são os dois métodos para manter o status de revogação de certificados? (Escolha dois.)**

* **CRL (A)**
* DNS
* subordinado CA
* **OCSP em OCSP**
* LDAP em

**Um** certificado digital pode precisar ser revogado se sua chave for comprometida ou não for mais necessária. A lista de revogação de certificados (CRL) e o protocolo de status de certificado on-line (OCSP) são dois métodos comuns para verificar o status de revogação de certificado.

**90 - Sim. Quais são os dois usos de uma lista de controle de acesso? (Escolha dois.)**

* **As ACLs fornecem um nível básico de segurança para acesso à rede.**
* **As ACLs podem controlar quais áreas um host pode acessar em uma rede.**
* As ACLs padrão podem restringir o acesso a aplicativos e portas específicas.
* As ACLs ajudam o roteador a determinar o melhor caminho para um destino.
* As ACLs podem permitir ou negar o tráfego com base no endereço MAC originado no roteador.

**Explicação:** As ACLs podem ser usadas para o seguinte: Limitar o tráfego de rede para fornecer um desempenho adequado da rede   
Restringir a entrega de atualizações de roteamento   
Fornecer um nível básico de segurança   
Filtre o tráfego com base no tipo de tráfego que está sendo enviado   
Filtre o tráfego com base no endereçamento IP

**91 (em que precede o tempo). Um cliente está usando o SLAAC para obter um endereço IPv6 para a interface. Depois que um endereço foi gerado e aplicado à interface, o que o cliente deve fazer antes de começar a usar esse endereço IPv6?**

* Ele deve enviar uma mensagem de solicitação de roteador ICMPv6 para determinar qual gateway padrão ele deve usar.
* Ele deve enviar uma mensagem de solicitação de roteador ICMPv6 para solicitar o endereço do servidor DNS.
* **Deve enviar uma mensagem de solicitação de vizinho ICMPv6 para garantir que o endereço ainda não esteja em uso na rede.**
* Ele deve esperar por uma mensagem de anúncio do roteador ICMPv6 dando permissão para usar esse endereço.

**O** DHCPv6 alonos usa um servidor DHCPCP6, mas **o** Stateless Address Autoconfiguration (SLAAC) não. Um cliente SLAAC pode gerar automaticamente um endereço baseado em informações de roteadores locais por meio de mensagens de publicidade do roteador (RA). Uma vez que um endereço foi atribuído a uma interface via SLAAC, o cliente deve garantir através de Detecção de Endereço de Duplicado (DAD) que o endereço ainda não está em uso. Ele faz isso enviando uma mensagem de solicitação de vizinhança ICMPv6 e ouvindo uma resposta. Se uma resposta for recebida, isso significa que outro dispositivo já está usando esse endereço.

**92 - O que se passa com o que dizer. Um técnico está solucionando problemas de conectividade de rede. Pings para o roteador sem fio local são bem sucedidos, mas os pings para um servidor na Internet não são bem sucedidos. Qual comando CLI poderia ajudar o técnico a encontrar a localização do problema de rede?**

* **tracert**
* ipconfig (
* msconfig (
* ipconfig/renew

**Explicação:** A utlility tracert (também conhecida como o comando tracert ou ferramenta tracert) permitirá que o técnico localize o link para o servidor que está incerto. O comando ipconfig exibe os detalhes de configuração da rede do computador. O comando ipconfig/renew solicita um endereço IP de um servidor DHCP. O Msconfig não é um comando de solução de problemas de rede.

**93. Quais são as duas técnicas de evasão usadas por hackers? (Escolha dois.)**

* Cavalo de Tróia
* **pivot**
* **rootkit**
* reconhecimento
* phishing

**Os** seguintes métodos são usados por hackers para evitar a detecção:Encriptação e tunelamento – ocultar ou embaralhar o conteúdo do malware   
Exaustão de recursos – mantém o dispositivo host muito ocupado para detectar a invasão   
Fragmentação do tráfego – divide o malware em vários pacotes   
Interpretação incorreta em nível de protocolo – se esgueira pelo firewall   
Pivot – usa um dispositivo de rede comprometido para tentar acessar outro dispositivo   
Rootkit – permite que o hacker não seja detectado e o software de couro instalado pelo hacker

**94. Quando um ataque de segurança ocorreu, quais duas abordagens devem tomar para mitigar um sistema comprometido durante a etapa Ações de Objetivos, conforme definido pelo modelo Cyber Kill Chain? (Escolha dois.)**

* **Realizar análise forense de endpoints para triagem rápida.**
* Treine desenvolvedores web para proteger o código.
* Construa detecções para o comportamento de malware conhecido.
* Colete arquivos de malware e metadados para análise futura.
* **Detecte a exfiltração de dados, o movimento lateral e o uso de credenciais não autorizada.**

**Quando** os profissionais de segurança são alertados sobre os compromissos do sistema, a análise forense dos endpoints deve ser realizada imediatamente para triagem rápida. Além disso, os esforços de detecção para atividades de ataque, como exfiltração de dados, movimento lateral e uso de credenciais não autorizadas, devem ser aprimorados para reduzir os danos ao mínimo.

**95 anos. Coloque as sete etapas definidas na Cyber Kill Chain na ordem correta.**   


**96 anos. Quais são os três objetivos de um ataque de varredura de porta? (Escolha três.)**

* para identificar configurações periféricas
* **para determinar possíveis vulnerabilidades**
* para desativar os portos e serviços usados
* **para identificar os sistemas operacionais**
* **para identificar serviços ativos**
* para descobrir senhas do sistema

**97. Qual campo no cabeçalho TCP indica o status do processo de aperto de mão de três vias?**

* **bits de controle**
* Janela de janela
* Reservados
* checksum

**O** valor nos bits de controle do cabeçalho do cabeçalho TCP indica o progresso e o status da conexão.

**98. Um usuário abre três navegadores no mesmo PC para acessar www.cisco.com para procurar informações do curso de certificação. O servidor web da Cisco envia um datagrama como uma resposta à solicitação de um dos navegadores da Web. Quais informações são usadas pela pilha de protocolo TCP/IP no PC para identificar quais dos três navegadores da Web devem receber a resposta?**

* o endereço IP da fonte
* **o número da porta de destino**
* Endereço IP de destino
* o número da porta de origem

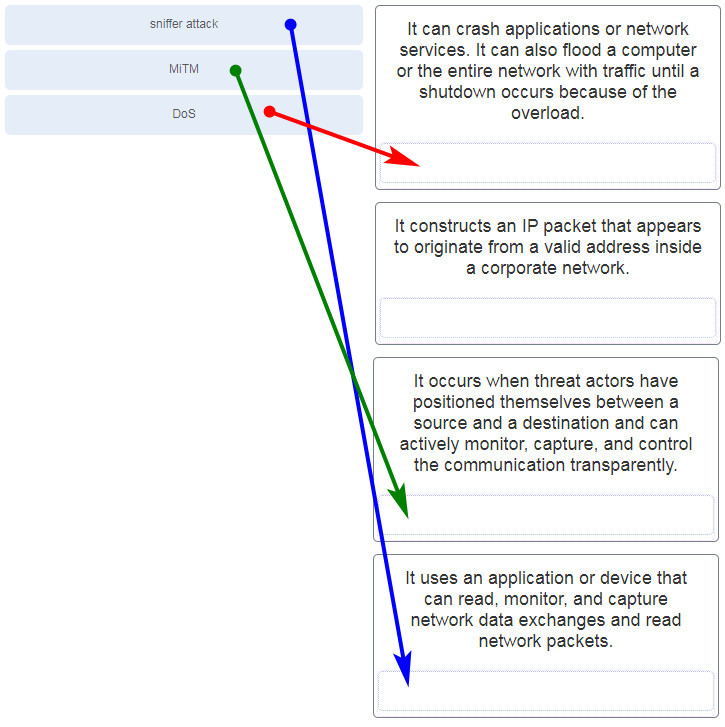
**Cada** aplicativo cliente do navegador da Web abre um número de porta gerado aleatoriamente no intervalo das portas registradas e usa esse número como o número da porta de origem no datagrama que ele envia para um servidor. O servidor então usa esse número de porta como o número da porta de destino no datagrama de resposta que ele envia para o navegador da web. O PC que está executando o aplicativo do navegador da Web recebe o datagrama e usa o número da porta de destino contido neste datagrama para identificar o aplicativo cliente.

**99. Quais são os dois cenários em que a análise de segurança probabilística é mais adequada? (Escolha dois.)**

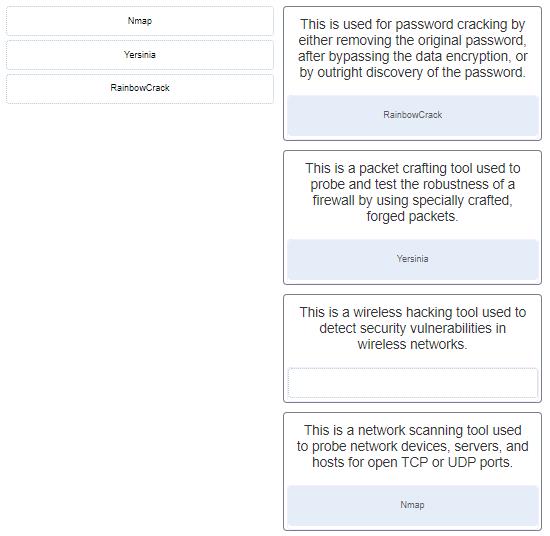
* quando aplicações que estão em conformidade com os padrões de aplicação/rede de rede são analisadas
* **ao analisar eventos com a suposição de que seguem etapas predefinidas**
* quando variáveis aleatórias criam dificuldade em conhecer com certeza o resultado de qualquer evento
* **ao analisar aplicativos projetados para contornar firewalls**
* Quando cada evento é o resultado inevitável de causas antecedentes

**100. Qual ferramenta é um aplicativo da Web que fornece ao analista de segurança cibernética um meio de fácil leitura de visualizar uma sessão inteira da Camada 4?**

* Snort (su-t
* Zeek (é de Ze
* **CapME (é)**
* OSSEC em OSSEC

**101. Combine a categoria de ataques com a descrição. (Nem todas as opções são usadas.)**   


**102. Combine as ferramentas de ataque com a descrição. (Nem todas as opções são usadas.)**



**103. Quais são as duas características do ARP? (Escolha dois.)**

* Quando um host está encapsulando um pacote em um quadro, ele se refere à tabela de endereços MAC para determinar o mapeamento de endereços IP para endereços MAC.
* Se um host estiver pronto para enviar um pacote para um dispositivo de destino local e tiver o endereço IP, mas não o endereço MAC do destino, ele gera uma transmissão ARP.
* Se um dispositivo que recebe uma solicitação ARP tiver o endereço IPv4 de destino, ele responderá com uma resposta ARP.
* Se nenhum dispositivo responder à solicitação ARP, o nó de origem transmitirá o pacote de dados para todos os dispositivos no segmento de rede.
* Uma solicitação ARP é enviada para todos os dispositivos na LAN Ethernet e contém o endereço IP do host de destino e o endereço MAC multicast.

**Quando** um nó encapsula um pacote de dados em um quadro, ele precisa do endereço MAC de destino. Primeiro, determina se o dispositivo de destino está na rede local ou em uma rede remota. Em seguida, ele verifica a tabela ARP (não a tabela MAC) para ver se existe um par de endereços IP e endereço MAC para o endereço IP de destino (se o host de destino estiver na rede local) ou o endereço IP do gateway padrão (se o host de destino estiver em uma rede remota). Se a correspondência não existir, gera uma transmissão ARP para procurar o endereço IP para resolução de endereço MAC. Como o endereço MAC de destino é desconhecido, a solicitação ARP é transmitida com o endereço MAC FFFF.FFFF.FFFFFF.FFFF. O dispositivo de destino ou o gateway padrão responderá com seu endereço MAC, que permite que o nó de envio monte o quadro. Se nenhum dispositivo responder à solicitação ARP, o nó de origem descartará o pacote porque um quadro não pode ser criado.

**104 anos. O que é uma propriedade da tabela ARP em um dispositivo?**

* As entradas em uma tabela ARP são carimbadas e são expurgadas após o tempo limite expirar.
* Cada sistema operacional usa o mesmo temporizador para remover entradas antigas do cache ARP.
* As entradas de endereço IP-to-MAC estáticas são removidas dinamicamente da tabela ARP.
* Os sistemas operacionais Windows armazenam entradas de cache ARP por 3 minutos.

**105. Qual é o propósito do Tor?**

* para permitir que os usuários naveguem na Internet anonimamente
* para se conectar com segurança a uma rede remota através de um link inseguro, como uma conexão com a Internet
* para doar ciclos de processador para tarefas computacionais distribuídas em um processador compartilhando rede P2P
* para inspecionar o tráfego de entrada e procurar qualquer que viole uma regra ou corresponda à assinatura de um exploit conhecido

**O** Tor é uma plataforma de software e rede de hosts peer-to-peer (P2P) que funcionam como roteadores. Os usuários acessam a rede Tor usando um navegador especial que lhes permite navegar anonimamente.

**106. Quais são as duas técnicas usadas em um ataque de smurf? (Escolha dois.)**

* Sequestro de sessão
* Exaustão de recursos
* Botnets (ebotnets
* **amplificação**
* **A reflexão**

**No 107. Qual é o objetivo principal de uma plataforma de inteligência de ameaças (TIP)?**

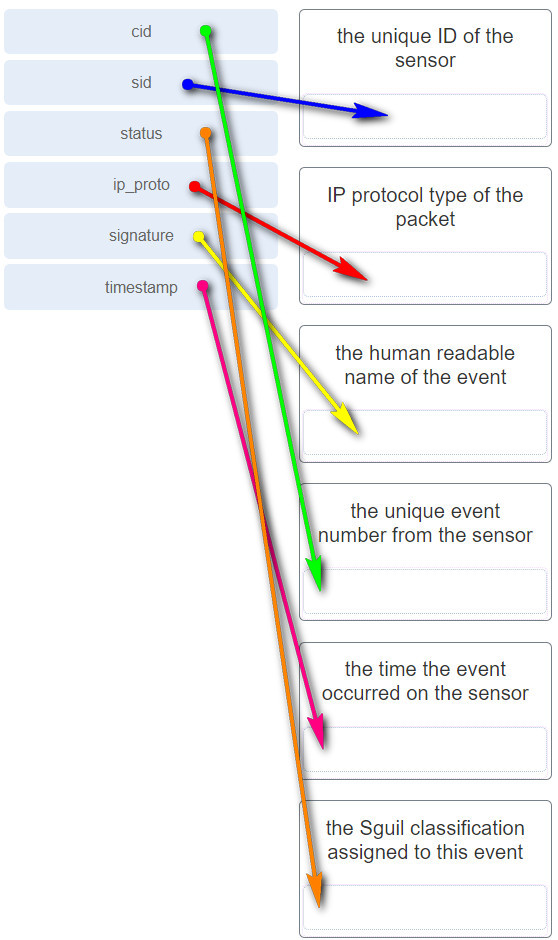
* agregar os dados em um só lugar e apresentá-lo em um formato compreensível e utilizável
* fornecer uma especificação para um protocolo de camada de aplicativo que permite a comunicação de CTI sobre HTTPS
* fornecer um esquema padronizado para especificar, capturar, caracterizar e comunicar eventos e propriedades de operações de rede
* **fornecer uma plataforma de operações de segurança que integre e aprimore diversas ferramentas de segurança e inteligência de ameaças**

**108 anos. Qual parâmetro sem fio é usado por um ponto de acesso para transmitir quadros que incluem o SSID?**

* Modo de segurança
* Modo ativo
* **modo passivo**
* configuração do canal

**Explicação:** Os dois modos de digitalização ou sondagem em que um ponto de acesso pode ser colocado são passivos ou ativos. No modo passivo, o AP anuncia o SSID, padrões suportados e configurações de segurança em quadros de farol de transmissão. No modo ativo, o cliente sem fio deve ser configurado manualmente para os mesmos parâmetros sem fio que o AP tenha configurado.

**109. Combine o campo na tabela de eventos de Sguil com a descrição.**

Combine o campo na tabela de eventos de Sguil com a descrição

**110. Um funcionário se conecta sem fio à rede da empresa usando um telefone celular. O funcionário então configura o celular para atuar como um ponto de acesso sem fio que permitirá que novos funcionários se conectem à rede da empresa. Qual é o tipo de ameaça de segurança que melhor descreve essa situação?**

* **Ponto de acesso desonesto**
* cracking
* A negação do serviço
* spoofing

**111. Quais informações são necessárias para uma consulta WHOIS?**

* Fora do endereço global do cliente
* Endereço do servidor de lookup da ICANN
* Link-local endereçamento do proprietário do domínio
* **FQDN do domínio**

**112. Quais duas afirmações descrevem as características dos algoritmos simétricos? (Escolha dois.)**

* **Eles são referidos como uma chave pré-compartilhada ou chave secreta.**
* Eles usam um par de uma chave pública e uma chave privada.
* **Eles são comumente usados com tráfego VPN.**
* Eles fornecem confidencialidade, integridade e disponibilidade.

**Explicação:** Os algoritmos de criptografia simétrica usam a mesma chave (também chamada de segredo compartilhado) para criptografar e descriptografar os dados. Em contraste, os algoritmos de criptografia assimétrica usam um par de chaves, uma para criptografia e outra para descriptografia.

**113. Quais são duas desvantagens para usar o HIPS? (Escolha dois.)**

* Com o HIPS, o sucesso ou o fracasso de um ataque não pode ser prontamente determinado.
* **Com o HIPS, o administrador de rede deve verificar o suporte para todos os diferentes sistemas operacionais usados na rede.**
* **O HIPS tem dificuldade em construir uma imagem de rede precisa ou coordenar eventos que ocorrem em toda a rede.**
* Se o fluxo de tráfego de rede for criptografado, o HIPS não conseguirá acessar formulários não criptografados do tráfego.
* As instalações HIPS são vulneráveis a ataques de fragmentação ou ataques TTL variáveis

**114. Quais são as três funções fornecidas pelo serviço syslog? (Escolha três.)**

* **para selecionar o tipo de informação de registro que é capturada**
* para periodicamente enquete agentes para dados
* para fornecer estatísticas sobre pacotes que estão fluindo através de um dispositivo Cisco
* para fornecer análise de tráfego
* **para coletar informações de registro para monitoramento e solução de problemas**
* **para especificar os destinos das mensagens capturadas**

**Explicação:**Existem três funções principais fornecidas pelo serviço syslog:

1. coleta de informações de registro
2. seleção do tipo de informação a ser registada
3. seleção do destino das informações registradas

**115 ('). Qual consideração é importante na implementação do syslog em uma rede?**

* Habilite o nível mais alto de syslog disponível para garantir o registro de todas as mensagens de eventos possíveis.
* **Sincronize relógios em todos os dispositivos de rede com um protocolo como o Network Time Protocol.**
* Registre todas as mensagens para o buffer do sistema para que elas possam ser exibidas ao acessar o roteador.
* Use SSH para acessar informações do syslog

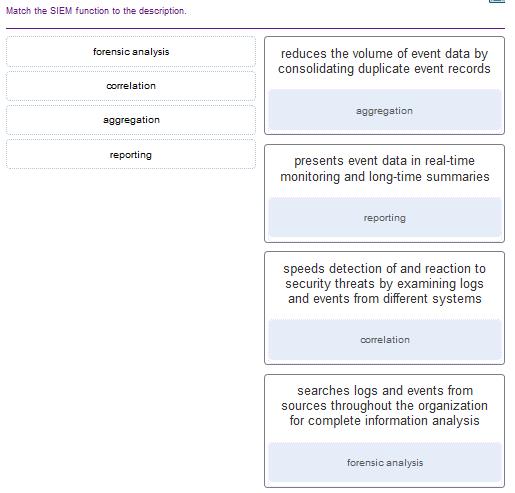
**116 anos. 116 Quais são as duas maneiras pelas quais os agentes de ameaças usam o NTP? (Escolha dois.)**

* Eles colocam um anexo dentro de uma mensagem de e-mail.
* **Eles atacam a infraestrutura do NTP para corromper as informações usadas para registrar o ataque.**
* Eles colocam iFrames em uma página da web corporativa frequentemente usada.
* Eles codificam dados roubados como a parte do subdomínio onde o nomeador está sob controle de um invasor.
* **Os agentes de ameaças usam sistemas NTP para direcionar ataques DDoS.**

**117 (em inglês). Quais são os dois recursos incluídos pelos protocolos TACACS+ e RADIUS? (Escolha dois.)**

* criptografia de senha
* **Processos separados de autenticação e autorização**
* Suporte do SIP
* **utilização dos protocolos da camada de transporte**
* Suporte do 802.1X

**Explicação:** Tanto a criptografia de senha de suporte TACACS+ quanto RADIUS (TACACS+ criptografa toda a comunicação) e usam o protocolo Layer 4 (TACACS+ usa TCP e RADIUS usa UDP). O TACACS+ suporta a separação dos processos de autenticação e autorização, enquanto o RADIUS combina autenticação e autorização como um processo. O RADIUS suporta a tecnologia de acesso remoto, como 802.1x e SIP; TACACS+ não.

**118 (em (em). 118 Combine a função SIEM com a descrição.**   


**119 (em inglês). Quais são os dois tipos de ataques usados em resolvedores abertos de DNS? (Escolha dois.)**

* **Amplificação e reflexão**
* Fluxo rápido
* Envenenamento de ARP
* **utilização de recursos**
* amortecimento

**Três** tipos de ataques usados em resolvedores abertos de DNS são os seguintes:DS cache envenenamento por cache – o invasor envia informações falsificadas para redirecionar usuários de sites legítimos para sites maliciosos   
Amplificação de DNS e ataques de reflexão – o invasor envia um volume aumentado de ataques para mascarar a verdadeira fonte do ataque   
Ataques de utilização de recursos de DNS – um ataque de negação de serviço (DoS) que consome recursos do servidor

**120. Qual firewall baseado em host usa uma abordagem de três perfis para configurar a funcionalidade de firewall?**

* iptables (esufláveis)
* Firewall do Windows
* **nftables em**
* TCP Wrapper em

**121. Qual protocolo ou serviço usa UDP para uma comunicação cliente-a-servidor e TCP para comunicação servidor-a-servidor?**

* O HTTP
* FTP (PT)
* **DNS**
* SMTP (PT)

**Explicação:** Algumas aplicações podem usar TCP e UDP. O DNS usa UDP quando os clientes enviam solicitações para um servidor DNS e o TCP quando dois DNS servem diretamente.

**122. Quais dois protocolos de rede podem ser usados por um agente de ameaças para extrofiar dados no tráfego que é disfarçado como tráfego de rede normal? (Escolha dois.)**

* NTP em
* DNS
* O HTTP
* syslog (peslo)
* SMTP (PT)

**123 (em Inglês). Qual é a diferença fundamental entre os dados capturados pelo NetFlow e os dados capturados pela Wireshark?**

* Os dados do NetFlow mostram o conteúdo do fluxo de rede, enquanto os dados do Wireshark mostram as estatísticas de fluxo de rede.
* Os dados do NetFlow são analisados por tcpdump enquanto os dados do Wireshark são analisados por nfdump.
* O NetFlow fornece dados de transação, enquanto o Wireshark fornece dados de sessão.
* O NetFlow coleta metadados de um fluxo de rede, enquanto o Wireshark captura pacotes de dados completos.

**O** Wireshark captura todo o conteúdo de um pacote. O NetFlow não. Em vez disso, o NetFlow coleta metadados ou dados sobre o fluxo.

**124. Qual ferramenta captura pacotes de dados completos apenas com uma interface de linha de comando?**

* nfdump (la de rú
* Wireshark (a)
* NBAR2 (
* Tcpdump (cidade)

**Explicação:** A ferramenta de linha de comando tcpdump é um analisador de pacotes. Wireshark é um analisador de pacotes com uma interface GUI.

Qual método pode ser usado para proteger um dispositivo?

**125 anos. Qual método pode ser usado para endurecer um dispositivo?**

* Manter o uso das mesmas senhas
* permitir que os serviços padrão permaneçam ativados
* permitir a detecção automática de USB
* usar SSH e desativar o acesso à conta raiz sobre SSH

**As** melhores práticas básicas para o endurecimento dos dispositivos são as seguintes:   
Garanta a segurança física.   
Minimize os pacotes instalados.   
Desativar serviços não utilizados.   
Use o SSH e desabilite o login da conta raiz sobre SSH.   
Mantenha o sistema atualizado.   
Desativar a detecção automática USB.   
Apurre senhas fortes.   
Forçar alterações periódicas de senha.   
Impedir que os usuários reutilizem senhas antigas.   
Revise os registros regularmente.

**126 (em Inglês, 126). Em um sistema operacional Linux, qual componente interpreta os comandos do usuário e tenta executá-los?**

* GUI (A GUI
* daemon (em of
* kernel (
* Concha de con

**127 (em inglês). Um administrador de rede está configurando um servidor AAA para gerenciar a autenticação RADIUS. Quais são os dois recursos incluídos na autenticação RADIUS? (Escolha dois.)**

* criptografia para todas as comunicações
* criptografia apenas para os dados
* Processo único para autenticação e autorização
* processos separados para autenticação e autorização
* Senhas ocultas durante a transmissão

**128 - É o 128. O que é a escalada de privilégios?**

* Vulnerabilidades em sistemas são exploradas para conceder níveis mais elevados de privilégio do que alguém ou algum processo deveria ter.
* Todo mundo recebe plenos direitos por padrão para tudo e os direitos são retirados somente quando alguém abusa de privilégios.
* Alguém recebe direitos porque recebeu uma promoção.
* Um problema de segurança ocorre quando funcionários corporativos de alto escalão exigem direitos sobre sistemas ou arquivos que eles não deveriam ter.

**Com** a escalada de privilégios, vulnerabilidades são exploradas para conceder níveis mais elevados de privilégio. Depois que o privilégio é concedido, o agente de ameaça pode acessar informações confidenciais ou assumir o controle do sistema.

**129 anos. 129 Que duas garantias a assinatura digital fornece sobre o código que é baixado da Internet? (Escolha dois.)**

* O código não contém vírus.
* O código não foi modificado desde que deixou o editor de software.
* O código é autêntico e é realmente originado pelo editor.
* O código não contém erros.
* O código foi criptografado com uma chave privada e pública.

**Explicação:** Assinatura digital de código fornece várias garantias sobre o código:   
O código é autêntico e é realmente originado pelo editor.   
O código não foi modificado desde que deixou o editor de software.   
A editora publicou inegavelmente o código. Isso fornece não-repúdio do ato de publicação.

**130. Uma empresa de TI está recomendando o uso de aplicativos PKI para trocar informações com segurança entre os funcionários. Em que dois casos uma organização pode usar aplicativos PKI para trocar informações com segurança entre usuários? (Escolha dois.)**

* Serviço Web HTTPS
* Autenticação 802.1x
* Servidor NTP local
* Transferências de FTP
* permissão de acesso de arquivo e diretório

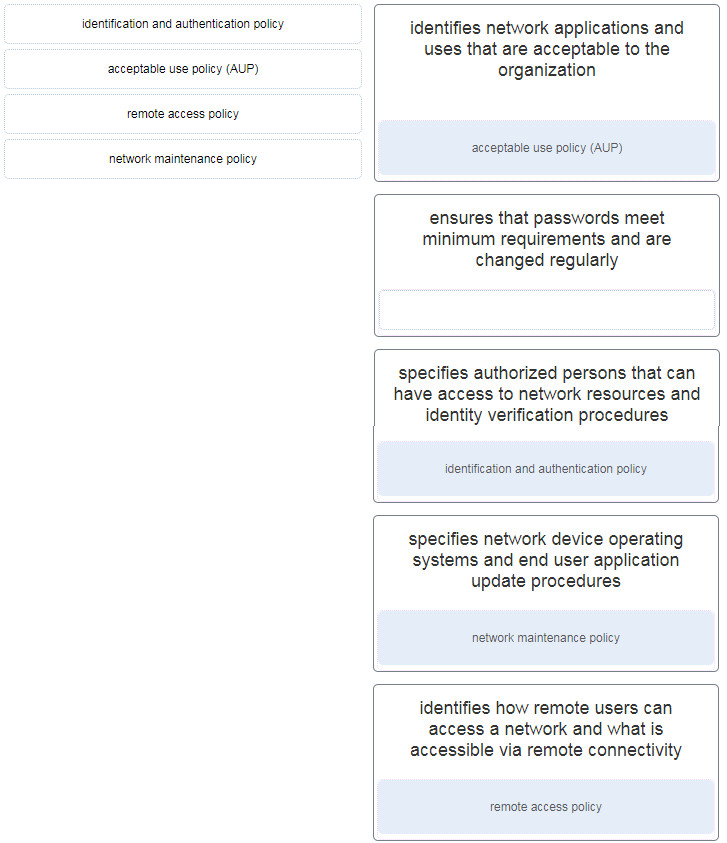
**131. Que medida pode um analista de segurança fazer para realizar um monitoramento de segurança eficaz contra o tráfego de rede criptografado pela tecnologia SSL?**

* Use um servidor Syslog para capturar o tráfego de rede.
* Implante um Cisco SSL Appliance.
* Exigir conexões de acesso remoto através da VPN IPsec.
* Implante um Cisco ASA.

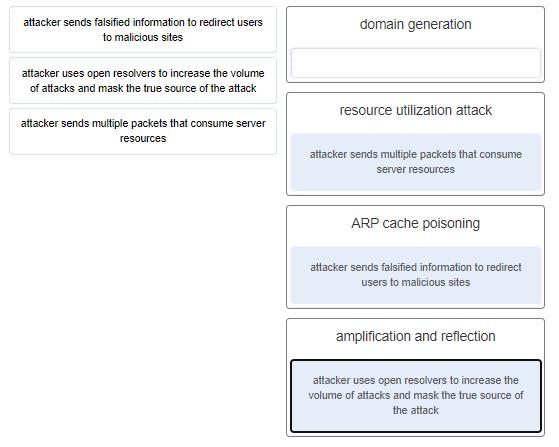
**132. Um administrador está tentando desenvolver uma política de segurança BYOD para funcionários que estão trazendo uma ampla gama de dispositivos para se conectar à rede da empresa. Quais os três objetivos que a política de segurança BYOD deve abordar? (Escolha três.)**

* Todos os dispositivos devem ser segurados contra responsabilidade se usados para comprometer a rede corporativa.
* Todos os dispositivos devem ter autenticação aberta com a rede corporativa.
* Os direitos e atividades permitidos na rede corporativa devem ser definidos.
* As salvaguardas devem ser colocadas em prática para que qualquer dispositivo pessoal seja comprometido.
* O nível de acesso dos funcionários ao se conectar à rede corporativa deve ser definido.
* Todos os dispositivos devem ser autorizados a se conectar à rede corporativa perfeitamente.

**133. Combine a política de segurança com a descrição. (Nem todas as opções são usadas.)**



**134. Combine o ataque com a definição. (Nem todas as opções são usadas.)**



**135. Que tipo de ataque tem como alvo um banco de dados SQL usando o campo de entrada de um usuário?**

* Injeção de XML
* buffer overflow
* Roteiro entre sites
* Injeção de SQL

**Um** criminoso pode inserir uma instrução SQL maliciosa em um campo de entrada em um site onde o sistema não filtra a entrada do usuário corretamente.

**136. Quais são as duas características dos endereços MAC Ethernet? (Escolha dois.)**

* Os endereços MAC usam uma estrutura hierárquica flexível.
* Eles são expressos como 12 dígitos hexadecimais.
* Eles são globalmente únicos.
* Eles são rotíveis na internet.
* Os endereços MAC devem ser exclusivos para interfaces Ethernet e serial em um dispositivo.

**137 (em inglês). Um usuário chama para relatar que um PC não pode acessar a internet. O técnico de rede pede ao usuário que emita o comando ping 127.0.0.1em uma janela de prompt de comando. O usuário relata que o resultado é quatro respostas positivas. Que conclusão pode ser tirada com base neste teste de conectividade?**

* O endereço IP obtido a partir do servidor DHCP está correto.
* O PC pode acessar a rede. O problema existe além da rede local.
* O PC pode acessar a Internet. No entanto, o navegador não pode funcionar.
* A implementação TCP/IP é funcional.

**138 ('). 138 O que caracteriza um agente de ameaças?**

* Eles são todos indivíduos altamente qualificados.
* Eles sempre usam ferramentas avançadas para lançar ataques.
* Eles sempre tentam causar algum dano a um indivíduo ou organização.
* Todos pertencem ao crime organizado.

**139 (em Inglês) Um computador está apresentando um usuário com uma tela solicitando pagamento antes que os dados do usuário possam ser acessados pelo mesmo usuário. Que tipo de malware é esse?**

* Um tipo de bomba lógica
* Um tipo de vírus
* Um tipo de worm
* Um tipo de ransomware

**Explicação:** Ransomware geralmente criptografa dados em um computador e torna os dados indisponíveis até que o usuário do computador pague uma quantia específica de dinheiro

**140. Qual tipo de mensagem ICMPv6 fornece informações de endereçamento de rede para hosts que usam SLAAC?**

* solicitação do roteador
* Anúncio de vizinhos
* Solicitação de vizinho
* propaganda do roteador

**141. Um cliente está usando o SLAAC para obter um endereço IPv6 para a interface. Depois que um endereço foi gerado e aplicado à interface, o que o cliente deve fazer antes de começar a usar esse endereço IPv6?**

* Ele deve esperar por uma mensagem de anúncio do roteador ICMPv6 dando permissão para usar esse endereço.
* Ele deve enviar uma mensagem de solicitação de roteador ICMPv6 para determinar qual gateway padrão ele deve usar.
* Deve enviar uma mensagem de solicitação de vizinho ICMPv6 para garantir que o endereço ainda não esteja em uso na rede.
* Ele deve enviar uma mensagem de solicitação de roteador ICMPv6 para solicitar o endereço do servidor DNS.

**142. Quais dois tipos de tráfego de rede não legível poderia ser eliminado dos dados coletados pelo NSM? (Escolha dois.)**

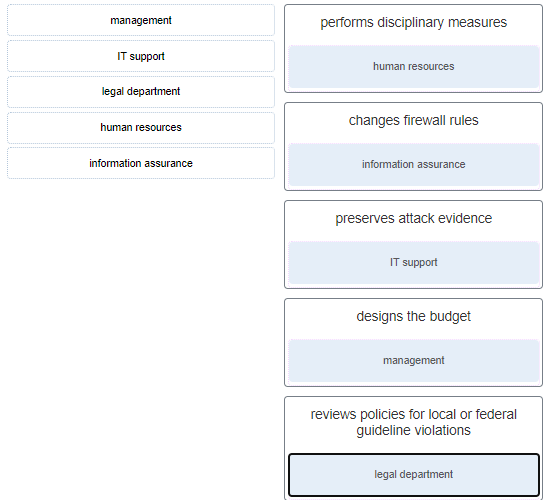
* Tráfego do STP
* Tráfego de IPsec
* routing atualiza o tráfego
* Tráfego de SSL
* tráfego de transmissão

**Para** reduzir a enorme quantidade de dados coletados para que os analistas de segurança cibernética possam se concentrar em ameaças críticas, alguns dados menos importantes ou inutilizáveis podem ser eliminados dos conjuntos de dados. Por exemplo, dados criptografados, como IPsec e tráfego SSL, podem ser eliminados porque são imutáveis em um prazo razoável.

**143. Qual componente central de código aberto do Elastic-stack é responsável por aceitar os dados em seu formato nativo e tornar os elementos dos dados consistentes em todas as fontes?**

* Logstash em
* Kibana (Ianbana
* Beats (taça)
* Elasticsearch (procura-se

**144. Combine o incidente de segurança com o papel.**

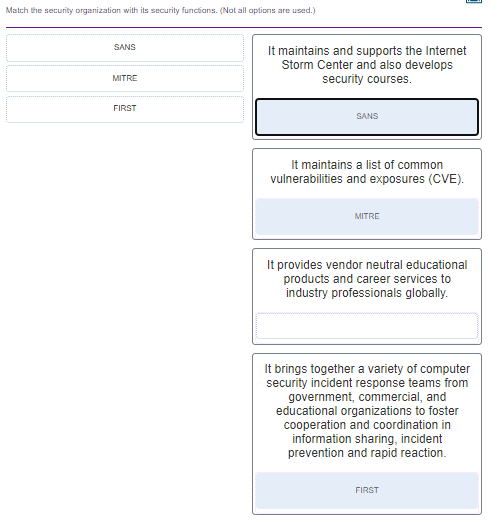


**145. No ciclo de vida do processo de resposta a incidentes do NIST, que tipo de vetor de ataque envolve o uso de força bruta contra dispositivos, redes ou serviços?**

* A mídia
* personificação de representação
* attrition (
* perda ou roubo

**Explicação:** Vetores de ataque comuns incluem mídia, atrito, personificação e perda ou roubo. Ataques de atrito são ataques que usam força bruta. Ataques de mídia são aqueles iniciados a partir de dispositivos de armazenamento. Os ataques de imitação ocorrem quando algo ou alguém é substituído para o propósito do ataque, e ataques de perda ou roubo são iniciados por equipamentos dentro da organização.

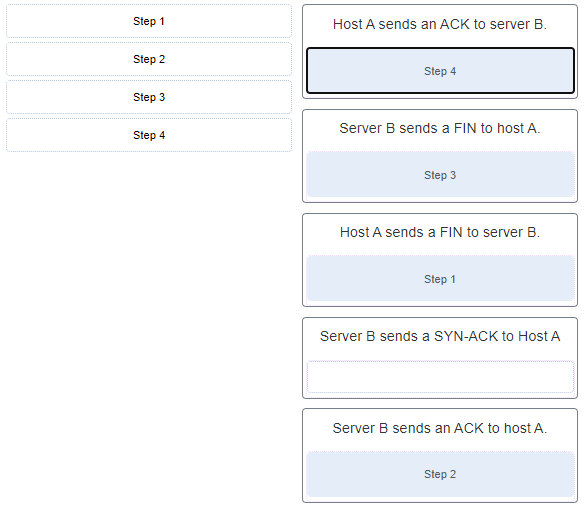
**146. Combine a organização de segurança com suas funções de segurança. (Nem todas as opções são usadas.)**



**147. O que é uma característica do CybOX?**

* É um conjunto de esquemas padronizados para especificar, capturar, caracterizar e comunicar eventos e propriedades de operações de rede.
* Permite a troca em tempo real de indicadores de ameaças cibernéticas entre os EUA. Governo Federal e o setor privado.
* É um conjunto de especificações para a troca de informações de ameaças cibernéticas entre organizações.
* É a especificação para um protocolo de camada de aplicação que permite a comunicação de CTI sobre HTTPS.

**148. Depois que o host A recebe uma página da Web do servidor B, o host A encerra a conexão com o servidor B. Combine cada etapa com a opção correta no processo normal de terminação para uma conexão TCP. (Nem todas as opções são usadas.)**



**149 (em inglês). Quais são as duas maneiras pelas quais o ICMP pode ser uma ameaça à segurança de uma empresa? (Escolha dois.)**

* Colecionando informações sobre uma rede
* corrompendo dados entre servidores de e-mail e destinatários de e-mail
* por infiltração de páginas web
* corrompendo pacotes de dados IP de rede
* fornecendo um canal para ataques DoS

**O** ICMP pode ser usado como um conduíte para ataques DoS. Ele pode ser usado para coletar informações sobre uma rede, como a identificação de hosts e estrutura de rede, e determinando os sistemas operacionais que estão sendo usados na rede.

**150. Quais campos de cabeçalho IPv4 não têm equivalente em um cabeçalho IPv6? (Escolha três.)**

* offset do fragmento
* Protocolo de
* Bandeira
* TTL em Inglês
* A identificação
* Versão da versão

**Ao** contrário **do** IPv4, os roteadores IPv6 não realizam a fragmentação. Portanto, todos os três campos que suportam a fragmentação no cabeçalho IPv4 são removidos e não têm equivalente no cabeçalho IPv6. Estes três campos são deslocamento de fragmento, bandeira e identificação. O IPv6 suporta a fragmentação de pacotes host através do uso de cabeçalhos de extensão, que não fazem parte do cabeçalho IPv6.

**151. Um administrador descobre que um usuário está acessando um site recém-criado que pode ser prejudicial para a segurança da empresa. Que medidas deve o administrador tomar primeiro em termos da política de segurança?**

* Peça ao usuário para parar imediatamente e informar o usuário que isso constitui motivo para demissão.
* Crie uma regra de firewall bloqueando o respectivo site.
* **Revise o AUP imediatamente e obtenha todos os usuários para assinar o AUP atualizado.**
* Suspender imediatamente os privilégios de rede do usuário.

Quais são as três funções disponibilizadas pelo serviço syslog? (Escolha três.)

* especificação dos destinos das mensagens registradas
* seleção do tipo de informações de registro que são capturadas
* coleta de informações de registro para monitorar e solucionar problemas

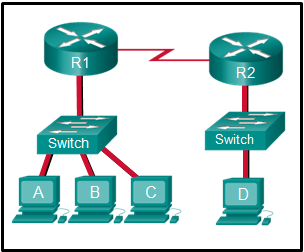
Quais as duas tarefas que podem ser executadas por um servidor DNS local? (Escolha duas.)

Mapear nome para endereço IP pra hosts internos

Encaminhar requisições de resolução de nome entre servidores

47. Quais são os dois possíveis problemas de rede que podem resultar da operação do ARP? (Escolha dois.)

* A configuração manual de associações ARP estáticas pode facilitar o envenenamento de ARP ou a falsificação de endereço MAC.
* Em grandes redes com baixa largura de banda, múltiplas transmissões ARP podem causar atrasos na comunicação de dados.
* Os invasores de rede podem manipular mapeamentos de endereços MAC e IP em mensagens ARP com a intenção de interceptar o tráfego de rede.
* Um grande número de transmissões de solicitação ARP pode causar o estouro da tabela de endereços MAC do host e impedir que o host se comunique na rede.
* Múltiplas respostas ARP resultam na tabela de endereços MAC do switch contendo entradas que correspondem aos endereços MAC dos hosts conectados à porta do switch relevante.

29

Consulte a figura. Os switches têm uma configuração padrão. O host A precisa se comunicar com o host D, mas o host A não tem o endereço MAC do gateway padrão. Quais dispositivos de rede receberão a solicitação ARP enviada pelo host A?

somente os hosts B, C e o roteador R1

Quando um usuário visita o site de uma loja online que usa HTTPS, o navegador do usuário consulta a CA para obter uma CRL. Qual é o objetivo desta consulta?

para verificar a validade do certificado digital

Um analista de segurança cibernética precisa coletar dados de alerta. Quais são as três ferramentas de detecção para executar essa tarefa na arquitetura Security Onion? (Escolha três.)

* CapME
* Wazuh
* Kibana
* Zeek
* Sguil
* Wireshark

O que é uma network tap?

O que é escalonamento de privilégios?

* Vulnerabilidades nos sistemas são exploradas para conceder níveis de privilégio mais altos do que alguém ou algum processo deveria ter.