Primeira Bateria de Questões Com Resolução Assistida

Segurança em redes de computadores

Prevenção e tratamento de incidentes

1. No tocante a protocolos, serviços, padrões e topologias de redes, julgue os itens subsequentes.

[101] A topologia lógica de interconexão de uma rede corporativa complexa precisa refletir a topologia física dessa rede, de modo que os requisitos de segurança lógica da rede sejam de implementação direta a partir dos aspectos da segurança física das instalações de TI da organização.

1. No tocante a protocolos, serviços, padrões e topologias de redes, julgue os itens subsequentes.

~~[101] A topologia lógica de interconexão de uma rede corporativa complexa precisa refletir a topologia física dessa rede, de modo que os requisitos de segurança lógica da rede sejam de implementação direta a partir dos aspectos da segurança física das instalações de TI da organização.~~

2. Com relação à segurança em redes de computadores, julgue os itens subsequentes.

[158] Uma das fases do processo de tratamento e resposta a incidentes de segurança em redes de computadores é a preparação, na qual são sanitizadas mídias para armazenamento e confeccionados kits de ferramentas em meio read-only.

[160] VPNs implementam redes seguras a fim de prover confidencialidade, integridade e autenticidade em canais públicos compartilhados.

2. Com relação à segurança em redes de computadores, julgue os itens subsequentes.

[158] Uma das fases do processo de tratamento e resposta a incidentes de segurança em redes de computadores é a preparação, na qual são sanitizadas mídias para armazenamento e confeccionados kits de ferramentas em meio read-only.

[160] VPNs implementam redes seguras a fim de prover confidencialidade, integridade e autenticidade em canais públicos compartilhados.

3. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[96] O uso de criptografia SSL (Secure Socket Layer) como item de segurança nas transmissões de dados via Internet dificulta o monitoramento realizado por sistemas de detecção de intrusos (IDS) de redes. Uma solução para esse problema é o uso de proxies reversos, que permite retirar o processo de criptografia do servidor web e, conseqüentemente, possibilita ao IDS o monitoramento do tráfego.

[97] A captura de quadros de redes wireless IEEE 802.11 geralmente não é alcançada com o uso do modo promíscuo da interface de rede, sendo necessário configurar a interface de rede para o modo de monitoramento (monitor mode). Além disso, pode haver restrições por parte do sistema operacional, como ocorre no Windows, o que impede a captura de quadros desse tipo.

[98] O WIPS (Wireless Intrusion Prevention System) é um dispositivo que monitora o espectro de ondas de rádio, buscando identificar a presença de pontos de acesso não autorizados. Ao detectar a presença de sinais de rádio não autorizados, o WIPS pode enviar alerta ao administrador ou ao firewall da rede para prevenir possíveis ataques.

3. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[96] O uso de criptografia SSL (Secure Socket Layer) como item de segurança nas transmissões de dados via Internet dificulta o monitoramento realizado por sistemas de detecção de intrusos (IDS) de redes. Uma solução para esse problema é o uso de proxies reversos, que permite retirar o processo de criptografia do servidor web e, conseqüentemente, possibilita ao IDS o monitoramento do tráfego.

[97] A captura de quadros de redes wireless IEEE 802.11 geralmente não é alcançada com o uso do modo promíscuo da interface de rede, sendo necessário configurar a interface de rede para o modo de monitoramento (monitor mode). Além disso, pode haver restrições por parte do sistema operacional, como ocorre no Windows, o que impede a captura de quadros desse tipo.

[98] O WIPS (Wireless Intrusion Prevention System) é um dispositivo que monitora o espectro de ondas de rádio, buscando identificar a presença de pontos de acesso não autorizados. Ao detectar a presença de sinais de rádio não autorizados, o WIPS pode enviar alerta ao administrador ou ao firewall da rede para prevenir possíveis ataques.

4. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[101] Traffic shaping é uma prática que tem sido adotada por empresas de telefonia e provedoras de acesso à Internet que, apesar de ser considerada abusiva por parte de órgãos de defesa do consumidor, geralmente é utilizada para otimizar o uso da largura de banda disponível, restringindo a banda para serviços que demandam a transferência de grande volume de dados, como P2P e FTP.

4. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[101] Traffic shaping é uma prática que tem sido adotada por empresas de telefonia e provedoras de acesso à Internet que, apesar de ser considerada abusiva por parte de órgãos de defesa do consumidor, geralmente é utilizada para otimizar o uso da largura de banda disponível, restringindo a banda para serviços que demandam a transferência de grande volume de dados, como P2P e FTP.

5. Com relação à segurança em redes de computadores, julgue os itens que se seguem.

[83] Os bots são programas maliciosos armazenados na área de boot do disco de uma estação de trabalho. Eles são capazes de se reproduzir, de modo que o invasor consegue orientar o bot a realizar ataques em um ambiente em rede.

[84] Para segurança dos programas e dos sistemas, é comum as organizações armazenarem informações denominadas accounting, que identificam o responsável pelo processamento, o nome do programa, o tipo de processamento, a área de execução, a periodicidade, a prioridade, o tempo estimado, entre outros.

5. Com relação à segurança em redes de computadores, julgue os itens que se seguem.

~~[83] Os bots são programas maliciosos armazenados na área de boot do disco de uma estação de trabalho. Eles são capazes de se reproduzir, de modo que o invasor consegue orientar o bot a realizar ataques em um ambiente em rede.~~

[84] Para segurança dos programas e dos sistemas, é comum as organizações armazenarem informações denominadas accounting, que identificam o responsável pelo processamento, o nome do programa, o tipo de processamento, a área de execução, a periodicidade, a prioridade, o tempo estimado, entre outros.

6. Considerando os conceitos de segurança em redes de comunicações, julgue os itens seguintes.

[106] Uma das vantagens da detecção de intrusão baseada em anomalias é a eficiência na detecção, comparativamente à detecção baseada em assinaturas, uma vez que não gera grande número de alarmes falsos.

[107] Com o filtro de pacotes de um roteador, um conjunto restrito de usuários internos pode receber, ao invés de endereços IP, o serviço Telnet, devendo esses usuários, se autenticarem antes de obter permissão para criar sessões Telnet com computadores externos.

6. Considerando os conceitos de segurança em redes de comunicações, julgue os itens seguintes.

~~[106] Uma das vantagens da detecção de intrusão baseada em anomalias é a eficiência na detecção, comparativamente à detecção baseada em assinaturas, uma vez que não gera grande número de alarmes falsos.~~

~~[107] Com o filtro de pacotes de um roteador, um conjunto restrito de usuários internos pode receber, ao invés de endereços IP, o serviço Telnet, devendo esses usuários, se autenticarem antes de obter permissão para criar sessões Telnet com computadores externos.~~

7. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[109] São dispositivos constitucionais relacionados com a segurança dos sistemas de informação em organizações públicas brasileiras: o direito à privacidade, que define a aplicação do sigilo das informações relacionadas à intimidade ou vida privada de alguém; o direito à informação e ao acesso aos registros públicos; o dever do estado de proteger documentos e obras; e o dever do estado de promover a gestão documental.

[111] Envenenamento ARP (ARP poisoning), SYN flooding attack e roubo de sessão TCP (TCP session hijacking) são tipos de ataque que estações pertencentes a uma rede IPv4 podem sofrer. Esses três tipos podem ser usados para produzir negação de serviço, com a diferença de que, para realizar o primeiro, o host atacante deve estar fisicamente localizado no mesmo segmento do host atacado, enquanto os dois últimos podem ser efetuados por meio da Internet.

7. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[109] São dispositivos constitucionais relacionados com a segurança dos sistemas de informação em organizações públicas brasileiras: o direito à privacidade, que define a aplicação do sigilo das informações relacionadas à intimidade ou vida privada de alguém; o direito à informação e ao acesso aos registros públicos; o dever do estado de proteger documentos e obras; e o dever do estado de promover a gestão documental.

[111] Envenenamento ARP (ARP poisoning), SYN flooding attack e roubo de sessão TCP (TCP session hijacking) são tipos de ataque que estações pertencentes a uma rede IPv4 podem sofrer. Esses três tipos podem ser usados para produzir negação de serviço, com a diferença de que, para realizar o primeiro, o host atacante deve estar fisicamente localizado no mesmo segmento do host atacado, enquanto os dois últimos podem ser efetuados por meio da Internet.

8. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[112] Os processos de definição, implantação e gestão de políticas de segurança da informação devem ser aprovados pelo pessoal de nível operacional e devem se subordinar às normas e procedimentos de segurança vigentes na organização.

[113] Se a segurança demandada por uma comunicação referir-se apenas à integridade das mensagens, é adequado o uso de hashes criptográficos, o que, além do mais, não apresenta o inconveniente da complexidade técnico-operacional que caracteriza o gerenciamento de chaves.

[114] Protetor contra surtos elétricos, sanitização de entrada de dados, proteção de memória, firewall de aplicação, controle de acesso com base em papéis, firewall statefull, verificação de antecedentes e sensores de fumaça são, respectivamente, meios de proteção contra ataques relativos a hardware, software, sistemas operacionais, aplicações, bancos de dados, redes, pessoas e ambiente físico.

8. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

~~[112] Os processos de definição, implantação e gestão de políticas de segurança da informação devem ser aprovados pelo pessoal de nível operacional e devem se subordinar às normas e procedimentos de segurança vigentes na organização.~~

[113] Se a segurança demandada por uma comunicação referir-se apenas à integridade das mensagens, é adequado o uso de hashes criptográficos, o que, além do mais, não apresenta o inconveniente da complexidade técnico-operacional que caracteriza o gerenciamento de chaves.

[114] Protetor contra surtos elétricos, sanitização de entrada de dados, proteção de memória, firewall de aplicação, controle de acesso com base em papéis, firewall statefull, verificação de antecedentes e sensores de fumaça são, respectivamente, meios de proteção contra ataques relativos a hardware, software, sistemas operacionais, aplicações, bancos de dados, redes, pessoas e ambiente físico.

9. Acerca de prevenção e tratamento a ataques a redes de computadores, julgue os itens subsecutivos.

[118] O processo de tratamento e de resposta a incidentes de segurança da informação é independente da política de continuidade de negócio.

[119] Ataques de negação de serviço volumétricos são prevenidos de maneira eficaz por filtros orientados a conteúdo.

[120] Ataques de buffer overflow não são evitados com a inspeção de cabeçalhos.

9. Acerca de prevenção e tratamento a ataques a redes de computadores, julgue os itens subsecutivos.

~~[118] O processo de tratamento e de resposta a incidentes de segurança da informação é independente da política de continuidade de negócio.~~

~~[119] Ataques de negação de serviço volumétricos são prevenidos de maneira eficaz por filtros orientados a conteúdo.~~

[120] Ataques de buffer overflow não são evitados com a inspeção de cabeçalhos.

10. A respeito de ataques a redes de computadores, prevenção e tratamento de incidentes, julgue os itens subsecutivos

[108] Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidente de segurança da informação.

[110] Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.

10. A respeito de ataques a redes de computadores, prevenção e tratamento de incidentes, julgue os itens subsecutivos

[108] Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidente de segurança da informação.

[110] Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.

GABARITO

1. E
2. C, C,
3. C, C, C
4. C
5. E, C
6. E, E
7. C, C
8. E, C, C
9. E, E, C
10. C, C

Segunda Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:
FIREWALL, IDS, IPS

1. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

[76] Um dispositivo do tipo IDS (intrusion detection system) atua com proatividade, prevendo ataques e antecipando-se a explorações de vulnerabilidades, a partir de assinaturas frequentemente atualizadas

1. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

~~[76] Um dispositivo do tipo IDS (intrusion detection system) atua com proatividade, prevendo ataques e antecipando-se a explorações de vulnerabilidades, a partir de assinaturas frequentemente atualizadas~~

2. Acerca das características e dos processos de mitigação de um ataque de negação de serviço distribuído, julgue os itens subsequentes.

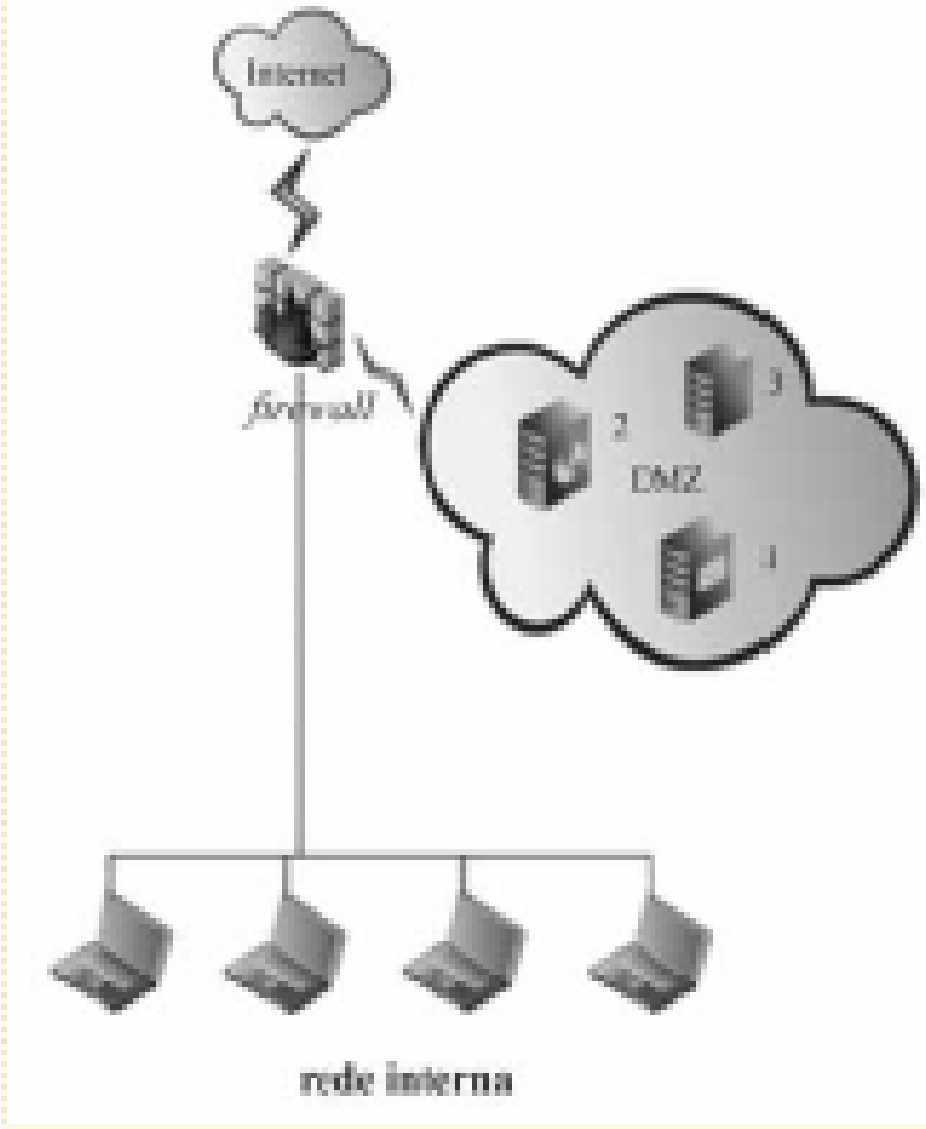
[84] Ataques de negação de serviço distribuído com base em HTTP devem ser mitigados em firewall de camada de aplicação. Nesse caso, se for utilizado o protocolo HTTPS, a mitigação não será possível porque os dados trafegados são cifrados.

[85] Um DDoS com base em ICMP será efetivo somente se for realizado no protocolo IPv4, uma vez que, em IPv6, o uso de ICMP é restrito para interface de loopback.

2. Acerca das características e dos processos de mitigação de um ataque de negação de serviço distribuído, julgue os itens subsequentes.

~~[84] Ataques de negação de serviço distribuído com base em HTTP devem ser mitigados em firewall de camada de aplicação. Nesse caso, se for utilizado o protocolo HTTPS, a mitigação não será possível porque os dados trafegados são cifrados.~~

~~[85] Um DDoS com base em ICMP será efetivo somente se for realizado no protocolo IPv4, uma vez que, em IPv6, o uso de ICMP é restrito para interface de loopback.~~



3. Considerado a figura acima, que representa a topologia simplificada da rede de dados de uma organização, julgue os itens a seguir.

[78] Se um IPS (intrusion prevention system) for instalado logo acima do firewall, haverá um ganho de segurança, visto que esse sistema poderá ser baseado em assinaturas de ataques e terá capacidade para bloquear possíveis ameaças.

[79] O firewall representado é um sistema que isola áreas distintas da rede de dados e que delimita os domínios de confiança.

[80] Qualquer usuário conectado à Internet pode acessar o servidor 2 da DMZ na porta 80, pois não foram implementadas políticas específicas para essa rede, que consiste em uma zona desmilitarizada.

[81] Como o servidor 1 está na DMZ, que, por definição, não tem controle de acesso, não será possível ao usuário da rede interna acessar e encaminhar uma mensagem eletrônica assinada com base em um algoritmo de criptografia de chaves públicas.

3. Considerado a figura acima, que representa a topologia simplificada da rede de dados de uma organização, julgue os itens a seguir.

[78] Se um IPS (intrusion prevention system) for instalado logo acima do firewall, haverá um ganho de segurança, visto que esse sistema poderá ser baseado em assinaturas de ataques e terá capacidade para bloquear possíveis ameaças.

[79] O firewall representado é um sistema que isola áreas distintas da rede de dados e que delimita os domínios de confiança.

~~[80] Qualquer usuário conectado à Internet pode acessar o servidor 2 da DMZ na porta 80, pois não foram implementadas políticas específicas para essa rede, que consiste em uma zona desmilitarizada.~~

~~[81] Como o servidor 1 está na DMZ, que, por definição, não tem controle de acesso, não será possível ao usuário da rede interna acessar e encaminhar uma mensagem eletrônica assinada com base em um algoritmo de criptografia de chaves públicas.~~

4. Acerca de firewall, assinale a opção correta.

A. Apesar de serem dependentes de aplicativos e de ignorar os endereços IPs, os firewalls de filtragem de pacotes são mais seguros em comparação com os do tipo proxy.

B. Além de controlar e conectar o tráfego entre redes, um firewall pode criar redes privadas virtuais (VPN), suportar varreduras de vírus no correio eletrônico e filtrar aplicativos para bloquear acesso não autorizado aos aplicativos remotos.

C. Em comparação com um firewall de filtragem de pacotes, os aplicativos de firewall e de proxy são mais rápidos, mais baratos e suportam o protocolo UDP.

D. Os firewalls do tipo filtragem de pacotes são voltados para tratamento de códigos maliciosos, como, por exemplo, cavalos de tróia.

E. Os firewalls do tipo inspeção de pacotes com informação de estado funcionam nas camadas de 3 a 7 para proteção e tratamento de vírus de rede.

4. Acerca de firewall, assinale a opção correta.

A. Apesar de serem dependentes de aplicativos e de ignorar os endereços IPs, os firewalls de filtragem de pacotes são mais seguros em comparação com os do tipo proxy.

B. Além de controlar e conectar o tráfego entre redes, um firewall pode criar redes privadas virtuais (VPN), suportar varreduras de vírus no correio eletrônico e filtrar aplicativos para bloquear acesso não autorizado aos aplicativos remotos.

C. Em comparação com um firewall de filtragem de pacotes, os aplicativos de firewall e de proxy são mais rápidos, mais baratos e suportam o protocolo UDP.

D. Os firewalls do tipo filtragem de pacotes são voltados para tratamento de códigos maliciosos, como, por exemplo, cavalos de tróia.

E. Os firewalls do tipo inspeção de pacotes com informação de estado funcionam nas camadas de 3 a 7 para proteção e tratamento de vírus de rede.

5. Acerca de proteção de estações de trabalho, julgue os próximos itens.

[89] Se o firewall pessoal estiver habilitado na estação de trabalho, ele será capaz de bloquear o tráfego de rede com destino final à estação de trabalho ao ser direcionado a uma porta específica.

[90] Entre as ações que integram o processo de hardening incluem-se desinstalar softwares desnecessários para o cotidiano do usuário na estação de trabalho e instalar antispyware

5. Acerca de proteção de estações de trabalho, julgue os próximos itens.

[89] Se o firewall pessoal estiver habilitado na estação de trabalho, ele será capaz de bloquear o tráfego de rede com destino final à estação de trabalho ao ser direcionado a uma porta específica.

[90] Entre as ações que integram o processo de hardening incluem-se desinstalar softwares desnecessários para o cotidiano do usuário na estação de trabalho e instalar antispyware

6. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.

6. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

~~[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.~~

7. Assinale a opção em que são apresentadas as características genéricas de um firewall.

A. Validar select executado por uma aplicação web em um banco de dados DB2.

B. Permitir acesso a um sistema e a análise de ataques por meio de estatísticas de anomalia relacionadas aos comportamentos dos usuários.

C. Analisar switches defeituosos na rede de computadores.

D. Capacidade para concentrar e filtrar os acessos dial-in à rede e suportar a funcionalidade de proxy para serviços FTP.

E. Criptografar os dados de uma aplicação de intranet na rede interna

7. Assinale a opção em que são apresentadas as características genéricas de um firewall.

A. Validar select executado por uma aplicação web em um banco de dados DB2.

B. Permitir acesso a um sistema e a análise de ataques por meio de estatísticas de anomalia relacionadas aos comportamentos dos usuários.

C. Analisar switches defeituosos na rede de computadores.

D. Capacidade para concentrar e filtrar os acessos dial-in à rede e suportar a funcionalidade de proxy para serviços FTP.

E. Criptografar os dados de uma aplicação de intranet na rede interna

GABARITO

1. E
2. E, E
3. C, C, E, E
4. B
5. C, C
6. E
7. D

Terceira Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:
FIREWALL, IDS, IPS

1. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

[118] Firewalls conhecidos como filtro de pacotes, que atuam na camada de transporte do TCP/IP, são capazes de filtrar o tráfego de rede identificando o uso de softwares como Skype e Gtalk, sem a necessidade de filtrar o endereço IP da conexão.

[119] Ferramentas utilizadas para detecção de intrusão em redes adotam o recurso de captura de pacotes para análise e detecção de assinaturas de ataques conhecidos.

1. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

~~[118] Firewalls conhecidos como filtro de pacotes, que atuam na camada de transporte do TCP/IP, são capazes de filtrar o tráfego de rede identificando o uso de softwares como Skype e Gtalk, sem a necessidade de filtrar o endereço IP da conexão.~~

[119] Ferramentas utilizadas para detecção de intrusão em redes adotam o recurso de captura de pacotes para análise e detecção de assinaturas de ataques conhecidos.

2. A respeito de firewall, julgue os itens subsecutivos.

[67] Um firewall que trabalha especificamente na camada de aplicação tem a capacidade de estabelecer regras para registrar e descartar pacotes que sejam destinados a um endereço IP e a uma porta específica.

[68] Considere que, em um servidor com serviço de firewall habilitado e em funcionamento, o administrador de rede tenha verificado que existe muito tráfego de flags SYN do protocolo TCP, sem que ocorra o retorno da flag ACK do host a que foi destinada a flag SYN. Nessa situação, é possível que regras de firewall estejam descartando os pedidos de abertura de conexão.

2. A respeito de firewall, julgue os itens subsecutivos.

~~[67] Um firewall que trabalha especificamente na camada de aplicação tem a capacidade de estabelecer regras para registrar e descartar pacotes que sejam destinados a um endereço IP e a uma porta específica.~~

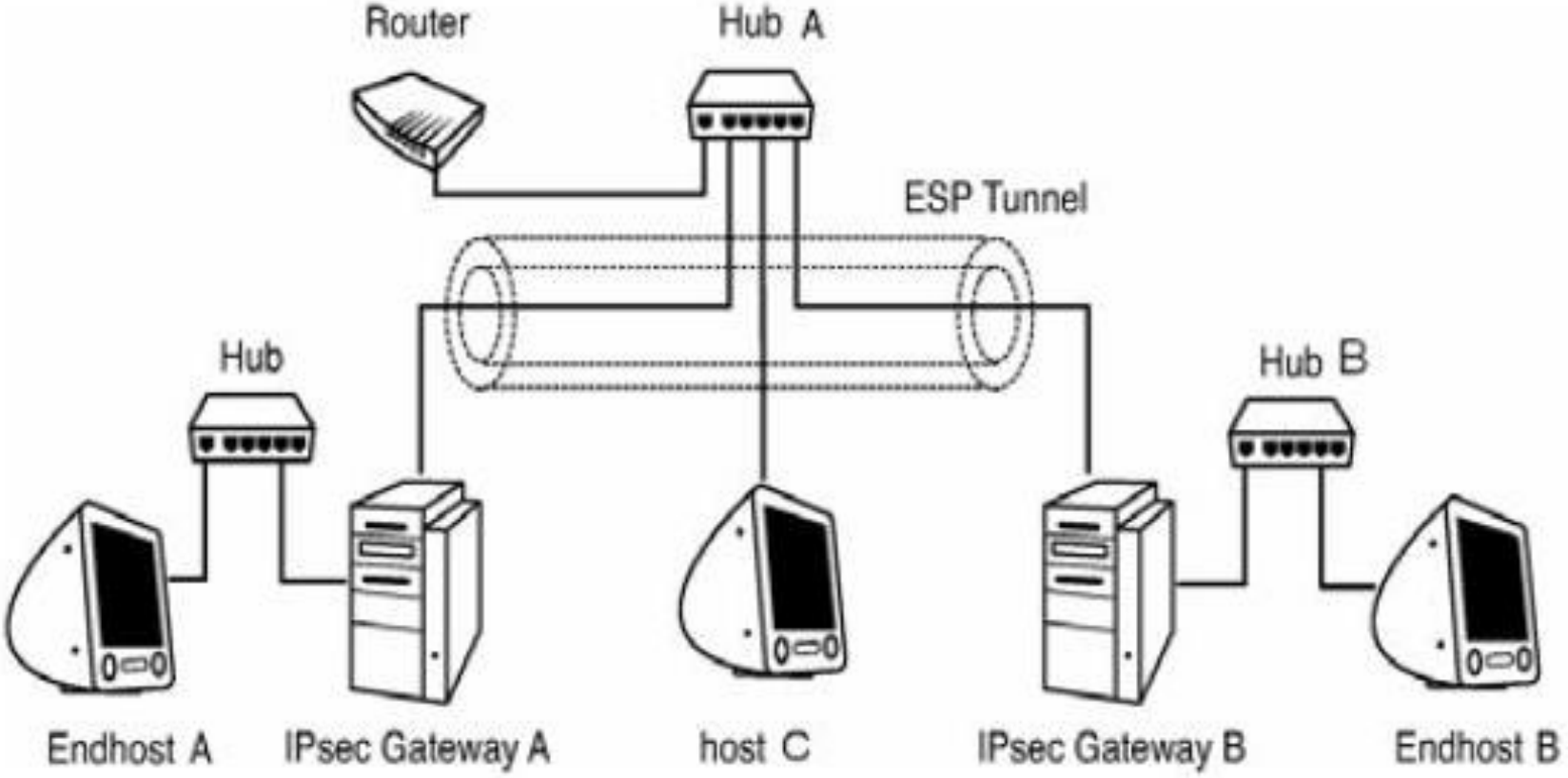
[68] Considere que, em um servidor com serviço de firewall habilitado e em funcionamento, o administrador de rede tenha verificado que existe muito tráfego de flags SYN do protocolo TCP, sem que ocorra o retorno da flag ACK do host a que foi destinada a flag SYN. Nessa situação, é possível que regras de firewall estejam descartando os pedidos de abertura de conexão.

3. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[59] Considere que, em uma rede dotada de firewall, um computador infectado por vírus esteja enviando grande quantidade de emails via servidor de email dessa rede. Nessa situação, até que o vírus seja removido do computador infectado, o firewall tem a capacidade de bloquear o acesso entre o computador e o servidor de email sem tornar indisponível, ao servidor de email, o uso dos outros computadores da mesma rede.

3. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[59] Considere que, em uma rede dotada de firewall, um computador infectado por vírus esteja enviando grande quantidade de emails via servidor de email dessa rede. Nessa situação, até que o vírus seja removido do computador infectado, o firewall tem a capacidade de bloquear o acesso entre o computador e o servidor de email sem tornar indisponível, ao servidor de email, o uso dos outros computadores da mesma rede.



4. O modelo da figura acima apresenta elementos individualmente nomeados e presentes em uma rede hipotética, acerca dos quais é possível inferir características de protocolos de segurança.

Julgue os itens seguintes, acerca das informações apresentadas e de dispositivos de segurança de redes de computadores.

[171] Se os Endhosts A e B trocarem vários pacotes por meio de seus respectivos gateways, então não haverá modo fácil de o host C identificar quais dos pacotes IP trafegados entre os gateways A e B são relativos à comunicação entre os Endhosts A e B.

[172] Considerando a necessidade de instalar um IDS para proteger a rede A, algumas opções podem ser adotadas, entre elas a de usar um sistema passivo ou ativo, bem como a de usar um sistema baseado em host ou em rede. Se a solução for adotar um sistema passivo e com base em host, então o host C poderá ser uma máquina adequada para essa necessidade. Se a solução for adotar um sistema reativo e embasado na rede, então podem-se usar os gateways A ou B. Se a solução for adotar um sistema reativo e baseado em host, então se poderá usar o host C.

4. O modelo da figura acima apresenta elementos individualmente nomeados e presentes em uma rede hipotética, acerca dos quais é possível inferir características de protocolos de segurança.

Julgue os itens seguintes, acerca das informações apresentadas e de dispositivos de segurança de redes de computadores.

[171] Se os Endhosts A e B trocarem vários pacotes por meio de seus respectivos gateways, então não haverá modo fácil de o host C identificar quais dos pacotes IP trafegados entre os gateways A e B são relativos à comunicação entre os Endhosts A e B.

~~[172] Considerando a necessidade de instalar um IDS para proteger a rede A, algumas opções podem ser adotadas, entre elas a de usar um sistema passivo ou ativo, bem como a de usar um sistema baseado em host ou em rede. Se a solução for adotar um sistema passivo e com base em host, então o host C poderá ser uma máquina adequada para essa necessidade. Se a solução for adotar um sistema reativo e embasado na rede, então podem-se usar os gateways A ou B. Se a solução for adotar um sistema reativo e baseado em host, então se poderá usar o host C.~~

5. Com relação a segurança de hosts e redes, julgue os itens seguintes

[168] Uma técnica comumente usada na segurança de redes é o estabelecimento de um perímetro de segurança cuja finalidade é controlar o tráfego ingresso na rede e o egresso da rede.

[169] Roteadores de borda, firewalls, IDSs, IPSs e VPNs são alguns dos principais elementos do perímetro de segurança da rede.

[172] Em geral, os firewalls inspecionam todo o pacote, enquanto os IDSs inspecionam apenas os cabeçalhos.

5. Com relação a segurança de hosts e redes, julgue os itens seguintes

[168] Uma técnica comumente usada na segurança de redes é o estabelecimento de um perímetro de segurança cuja finalidade é controlar o tráfego ingresso na rede e o egresso da rede.

[169] Roteadores de borda, firewalls, IDSs, IPSs e VPNs são alguns dos principais elementos do perímetro de segurança da rede.

~~[172] Em geral, os firewalls inspecionam todo o pacote, enquanto os IDSs inspecionam apenas os cabeçalhos~~.

GABARITO

1. E, C
2. E, C
3. C
4. C, E
5. C, C, E

Quarta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:
FIREWALL, IDS, IPS

1. Com relação a sistemas de proteção IDS, IPS e VLANs, assinale a opção correta.

A. O IDS (intrusion detection system) refere-se a meios técnicos de descobrir acessos não autorizados a uma rede, que podem indicar a ação de um cracker ou de funcionários mal-intencionados.

B. IPS (intrusion prevention systems), também denominado IDP (intrusion detection and prevention), são dispositivos de monitoramento de rede e(ou) atividades maliciosas de sistema empregados. Entre as suas funções estão a identificação das atividades maliciosas e a geração de log de informações acerca dessa atividade.

C. Os sistemas IPS são colocados em linha, contudo são incapazes de prevenir ativamente ou bloquear as intrusões detectadas.

D. O IPS envia alarme, prende os pacotes maliciosos, redefine a conexão e(ou) bloqueia o tráfego a partir do endereço IP incorreto.

E. São dois os métodos de estabelecer uma VLAN: o de marcação de quadro (frame-tagging), que não modifica a informação contida no quadro da camada 2, e o de filtragem de quadro (frame-filtering).

1. Com relação a sistemas de proteção IDS, IPS e VLANs, assinale a opção correta.

A. O IDS (intrusion detection system) refere-se a meios técnicos de descobrir acessos não autorizados a uma rede, que podem indicar a ação de um cracker ou de funcionários mal-intencionados.

B. IPS (intrusion prevention systems), também denominado IDP (intrusion detection and prevention), são dispositivos de monitoramento de rede e(ou) atividades maliciosas de sistema empregados. Entre as suas funções estão a identificação das atividades maliciosas e a geração de log de informações acerca dessa atividade.

C. Os sistemas IPS são colocados em linha, contudo são incapazes de prevenir ativamente ou bloquear as intrusões detectadas.

D. O IPS envia alarme, prende os pacotes maliciosos, redefine a conexão e(ou) bloqueia o tráfego a partir do endereço IP incorreto.

E. São dois os métodos de estabelecer uma VLAN: o de marcação de quadro (frame-tagging), que não modifica a informação contida no quadro da camada 2, e o de filtragem de quadro (frame-filtering).

2. Acerca de segurança na Internet e dispositivos de segurança de redes de computadores, julgue os itens que se seguem.

[64] Firewalls podem ser usados para estabelecer a chamada zona deslimitarizada (DMZ), que é um segmento de rede localizado entre a rede protegida e a rede desprotegida.

[65] Um IDS (intrusion detection system) permite monitorar o tráfego de rede em busca de atividades consideradas suspeitas, sem, entretanto, agir diretamente sobre as suspeitas identificadas.

2. Acerca de segurança na Internet e dispositivos de segurança de redes de computadores, julgue os itens que se seguem.

[64] Firewalls podem ser usados para estabelecer a chamada zona deslimitarizada (DMZ), que é um segmento de rede localizado entre a rede protegida e a rede desprotegida.

~~[65] Um IDS (intrusion detection system) permite monitorar o tráfego de rede em busca de atividades consideradas suspeitas, sem, entretanto, agir diretamente sobre as suspeitas identificadas.~~

3. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.

3. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

~~[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.~~

4. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[103] Considere que os auditores identifiquem, entre a rede de uma organização e a Internet, um sistema em funcionamento que realiza a filtragem e correção automática do fluxo de pacotes e datagramas estabelecidos entre os hosts da organização e aqueles da Internet. Considere também que o referido sistema realiza inspeção e eventuais ajustes nos pedidos e respostas http que trafegam em ambos sentidos. Nesse caso, diante das informações mencionadas, é correto afirmar que tal sistema pode ser classificado como de prevenção de intrusão em rede NIPS (network intrusion prevention system) e não apenas como de detecção de intrusão IDS (intrusion detection system).

4. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[103] Considere que os auditores identifiquem, entre a rede de uma organização e a Internet, um sistema em funcionamento que realiza a filtragem e correção automática do fluxo de pacotes e datagramas estabelecidos entre os hosts da organização e aqueles da Internet. Considere também que o referido sistema realiza inspeção e eventuais ajustes nos pedidos e respostas http que trafegam em ambos sentidos. Nesse caso, diante das informações mencionadas, é correto afirmar que tal sistema pode ser classificado como de prevenção de intrusão em rede NIPS (network intrusion prevention system) e não apenas como de detecção de intrusão IDS (intrusion detection system).

5. Os sistemas IDS (Intrusion Detection System) têm-se tornado componentes cada vez mais importantes em redes de computadores de várias corporações. Com referência aos IDS e suas características, julgue os seguintes itens.

- Apesar de ser uma ferramenta de segurança altamente específica, um IDS não deve ser utilizado em conjunto com um firewall, porque a quantidade de ataques que um IDS detecta é relativamente pequena em redes consideradas grandes.

- Um IDS pode detectar, de acordo com configurações específicas, se uma rede ou se um nodo em uma rede está sofrendo um ataque de DDoS (Distributed Denial of Service).

- Para a detecção de intrusão, um IDS usa técnicas de detecção de anomalia, detecção de uso impróprio (misuse detection) ou detecção de assinatura, entre outras técnicas.

- A técnica de detecção de anomalia consiste em o IDS reconhecer características consideradas como um padrão normal de funcionamento da rede. Qualquer variação brusca nesse padrão de comportamento é considerada como uma tentativa de intrusão na rede.

5. Os sistemas IDS (Intrusion Detection System) têm-se tornado componentes cada vez mais importantes em redes de computadores de várias corporações. Com referência aos IDS e suas características, julgue os seguintes itens.

- ~~Apesar de ser uma ferramenta de segurança altamente específica, um IDS não deve ser utilizado em conjunto com um firewall, porque a quantidade de ataques que um IDS detecta é relativamente pequena em redes consideradas grandes.~~

- Um IDS pode detectar, de acordo com configurações específicas, se uma rede ou se um nodo em uma rede está sofrendo um ataque de DDoS (Distributed Denial of Service).

- Para a detecção de intrusão, um IDS usa técnicas de detecção de anomalia, detecção de uso impróprio (misuse detection) ou detecção de assinatura, entre outras técnicas.

- A técnica de detecção de anomalia consiste em o IDS reconhecer características consideradas como um padrão normal de funcionamento da rede. Qualquer variação brusca nesse padrão de comportamento é considerada como uma tentativa de intrusão na rede.

6. Com relação à segurança em redes de computadores, julgue os itens subsequentes

[159] Firewalls, IDS e IPS são dispositivos que têm finalidades idênticas, porém tipicamente operam de formas distintas: o primeiro inspeciona integralmente os datagramas e reage bloqueando o tráfego indesejado; o segundo também inspeciona integralmente os datagramas, mas não bloqueia o tráfego indesejado, apenas emite alertas; e o terceiro inspeciona apenas os cabeçalhos dos datagramas e, como o primeiro, reage bloqueando o tráfego indesejado.

6. Com relação à segurança em redes de computadores, julgue os itens subsequentes

~~[159] Firewalls, IDS e IPS são dispositivos que têm finalidades idênticas, porém tipicamente operam de formas distintas: o primeiro inspeciona integralmente os datagramas e reage bloqueando o tráfego indesejado; o segundo também inspeciona integralmente os datagramas, mas não bloqueia o tráfego indesejado, apenas emite alertas; e o terceiro inspeciona apenas os cabeçalhos dos datagramas e, como o primeiro, reage bloqueando o tráfego indesejado.~~

7. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir

[101] A neutralização de backdoors é mais eficaz por meio de dispositivos de IPS e IDS que por meio de firewalls e sniffers.

7. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir

~~[101] A neutralização de backdoors é mais eficaz por meio de dispositivos de IPS e IDS que por meio de firewalls e sniffers.~~

8. Acerca dos dispositivos de segurança de redes de computadores, julgue os itens subsequentes.

[96] Um proxy, ao agir no lugar do cliente ou do usuário para prover acesso a um serviço de rede, protege tanto o cliente quanto o servidor de uma conexão direta.

[97] IDS e IPS são sistemas que protegem a rede de intrusões, diferindo no tratamento dado quando uma intrusão é detectada. Especificamente, o IPS limita-se a gerar alertas e ativar alarmes, e o IDS executa contramedidas, como interromper o fluxo de dados referente à intrusão detectada.

[98] A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.

[99] A inspeção de estados visa determinar se um pacote pode entrar ou sair de uma rede, tendo por base a verificação de informações localizadas no cabeçalho do pacote.

[100] Tanto na filtragem quanto na inspeção que se baseiam em estado, a informação de estado é mantida em uma tabela até que a conexão se encerre (como no tráfego TCP) ou ao atingir um limite de tempo (como no caso de tráfego TCP, UDP e ICMP).

8. Acerca dos dispositivos de segurança de redes de computadores, julgue os itens subsequentes.

[96] Um proxy, ao agir no lugar do cliente ou do usuário para prover acesso a um serviço de rede, protege tanto o cliente quanto o servidor de uma conexão direta.

~~[97] IDS e IPS são sistemas que protegem a rede de intrusões, diferindo no tratamento dado quando uma intrusão é detectada. Especificamente, o IPS limita-se a gerar alertas e ativar alarmes, e o IDS executa contramedidas, como interromper o fluxo de dados referente à intrusão detectada.~~

~~[98] A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.~~

~~[99] A inspeção de estados visa determinar se um pacote pode entrar ou sair de uma rede, tendo por base a verificação de informações localizadas no cabeçalho do pacote.~~

[100] Tanto na filtragem quanto na inspeção que se baseiam em estado, a informação de estado é mantida em uma tabela até que a conexão se encerre (como no tráfego TCP) ou ao atingir um limite de tempo (como no caso de tráfego TCP, UDP e ICMP).

9. Com relação a dispositivos de segurança de redes, julgue os próximos itens.

[110] Nos firewalls que utilizam inspeção de estado, esta é realizada no estado das conexões TCP.

[111] Os firewalls que usam filtragem de pacote tomam decisões de encaminhamento a partir de informações presentes nos cabeçalhos dos pacotes.

[112] Os IDS e IPS embasados em detecção por assinatura podem apresentar ocorrência de falsos-positivos, sendo mais severos os efeitos nos IPS que nos IDS.

9. Com relação a dispositivos de segurança de redes, julgue os próximos itens.

~~[110] Nos firewalls que utilizam inspeção de estado, esta é realizada no estado das conexões TCP.~~

[111] Os firewalls que usam filtragem de pacote tomam decisões de encaminhamento a partir de informações presentes nos cabeçalhos dos pacotes.

[112] Os IDS e IPS embasados em detecção por assinatura podem apresentar ocorrência de falsos-positivos, sendo mais severos os efeitos nos IPS que nos IDS.

10. Um firewall tem três interfaces, conectadas da seguinte forma: uma à rede externa; outra à rede interna; e a terceira a uma DMZ. Nessa situação, considerando que o firewall registre todas as suas ações referentes ao exame do tráfego, julgue os itens seguintes

[99] Nessa situação, as regras do firewall devem: permitir acesso da rede externa apenas aos servidores presentes na DMZ; negar acesso do tráfego da rede externa que tenha como origem endereços da rede interna; e negar acesso do tráfego da rede interna que tenha como origem endereços distintos dos utilizados na rede interna.

[100] Para a proteção do firewall em questão, é correto posicionar um IDS ou IPS, preferencialmente o último, entre a rede externa e o firewall.

[101] A presença de vários registros idênticos referentes a um mesmo fluxo de tráfego é consistente com um firewall que tem por base a inspeção de pacotes.

10. Um firewall tem três interfaces, conectadas da seguinte forma: uma à rede externa; outra à rede interna; e a terceira a uma DMZ. Nessa situação, considerando que o firewall registre todas as suas ações referentes ao exame do tráfego, julgue os itens seguintes

[99] Nessa situação, as regras do firewall devem: permitir acesso da rede externa apenas aos servidores presentes na DMZ; negar acesso do tráfego da rede externa que tenha como origem endereços da rede interna; e negar acesso do tráfego da rede interna que tenha como origem endereços distintos dos utilizados na rede interna.

~~[100] Para a proteção do firewall em questão, é correto posicionar um IDS ou IPS, preferencialmente o último, entre a rede externa e o firewall.~~

[101] A presença de vários registros idênticos referentes a um mesmo fluxo de tráfego é consistente com um firewall que tem por base a inspeção de pacotes.

GABARITO

1. A
2. C, E
3. E
4. C
5. E, C, C, C
6. E
7. E
8. C, E, E, E, C
9. E, C, C
10. C, E, C

Quinta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **Proxies**

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

~~[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.~~

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.

[89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

~~[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.~~

[89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.

4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.

4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.

5. Julgue os itens a seguir, a respeito de segurança da informação.

[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.

5. Julgue os itens a seguir, a respeito de segurança da informação.

~~[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.~~

6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

[70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

[73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

[70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

[73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

[82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

[83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

[82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

[83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

GABARITO

1. E
2. E, C
3. C
4. C
5. E
6. C, C
7. C, C

Sexta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: Proxies

1. De acordo com a ABNT NBR ISO/IEC 27002, devem ser implementados controles contra códigos maliciosos. Um mecanismo de controle contra esses códigos consiste no serviço de

A. páginas web.

B. compartilhamento de arquivos.

C. roteamento de computadores.

D. resolução de nomes.

E. proxy integrado com antivírus.

1. De acordo com a ABNT NBR ISO/IEC 27002, devem ser implementados controles contra códigos maliciosos. Um mecanismo de controle contra esses códigos consiste no serviço de

~~A. páginas web.~~

~~B. compartilhamento de arquivos.~~

~~C. roteamento de computadores.~~

~~D. resolução de nomes.~~

E. proxy integrado com antivírus.

2. No que concerne a firewall, julgue os itens a seguir.

[101] Os gateways de técnica de inspeção de estado comparam o padrão de bits de cada pacote de dados com um padrão conhecido e confiável, em vez de examinar os dados contidos no pacote.

[103] Em uma rede de computadores que utiliza o firewall do tipo roteador de barreira, o endereço IP dos pontos da rede interna é substituído pelo endereço do servidor de segurança da rede.

[104] Quando a rede de comunicação dispõe de firewall do tipo gateway servidor de proxy, é necessário o uso programas de administração para a filtragem dos pacotes com base no endereço IP.

2. No que concerne a firewall, julgue os itens a seguir.

[101] Os gateways de técnica de inspeção de estado comparam o padrão de bits de cada pacote de dados com um padrão conhecido e confiável, em vez de examinar os dados contidos no pacote.

~~[103] Em uma rede de computadores que utiliza o firewall do tipo roteador de barreira, o endereço IP dos pontos da rede interna é substituído pelo endereço do servidor de segurança da rede.~~

~~[104] Quando a rede de comunicação dispõe de firewall do tipo gateway servidor de proxy, é necessário o uso programas de administração para a filtragem dos pacotes com base no endereço IP.~~

3. Julgue os itens subsecutivos, referentes a proxy cache e proxy reverso.

[114] Proxy reverso pode encaminhar uma solicitação para um número de porta diferente da porta na qual a solicitação foi recebida originalmente.

[115] O proxy cache permite otimizar o tráfego originado da Internet, o que diminui o congestionamento e aumenta a velocidade de transferência de dados, contudo ele não desempenha nenhuma função relacionada com a segurança da rede de comunicação.

3. Julgue os itens subsecutivos, referentes a proxy cache e proxy reverso.

[114] Proxy reverso pode encaminhar uma solicitação para um número de porta diferente da porta na qual a solicitação foi recebida originalmente.

~~[115] O proxy cache permite otimizar o tráfego originado da Internet, o que diminui o congestionamento e aumenta a velocidade de transferência de dados, contudo ele não desempenha nenhuma função relacionada com a segurança da rede de comunicação.~~

4. A respeito dos conceitos de qualidade de serviço (QoS) e de segurança em redes de computadores, julgue os próximos itens.

[65] O firewall proxy de uma rede, quando recebe uma mensagem externa de um processo cliente-usuário, executa um processo de servidor para receber a solicitação, abre o pacote e determina se a solicitação é legítima. Em caso positivo, ele executa um processo cliente e envia a mensagem para o verdadeiro servidor na rede; em caso negativo, a mensagem é eliminada e um aviso de erro é enviado para o usuário externo.

4. A respeito dos conceitos de qualidade de serviço (QoS) e de segurança em redes de computadores, julgue os próximos itens.

[65] O firewall proxy de uma rede, quando recebe uma mensagem externa de um processo cliente-usuário, executa um processo de servidor para receber a solicitação, abre o pacote e determina se a solicitação é legítima. Em caso positivo, ele executa um processo cliente e envia a mensagem para o verdadeiro servidor na rede; em caso negativo, a mensagem é eliminada e um aviso de erro é enviado para o usuário externo.

5. Considere que a equipe de suporte técnico de determinada empresa necessite fazer escolhas, configurações e procedimentos concernentes a segurança da informação da rede de computadores dessa empresa. Nessa situação, julgue os itens seguintes.

[84] Se a empresa instalar um servidor proxy, este permitirá que se mantenha um registro dos sítios visitados pelos funcionários, contudo a utilização desse servidor causaria pequeno aumento do tempo de resposta a requisições HTTP de clientes.

[85] Ao se instalar um servidor proxy squid em computador com sistema operacional Linux, o serviço deve ser criado no usuário root, por motivo de segurança.

5. Considere que a equipe de suporte técnico de determinada empresa necessite fazer escolhas, configurações e procedimentos concernentes a segurança da informação da rede de computadores dessa empresa. Nessa situação, julgue os itens seguintes.

~~[84] Se a empresa instalar um servidor proxy, este permitirá que se mantenha um registro dos sítios visitados pelos funcionários, contudo a utilização desse servidor causaria pequeno aumento do tempo de resposta a requisições HTTP de clientes.~~

~~[85] Ao se instalar um servidor proxy squid em computador com sistema operacional Linux, o serviço deve ser criado no usuário root, por motivo de segurança.~~

6. Na rede de computadores de uma organização pública brasileira com diversos ativos, como, por exemplo, switches, roteadores, firewalls, estações de trabalho, hosts servidores de aplicação web, servidores de bancos de dados, é comum a ocorrência de ataques e de outros incidentes que comprometem a segurança de seus sistemas. Nessa organização, a definição de políticas e metodologias adequadas para se lidar com esse tipo de problema cabe ao departamento de TI.

A partir da situação apresentada acima, julgue os itens relativos à segurança da informação.

[180] Se o administrador da rede de computadores tiver de escolher entre implantar um proxy firewall ou um firewall do tipo packet filter, a sua decisão deverá basear-se em um dos dois critérios seguintes: necessidade de atuação na camada de aplicação ou maior vazão de dados. Se o critério preponderante for o primeiro, então, a decisão deve ser favorável à instalação de proxy firewalls; se for o segundo, deve ser escolhido um packet filter.

6. Na rede de computadores de uma organização pública brasileira com diversos ativos, como, por exemplo, switches, roteadores, firewalls, estações de trabalho, hosts servidores de aplicação web, servidores de bancos de dados, é comum a ocorrência de ataques e de outros incidentes que comprometem a segurança de seus sistemas. Nessa organização, a definição de políticas e metodologias adequadas para se lidar com esse tipo de problema cabe ao departamento de TI.

A partir da situação apresentada acima, julgue os itens relativos à segurança da informação.

[180] Se o administrador da rede de computadores tiver de escolher entre implantar um proxy firewall ou um firewall do tipo packet filter, a sua decisão deverá basear-se em um dos dois critérios seguintes: necessidade de atuação na camada de aplicação ou maior vazão de dados. Se o critério preponderante for o primeiro, então, a decisão deve ser favorável à instalação de proxy firewalls; se for o segundo, deve ser escolhido um packet filter.

7.Com relação a firewalls, julgue os itens subseqüentes

- Em uma rede protegida por firewall composto por proxies, quando um cliente, fora da rede, se comunica com um servidor, na rede, um proxy se faz passar pelo servidor e intermedeia a comunicação.

- Firewalls embasados em proxy são capazes de tratar diversos protocolos de aplicação. Por exemplo, um proxy de FTP deve ser capaz de tratar o protocolo de aplicação FTP para poder se fazer passar por esse serviço.

7.Com relação a firewalls, julgue os itens subseqüentes

- Em uma rede protegida por firewall composto por proxies, quando um cliente, fora da rede, se comunica com um servidor, na rede, um proxy se faz passar pelo servidor e intermedeia a comunicação.

- Firewalls embasados em proxy são capazes de tratar diversos protocolos de aplicação. Por exemplo, um proxy de FTP deve ser capaz de tratar o protocolo de aplicação FTP para poder se fazer passar por esse serviço.

8. Com relação segurança em redes de computadores, julgue os itens a seguir

[119] Com um proxy HTTP no firewall, os usuários remotos podem estabelecer uma conexão HTTP/TCP com o proxy, que examina o URL contido na mensagem de solicitação. Se a página solicitada for permitida para o host de origem, o proxy estabelece uma segunda conexão HTTP/TCP com o servidor e para ele encaminha a solicitação.

8. Com relação segurança em redes de computadores, julgue os itens a seguir

[119] Com um proxy HTTP no firewall, os usuários remotos podem estabelecer uma conexão HTTP/TCP com o proxy, que examina o URL contido na mensagem de solicitação. Se a página solicitada for permitida para o host de origem, o proxy estabelece uma segunda conexão HTTP/TCP com o servidor e para ele encaminha a solicitação.

9. Com relação a firewalls, proxies e IDS, julgue os itens seguintes

[144] Proxies têm funções idênticas a firewalls, mas, enquanto os proxies operam nas camadas TCP/IP 3 e 4, os firewalls atuam no nível da aplicação.

9. Com relação a firewalls, proxies e IDS, julgue os itens seguintes

~~[144] Proxies têm funções idênticas a firewalls, mas, enquanto os proxies operam nas camadas TCP/IP 3 e 4, os firewalls atuam no nível da aplicação.~~

GABARITO

1. E
2. C, E, E
3. C, E
4. C
5. E, E
6. C
7. C, C
8. C
9. E

Sétima Bateria de Questões Com Resolução Assistida

Malware: Vírus de computador, cavalo de tróia, adware, spyware, backdoors, keylogger, worms

1. Em relação à segurança e à proteção de informações na Internet, julgue os itens subsequentes

[107] Cavalo de Tróia, também conhecido como trojan, é um programa malicioso que, assim como os worms, possui instruções para auto-reaplicação.

[108] Spyware é um programa ou dispositivo que monitora as atividades de um sistema e transmite a terceiros informações relativas a essas atividades, sem o consentimento do usuário. Como exemplo, o keylogger é um spyware capaz de armazenar as teclas digitadas pelo usuário no teclado do computador.

[109] Vírus são programas que podem apagar arquivos importantes armazenados no computador, podendo ocasionar, até mesmo, a total inutilização do sistema operacional.

[110] Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.

1. Em relação à segurança e à proteção de informações na Internet, julgue os itens subsequentes

~~[107] Cavalo de Tróia, também conhecido como trojan, é um programa malicioso que, assim como os worms, possui instruções para auto-reaplicação.~~

[108] Spyware é um programa ou dispositivo que monitora as atividades de um sistema e transmite a terceiros informações relativas a essas atividades, sem o consentimento do usuário. Como exemplo, o keylogger é um spyware capaz de armazenar as teclas digitadas pelo usuário no teclado do computador.

[109] Vírus são programas que podem apagar arquivos importantes armazenados no computador, podendo ocasionar, até mesmo, a total inutilização do sistema operacional.

[110] Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.

2. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[100] Phishing é a técnica empregada por vírus e cavalos de tróia para obter informações confidenciais do usuário, como, por exemplo, dados bancários.

2. Julgue os seguintes itens, relativos à segurança em redes de computadores.

~~[100] Phishing é a técnica empregada por vírus e cavalos de tróia para obter informações confidenciais do usuário, como, por exemplo, dados bancários.~~

3. Os computadores conectados em redes ou à Internet estão expostos ao ataque de muitos tipos de programas maliciosos. Acerca desses programas, julgue os itens subsequentes:

[89] Para que seja instalado em um computador, é necessário que o spyware seja explicitamente executado pelo usuário.

[90] Um cavalo de tróia é um tipo de programa malicioso que, uma vez instalado no computador, possibilita o seu controle remotamente.

[91] Um vírus é um programa malicioso que tem a capacidade de se auto-replicar, independentemente da execução de qualquer outro programa.

3. Os computadores conectados em redes ou à Internet estão expostos ao ataque de muitos tipos de programas maliciosos. Acerca desses programas, julgue os itens subsequentes:

[89] Para que seja instalado em um computador, é necessário que o spyware seja explicitamente executado pelo usuário.

[90] Um cavalo de tróia é um tipo de programa malicioso que, uma vez instalado no computador, possibilita o seu controle remotamente.

~~[91] Um vírus é um programa malicioso que tem a capacidade de se auto-replicar, independentemente da execução de qualquer outro programa.~~

4. Acerca da identificação de códigos maliciosos e de técnicas de phishing e spam, julgue os próximos itens

[93] Uma das maneiras de se combater, com antecedência, o ataque de phishing é a utilização de um servidor NFS (network file system) na rede local para os usuários.

[94] Em computador infectado com um código malicioso conhecido como cavalo de tróia (trojan), não são disponibilizadas portas para acessos de outros computadores.

[95] Uma das técnicas de phishing consiste em envenenar cache de servidores DNS, fornecendo, assim, URLs falsas aos usuários que consultam esse servidor DNS e apontando para servidores diferentes do original.

4. Acerca da identificação de códigos maliciosos e de técnicas de phishing e spam, julgue os próximos itens

~~[93] Uma das maneiras de se combater, com antecedência, o ataque de phishing é a utilização de um servidor NFS (network file system) na rede local para os usuários.~~

~~[94] Em computador infectado com um código malicioso conhecido como cavalo de tróia (trojan), não são disponibilizadas portas para acessos de outros computadores.~~

[95] Uma das técnicas de phishing consiste em envenenar cache de servidores DNS, fornecendo, assim, URLs falsas aos usuários que consultam esse servidor DNS e apontando para servidores diferentes do original.

5. Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Com relação a esse tema, julgue os próximos itens.

[37] Firewalls são dispositivos de segurança que podem evitar a contaminação e a propagação de vírus. Por outro lado, antivírus são ferramentas de segurança capazes de detectar e evitar ataques provenientes de uma comunicação em rede.

[38] Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

5. Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Com relação a esse tema, julgue os próximos itens.

~~[37] Firewalls são dispositivos de segurança que podem evitar a contaminação e a propagação de vírus. Por outro lado, antivírus são ferramentas de segurança capazes de detectar e evitar ataques provenientes de uma comunicação em rede.~~

[38] Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

6. Acerca da segurança da informação, julgue os itens subsequentes.

[57] Considere que uma mensagem de correio eletrônico, supostamente vinda do provedor de Internet, sob a alegação de que o computador que recebia a mensagem estava infectado por um vírus, sugeria que fosse instalada uma ferramenta de desinfecção. Considere ainda que na verdade, a ferramenta oferecida era um programa malicioso que, após a instalação, tornou os dados pessoais do usuário acessíveis ao remetente da mensagem. Nessa situação hipotética, é correto afirmar que houve um ataque de engenharia social.

6. Acerca da segurança da informação, julgue os itens subsequentes.

[57] Considere que uma mensagem de correio eletrônico, supostamente vinda do provedor de Internet, sob a alegação de que o computador que recebia a mensagem estava infectado por um vírus, sugeria que fosse instalada uma ferramenta de desinfecção. Considere ainda que na verdade, a ferramenta oferecida era um programa malicioso que, após a instalação, tornou os dados pessoais do usuário acessíveis ao remetente da mensagem. Nessa situação hipotética, é correto afirmar que houve um ataque de engenharia social.

7. A respeito da segurança de redes de computadores, julgue os itens

[87] Os ataques a computadores na Internet acontecem de diversas formas. Uma delas é a negação de serviço, na qual o computador atacado recebe diversas tentativas de acesso a determinado serviço até que usuário e senha sejam finalmente descobertos. Tal ataque é conhecido como DdoS (distributed denial of service).

7. A respeito da segurança de redes de computadores, julgue os itens

~~[87] Os ataques a computadores na Internet acontecem de diversas formas. Uma delas é a negação de serviço, na qual o computador atacado recebe diversas tentativas de acesso a determinado serviço até que usuário e senha sejam finalmente descobertos. Tal ataque é conhecido como DdoS (distributed denial of service).~~

8. Com relação a sistemas antivírus e malwares, em geral, julgue os próximos itens.

[71] Um mesmo vírus de computador é capaz de infectar várias máquinas. Uma estação de trabalho, normalmente, pode conter vários vírus diferentes e aptos a serem executados ao mesmo tempo.

[72] Uma característica dos vírus de computador do tipo worm é a sua incapacidade de se disseminar autonomamente: eles necessitam da intervenção de um usuário que os execute e, só assim, se propagam e infectam outros usuários.

8. Com relação a sistemas antivírus e malwares, em geral, julgue os próximos itens.

[71] Um mesmo vírus de computador é capaz de infectar várias máquinas. Uma estação de trabalho, normalmente, pode conter vários vírus diferentes e aptos a serem executados ao mesmo tempo.

~~[72] Uma característica dos vírus de computador do tipo worm é a sua incapacidade de se disseminar autonomamente: eles necessitam da intervenção de um usuário que os execute e, só assim, se propagam e infectam outros usuários.~~

9. Julgue os itens subsequentes, acerca de antivírus.

[99] Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.

[100] Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.

[101] As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

9. Julgue os itens subsequentes, acerca de antivírus.

[99] Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.

~~[100] Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.~~

~~[101] As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.~~

10. Quanto à segurança em rede de computadores, julgue os itens .

[76] Worm é um vírus que tem a capacidade de auto-replicação, espalhando-se rapidamente de uma rede para outra, mas somente causa danos se for ativado pelo usuário.

[77] Adware é qualquer programa que, depois de instalado, automaticamente executa, mostra ou baixa publicidade para o computador. Alguns desses programas têm instruções para captar informações pessoais e passá-la para terceiros, sem a autorização ou o conhecimento do usuário, o que caracteriza a prática conhecida como spyware.

[78] Backdoor consiste em uma falha de segurança que pode existir em um programa de computador ou sistema operacional. Essa falha permite que sejam instalados vírus de computador ou outros programas maliciosos, conhecidos como malware, utilizando-se exclusivamente de serviços executados em background.

[79] Keylogger é um programa de computador do tipo spyware cuja finalidade é monitorar tudo o que for digitado, a fim de descobrir senhas de banco, números de cartão de crédito e afins. Alguns casos de phishing e determinados tipos de fraudes virtuais baseiam-se no uso de keylogger.

10. Quanto à segurança em rede de computadores, julgue os itens .

~~[76] Worm é um vírus que tem a capacidade de auto-replicação, espalhando-se rapidamente de uma rede para outra, mas somente causa danos se for ativado pelo usuário.~~

[77] Adware é qualquer programa que, depois de instalado, automaticamente executa, mostra ou baixa publicidade para o computador. Alguns desses programas têm instruções para captar informações pessoais e passá-la para terceiros, sem a autorização ou o conhecimento do usuário, o que caracteriza a prática conhecida como spyware.

~~[78] Backdoor consiste em uma falha de segurança que pode existir em um programa de computador ou sistema operacional. Essa falha permite que sejam instalados vírus de computador ou outros programas maliciosos, conhecidos como malware, utilizando-se exclusivamente de serviços executados em background.~~

[79] Keylogger é um programa de computador do tipo spyware cuja finalidade é monitorar tudo o que for digitado, a fim de descobrir senhas de banco, números de cartão de crédito e afins. Alguns casos de phishing e determinados tipos de fraudes virtuais baseiam-se no uso de keylogger.

GABARITO

1. E, E, C, C, C
2. E
3. C, C, E
4. E, E, C
5. E, C
6. C
7. E
8. C, E
9. C, E, E
10. E, C, E, C

Oitava Bateria de Questões Com Resolução Assistida

Malware: **Vírus de computador, cavalo de tróia, adware, spyware, backdoors, keylogger, worms**

1. No que concerne à segurança, julgue os itens subsequentes.

[69] Os firewalls que mantêm o estado das conexões atuam na camada de rede, mas podem tomar decisões com base em informações das camadas de transporte e aplicação. Por esse motivo, conseguem perceber mais facilmente as tentativas de DOS (denial of service) nos servidores protegidos por esse firewall.

1. No que concerne à segurança, julgue os itens subsequentes.

[69] Os firewalls que mantêm o estado das conexões atuam na camada de rede, mas podem tomar decisões com base em informações das camadas de transporte e aplicação. Por esse motivo, conseguem perceber mais facilmente as tentativas de DOS (denial of service) nos servidores protegidos por esse firewall.

2. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[119] DDOS (distributed denial of service) é um tipo de ataque que tem a finalidade de inviabilizar o funcionamento de um computador. Para isso, a partir de vários computadores, é enviada grande quantidade de requisições a determinado serviço, a fim de consumir os recursos do computador alvo do ataque.

2. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[119] DDOS (distributed denial of service) é um tipo de ataque que tem a finalidade de inviabilizar o funcionamento de um computador. Para isso, a partir de vários computadores, é enviada grande quantidade de requisições a determinado serviço, a fim de consumir os recursos do computador alvo do ataque.

3. Considerando-se que ataques do tipo DOS (denial of service), conhecidos como ataques de negação de serviço, são capazes de indisponibilizar um serviço de rede, enviando um número de solicitações muito além do normal, uma das ações que permitem diminuir o impacto imediato desse tipo de ataque é a de

A. restringir a quantidade de conexões simultâneas aceitas no servidor para a manutenção do serviço disponível.

B. utilizar o protocolo HTTPS.

C. impedir acessos remotos para administração do servidor.

D. instalar um sniffer de rede, configurando-o para monitorar o tráfego.

E. monitorar o consumo de banda da rede

3. Considerando-se que ataques do tipo DOS (denial of service), conhecidos como ataques de negação de serviço, são capazes de indisponibilizar um serviço de rede, enviando um número de solicitações muito além do normal, uma das ações que permitem diminuir o impacto imediato desse tipo de ataque é a de

A. restringir a quantidade de conexões simultâneas aceitas no servidor para a manutenção do serviço disponível.

~~B. utilizar o protocolo HTTPS.~~

~~C. impedir acessos remotos para administração do servidor.~~

~~D. instalar um sniffer de rede, configurando-o para monitorar o tráfego.~~

~~E. monitorar o consumo de banda da rede~~

4. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir.

[100] Ataques de phishing são potencialmente mais comprometedores da disponibilidade que ataques de DDoS (distributed denial of service) provocados por worms.

4. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir.

~~[100] Ataques de phishing são potencialmente mais comprometedores da disponibilidade que ataques de DDoS (distributed denial of service) provocados por worms.~~

5. Quanto à segurança em rede de computadores, julgue os itens .

[71] Uma rede interna pode ser protegida contra o IP spoofing por meio da aplicação de filtros; como exemplo, se a rede tem endereços do tipo 100.200.200.0, então o firewall deve bloquear tentativas de conexão originadas externamente, caso a origem tenha endereços de rede do tipo 100.200.200.0.

[72] Em um ataque do tipo DoS (denial of service attack), os pacotes de resposta trazem informações do usuário para o hacker/cracker.

[73] O DDoS (distributed denial of service) é um tipo de ataque coordenado, no qual diversos hosts são atacados e coordenados pelo hacker, para a realização de ataques simultâneos aos alvos.

[74] O SYN flooding é um tipo de ataque que explora o mecanismo de conexões IP, gerando um grande número de requisições em um servidor web.

[75] Cavalo de tróia é um software legítimo que o usuário utiliza normalmente, mas, ao mesmo tempo, executa outras funções ilegais, como enviar mensagens e arquivos para o hacker ou abrir portas de entrada para futuras invasões.

5. Quanto à segurança em rede de computadores, julgue os itens .

[71] Uma rede interna pode ser protegida contra o IP spoofing por meio da aplicação de filtros; como exemplo, se a rede tem endereços do tipo 100.200.200.0, então o firewall deve bloquear tentativas de conexão originadas externamente, caso a origem tenha endereços de rede do tipo 100.200.200.0.

~~[72] Em um ataque do tipo DoS (denial of service attack), os pacotes de resposta trazem informações do usuário para o hacker/cracker.~~

[73] O DDoS (distributed denial of service) é um tipo de ataque coordenado, no qual diversos hosts são atacados e coordenados pelo hacker, para a realização de ataques simultâneos aos alvos.

~~[74] O SYN flooding é um tipo de ataque que explora o mecanismo de conexões IP, gerando um grande número de requisições em um servidor web.~~

[75] Cavalo de tróia é um software legítimo que o usuário utiliza normalmente, mas, ao mesmo tempo, executa outras funções ilegais, como enviar mensagens e arquivos para o hacker ou abrir portas de entrada para futuras invasões.

6. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.

[102] Considere que, utilizando um sniffer junto ao segmento que liga a rede de uma organização à Internet, um dos auditores identifique, durante poucos segundos, a ocorrência de milhares de pacotes SYN e SYN/ACK trafegando na rede, para os quais não havia correspondentes pacotes ACK. Considere ainda que o auditor constate que os endereços fonte dos pacotes SYN e os endereços destino dos pacotes SYN/ACK eram de um host desconhecido pela organização, enquanto os endereços destino dos pacotes SYN e os endereços fonte dos pacotes SYN/ACK eram de um host pertencente à rede DMZ da organização. Nesse caso, a partir dos dados coletados, é correto inferir que a organização poderia estar, naquele momento, sofrendo um ataque de negação de serviço DOS (denial of service).

6. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

~~[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.~~

[102] Considere que, utilizando um sniffer junto ao segmento que liga a rede de uma organização à Internet, um dos auditores identifique, durante poucos segundos, a ocorrência de milhares de pacotes SYN e SYN/ACK trafegando na rede, para os quais não havia correspondentes pacotes ACK. Considere ainda que o auditor constate que os endereços fonte dos pacotes SYN e os endereços destino dos pacotes SYN/ACK eram de um host desconhecido pela organização, enquanto os endereços destino dos pacotes SYN e os endereços fonte dos pacotes SYN/ACK eram de um host pertencente à rede DMZ da organização. Nesse caso, a partir dos dados coletados, é correto inferir que a organização poderia estar, naquele momento, sofrendo um ataque de negação de serviço DOS (denial of service).

7. As vulnerabilidades de segurança da família de protocolos TCP/IP têm sido ativamente exploradas nos últimos anos, visando à realização de ataques a sistemas computacionais interconectados à Internet. Em contrapartida a esses ataques, vários mecanismos e sistemas de proteção, defesa e contra-ataque têm sido criados, como firewalls, IPSs (intrusion prevention systems) e IDSs (intrusion detection systems). Com relação a vulnerabilidades e ataques às redes de computadores, julgue os itens seguintes.

I Entre os métodos de ataque relacionados a DoS (denial of service), está o ataque de smurf, concentrado na camada IP, embasado no protocolo ICMP, no spoof de endereços fonte em pacotes e com amplificação por meio de repasse de pacotes dirigidos a endereço de broadcast.

II O ataque ping da morte (ping of death), ainda comum nos sistemas Windows sem a proteção de firewalls, gera DoS devido à fragmentação entre as camadas de rede e de enlace, bem como devido à geração de buffer overflow.

III A tentativa de ataque embasada no spoof de endereços IP do tipo non-blind spoofing tem maior sucesso quando o alvo atacado estiver na mesma sub-rede do atacante.

IV Quando um spoofing IP tem por objetivo principal a negação de serviço e, não, a captura de sessão, há menor necessidade de um atacante manipular os números de sequência e acknowledgement presentes no cabeçalho de pacotes TCP.

V Ataques do tipo SYN flooding em geral são bem sucedidos quando esgotam a capacidade de recebimento de datagramas UDP por parte dos hosts alvos.

Estão certos apenas os itens

A. I, II e III.
B. I, II e V.
C. I, III e IV.
D. II, IV e V.
E. III, IV e V.

7. As vulnerabilidades de segurança da família de protocolos TCP/IP têm sido ativamente exploradas nos últimos anos, visando à realização de ataques a sistemas computacionais interconectados à Internet. Em contrapartida a esses ataques, vários mecanismos e sistemas de proteção, defesa e contra-ataque têm sido criados, como firewalls, IPSs (intrusion prevention systems) e IDSs (intrusion detection systems). Com relação a vulnerabilidades e ataques às redes de computadores, julgue os itens seguintes.

I Entre os métodos de ataque relacionados a DoS (denial of service), está o ataque de smurf, concentrado na camada IP, embasado no protocolo ICMP, no spoof de endereços fonte em pacotes e com amplificação por meio de repasse de pacotes dirigidos a endereço de broadcast.

II O ataque ping da morte (ping of death), ainda comum nos sistemas Windows sem a proteção de firewalls, gera DoS devido à fragmentação entre as camadas de rede e de enlace, bem como devido à geração de buffer overflow.

III A tentativa de ataque embasada no spoof de endereços IP do tipo non-blind spoofing tem maior sucesso quando o alvo atacado estiver na mesma sub-rede do atacante.

IV Quando um spoofing IP tem por objetivo principal a negação de serviço e, não, a captura de sessão, há menor necessidade de um atacante manipular os números de sequência e acknowledgement presentes no cabeçalho de pacotes TCP.

V Ataques do tipo SYN flooding em geral são bem sucedidos quando esgotam a capacidade de recebimento de datagramas UDP por parte dos hosts alvos.

Estão certos apenas os itens

~~A. I, II e III.~~

~~B. I, II e V.~~

C. I, III e IV.

~~D. II, IV e V.~~

~~E. III, IV e V.~~

8. A respeito de ataques a redes de computadores e de incidentes de segurança, julgue os itens.

[81] O incidente denominado DDoS deve ser tratado de maneira diferente de outros tipos de incidente de segurança, pois dificilmente um firewall ou IDS gerará log. Sua notificação de incidente deve informar o cabeçalho e o conteúdo completos da mensagem recebida pelo usuário.

[82] Um ataque de negação de serviço (DoS) não é uma invasão do sistema e objetiva tornar os recursos de um sistema indisponíveis para seus utilizadores. O ataque tenta indisponibilizar páginas hospedadas em servidores web e produz como efeito uma invalidação por sobrecarga.

[83] No phishing, diversas máquinas zumbis comandadas por um mestre fazem requisições ao mesmo tempo, gerando sobrecarga do recurso atacado, o que pode levar a máquina servidora a reiniciar ou a travar.

[84] No ping flood, o atacante sobrecarrega o sistema vítima com pactos ICMP echo request (pacotes ping). Para o ataque ser bem sucedido, o atacante deve possuir maior largura de banda que a vítima, que, ao tentar responder aos pedidos, irá consumir a sua própria largura de banda, impossibilitando-a de responder a pedidos de outros utilizadores. Uma das formas de prevenir esse tipo de ataque é limitar o tráfego de pacotes ICMP echo request.

[85] No syn flood ou ataque syn, o atacante envia uma sequência de requisições syn para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

8. A respeito de ataques a redes de computadores e de incidentes de segurança, julgue os itens.

~~[81] O incidente denominado DDoS deve ser tratado de maneira diferente de outros tipos de incidente de segurança, pois dificilmente um firewall ou IDS gerará log. Sua notificação de incidente deve informar o cabeçalho e o conteúdo completos da mensagem recebida pelo usuário.~~

[82] Um ataque de negação de serviço (DoS) não é uma invasão do sistema e objetiva tornar os recursos de um sistema indisponíveis para seus utilizadores. O ataque tenta indisponibilizar páginas hospedadas em servidores web e produz como efeito uma invalidação por sobrecarga.

~~[83] No phishing, diversas máquinas zumbis comandadas por um mestre fazem requisições ao mesmo tempo, gerando sobrecarga do recurso atacado, o que pode levar a máquina servidora a reiniciar ou a travar.~~

[84] No ping flood, o atacante sobrecarrega o sistema vítima com pactos ICMP echo request (pacotes ping). Para o ataque ser bem sucedido, o atacante deve possuir maior largura de banda que a vítima, que, ao tentar responder aos pedidos, irá consumir a sua própria largura de banda, impossibilitando-a de responder a pedidos de outros utilizadores. Uma das formas de prevenir esse tipo de ataque é limitar o tráfego de pacotes ICMP echo request.

[85] No syn flood ou ataque syn, o atacante envia uma sequência de requisições syn para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

9. Com relação a malwares, julgue os próximos itens.

[86] Um adware difere de um spyware pela intenção. O primeiro é projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros, e o segundo é projetado especificamente para apresentar propagandas.

[87] O cavalo de tróia (trojan horse) não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de software instalados em computadores.

[88] Ao se executar um programa previamente infectado - como, por exemplo, ao se abrir arquivo anexado a e-mail ou ao se instalar programas de procedência duvidosa ou desconhecida -, um vírus pode infectar o computador. Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador.

[89] Um worm pode realizar diversas funções maliciosas, como a instalação de keyloggers ou screenloggers, o furto de senhas e outras informações sensíveis, como números de cartões de crédito, a inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador, e a alteração ou destruição de arquivos.

[90] O worm costuma ser apenas um único arquivo que necessita ser executado para que infecte o computador destinatário e, de modo distinto do vírus ou do cavalo de tróia, não costuma infectar outros arquivos e nem propagar, automaticamente, cópias de si mesmo.

9. Com relação a malwares, julgue os próximos itens.

~~[86] Um adware difere de um spyware pela intenção. O primeiro é projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros, e o segundo é projetado especificamente para apresentar propagandas.~~

~~[87] O cavalo de tróia (trojan horse) não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de software instalados em computadores~~.

[88] Ao se executar um programa previamente infectado - como, por exemplo, ao se abrir arquivo anexado a e-mail ou ao se instalar programas de procedência duvidosa ou desconhecida -, um vírus pode infectar o computador. Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador.

~~[89] Um worm pode realizar diversas funções maliciosas, como a instalação de keyloggers ou screenloggers, o furto de senhas e outras informações sensíveis, como números de cartões de crédito, a inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador, e a alteração ou destruição de arquivos.~~

~~[90] O worm costuma ser apenas um único arquivo que necessita ser executado para que infecte o computador destinatário e, de modo distinto do vírus ou do cavalo de tróia, não costuma infectar outros arquivos e nem propagar, automaticamente, cópias de si mesmo.~~

10. Julgue os próximos itens no que se refere a ataques a redes de computadores e malwares.

[67] DoS e DDoS são ataques que têm por finalidade a indisponibilização dos serviços das redes. Um IDS, corretamente instalado e configurado, é capaz de proteger totalmente a rede de ataques do tipo DoS, mas não protege a rede de ataques do tipo DDoS.

[68] Cavalo de tróia é um malware que instala-se em uma máquina, sem que seu usuário perceba, para extrair ou destruir dados sem autorização. Esse tipo de programa é executado automaticamente e em background sempre que a máquina é inicializada.

10. Julgue os próximos itens no que se refere a ataques a redes de computadores e malwares.

~~[67] DoS e DDoS são ataques que têm por finalidade a indisponibilização dos serviços das redes. Um IDS, corretamente instalado e configurado, é capaz de proteger totalmente a rede de ataques do tipo DoS, mas não protege a rede de ataques do tipo DDoS.~~

~~[68] Cavalo de tróia é um malware que instala-se em uma máquina, sem que seu usuário perceba, para extrair ou destruir dados sem autorização. Esse tipo de programa é executado automaticamente e em background sempre que a máquina é inicializada.~~

GABARITO

1. C
2. C
3. A
4. E
5. C, E, C, E, C
6. E, C
7. C
8. E, C, E, C, C
9. E, E, C, E, E
10. E, E

Nona Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: NAT, VPN

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.

[114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

~~[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.~~

[114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

~~[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.~~

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.

[86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.

[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.

[89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

~~[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.~~

[86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

~~[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.~~

~~[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.~~

[89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

3. Assinale a opção correta acerca de NAT (network address translation).

A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.

B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.

C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.

D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.

E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

3. Assinale a opção correta acerca de NAT (network address translation).

A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.

B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.

C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.

D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.

E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.

B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.

C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.

D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.

E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.

B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.

C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.

D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.

E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

[85] As redes VPN oferecem suporte apenas ao protocolo IP.

[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.

[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

~~[85] As redes VPN oferecem suporte apenas ao protocolo IP.~~

[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.

~~[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.~~

6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.

6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.

7. Em relação à VPN (virtual private network), julgue os próximos itens.

[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.

[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.

7. Em relação à VPN (virtual private network), julgue os próximos itens.

~~[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.~~

~~[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.~~

8. Em relação a segurança da informação, julgue os itens seguintes.

[84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

[85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

8. Em relação a segurança da informação, julgue os itens seguintes.

[84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

[85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

~~[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.~~

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

[59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

[59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

~~[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.~~

GABARITO

1. E, C, E
2. E, C, E, E, C
3. C
4. B
5. E, C, E
6. C
7. E, E
8. C, C
9. E
10. C, E

Décima Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: NAT, VPN

1. Julgue os itens que se seguem, relativos a aplicações web e conceitos de VPN (virtual private network).

[71] Uma VPN é uma rede privada porque é de uso exclusivo de uma organização ou empresa e é uma rede virtual porque ela não constitui uma WAN privada real (ou física).

1. Julgue os itens que se seguem, relativos a aplicações web e conceitos de VPN (virtual private network).

[71] Uma VPN é uma rede privada porque é de uso exclusivo de uma organização ou empresa e é uma rede virtual porque ela não constitui uma WAN privada real (ou física).

2. Com relação a VPN, julgue os itens que se seguem.

[118] Uma VPN é uma conexão estabelecida sobre uma infra-estrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

[119] Apesar de ser uma opção disponível, não se recomenda o uso de autenticação junto com cifração em VPNs, considerando a diminuição de desempenho.

[120] Preferencialmente, as VPNs são implementadas sobre protocolos de rede orientados à conexão como o TCP.

2. Com relação a VPN, julgue os itens que se seguem.

[118] Uma VPN é uma conexão estabelecida sobre uma infra-estrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

~~[119] Apesar de ser uma opção disponível, não se recomenda o uso de autenticação junto com cifração em VPNs, considerando a diminuição de desempenho.~~

~~[120] Preferencialmente, as VPNs são implementadas sobre protocolos de rede orientados à conexão como o TCP.~~

3. Com relação a criptografia e VPN, julgue os itens subseqüentes

[146] Uma VPN é uma conexão estabelecida sobre uma infra-estrutura pública ou compartilhada usando-se tecnologias de criptografia e autenticação para garantir a segurança das informações trafegadas.

[147] Uma VPN pode ser estabelecida em várias camadas, tal como aplicação, transporte, redes ou enlace.

[148] Essencialmente, uma VPN é um túnel cifrado cujo estabelecimento está sujeito a autenticação.

3. Com relação a criptografia e VPN, julgue os itens subseqüentes

[146] Uma VPN é uma conexão estabelecida sobre uma infra-estrutura pública ou compartilhada usando-se tecnologias de criptografia e autenticação para garantir a segurança das informações trafegadas.

[147] Uma VPN pode ser estabelecida em várias camadas, tal como aplicação, transporte, redes ou enlace.

[148] Essencialmente, uma VPN é um túnel cifrado cujo estabelecimento está sujeito a autenticação.

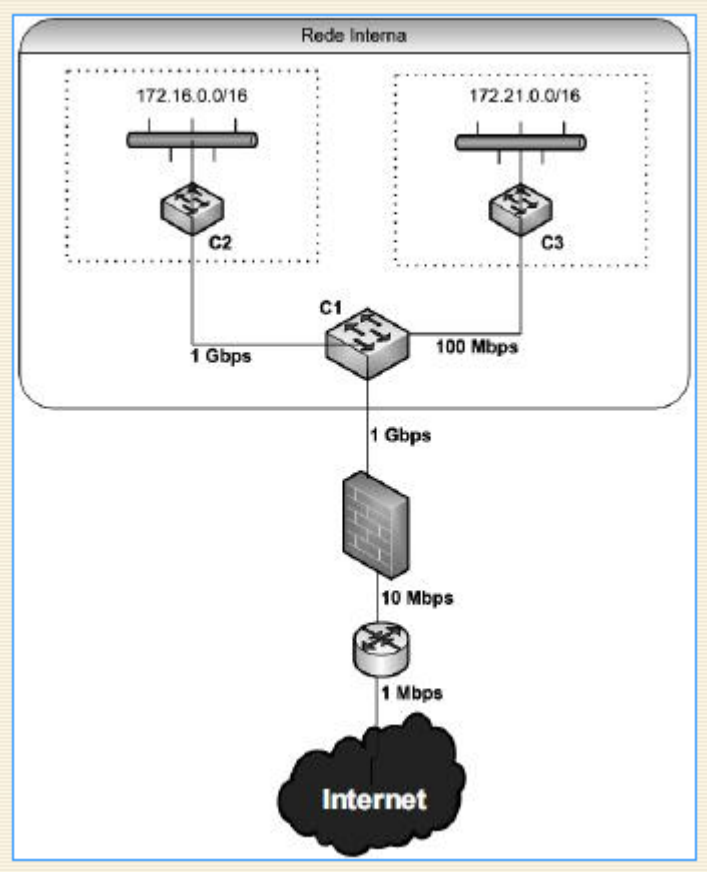
4. Julgue os próximos itens com relação ao emprego adequado de dispositivos de segurança de redes de computadores.

[102] Se o objetivo para implantação de uma VPN por meio da suíte IPSec for a garantia de integridade de dados, a autenticação de dados na origem, a confidencialidade e o antireplay, então é indicado o uso do protocolo ESP (encapsulation security payload) ao invés do protocolo AH (authentication header).

4. Julgue os próximos itens com relação ao emprego adequado de dispositivos de segurança de redes de computadores.

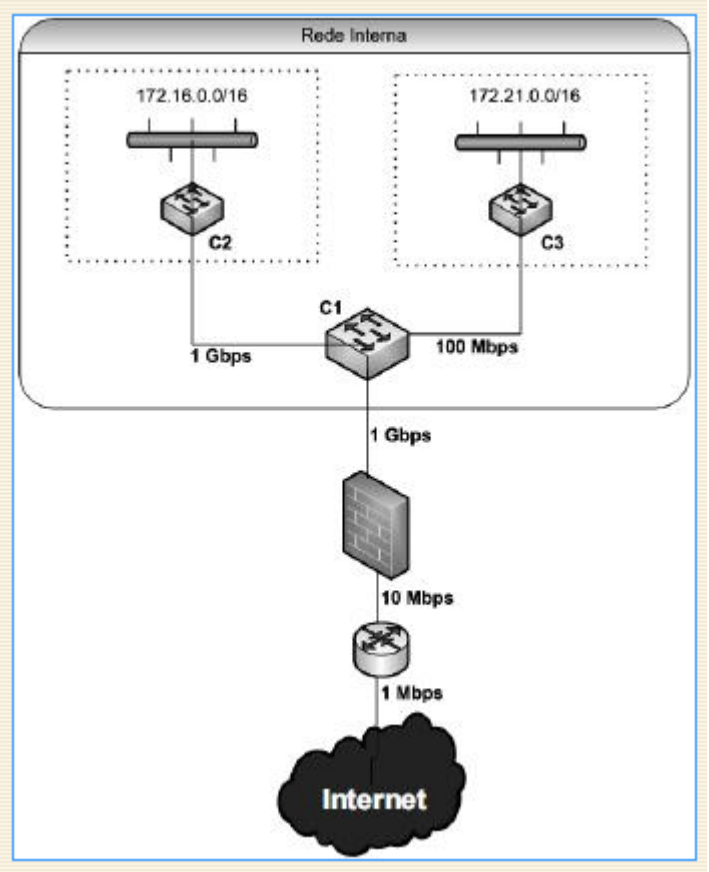
[102] Se o objetivo para implantação de uma VPN por meio da suíte IPSec for a garantia de integridade de dados, a autenticação de dados na origem, a confidencialidade e o antireplay, então é indicado o uso do protocolo ESP (encapsulation security payload) ao invés do protocolo AH (authentication header).

5. A partir da figura acima, julgue os itens a seguir, acerca de conexões e componentes de rede.

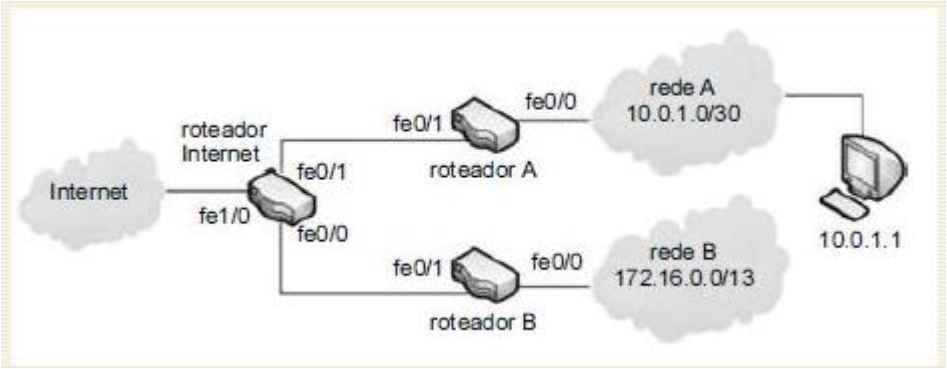


[96] O acesso à Internet, com base na configuração apresentada na figura, não requer o uso de um serviço de NAT (network address translation).

5. A partir da figura acima, julgue os itens a seguir, acerca de conexões e componentes de rede.

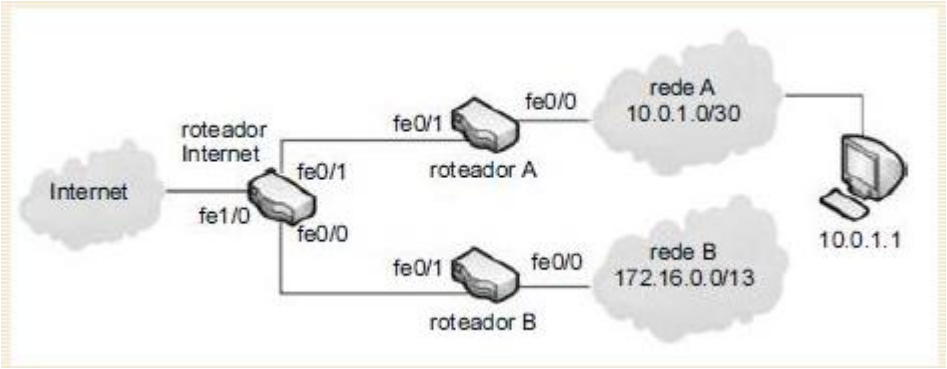


~~[96] O acesso à Internet, com base na configuração apresentada na figura, não requer o uso de um serviço de NAT (network address translation).~~



6. Considerando o esquema de rede apresentado na figura acima, julgue os itens a seguir.

[98] A interface fe1/0 deve possuir um IP privado e implementar NAT.



6. Considerando o esquema de rede apresentado na figura acima, julgue os itens a seguir.

~~[98] A interface fe1/0 deve possuir um IP privado e implementar NAT.~~

7. Julgue os itens, referentes a redes de computadores

[37] No endereçamento IPv4 em redes TCP/IP, as redes que empregam a numeração 10.0.0.0 podem usar um serviço de tradução de endereços (NAT) para que suas máquinas possam acessar a Internet. Definindo-se máscaras apropriadas, uma rede pode ser dividida em sub-redes e as sub-redes, por sua vez, podem ser divididas em outras sub-redes. Endereços na classe D visam possibilitar que datagramas sejam enviados para grupos de máquinas.

7. Julgue os itens, referentes a redes de computadores

~~[37] No endereçamento IPv4 em redes TCP/IP, as redes que empregam a numeração 10.0.0.0 podem usar um serviço de tradução de endereços (NAT) para que suas máquinas possam acessar a Internet. Definindo-se máscaras apropriadas, uma rede pode ser dividida em sub-redes e as sub-redes, por sua vez, podem ser divididas em outras sub-redes. Endereços na classe D visam possibilitar que datagramas sejam enviados para grupos de máquinas.~~

8. Um dos conceitos fundamentais para a formação de redes ligadas à Internet com uso de endereçamento IP pertencente ao bloco privativo, conforme especificado na RFC 1918, é a técnica de tradução de endereços de rede NAT (Network Address Translation). Com referência à NAT e aos cuidados e limitações que representam o seu uso, julgue os itens seguintes.

- Uma rede com endereços IP privativos, conectada à Internet por meio de um sistema proxy de rede usando NAT, possui a mesma conectividade com a Internet de uma rede que esteja diretamente ligada à Internet e que utilize endereços IP verdadeiros.
- Não há rotas na Internet para os endereços reservados a Internets privativas (bloco privativo). Portanto, um roteador que opere de acordo com as especificações usuais do protocolo IP deve rejeitar a inserção estática ou o manual de uma rota para um endereço IP pertencente a esse conjunto de endereços.
- NAT consiste essencialmente de uma técnica de mapeamento de vários endereços privados em um ou mais endereços verdadeiros. Para tanto, deve ser realizado o mapeamento de pacotes que saem da rede privativa para a Internet usando-se números de portas TCP e UDP como elo de ligação com os pacotes de resposta que entram na rede privativa.
- NAT não permite, em geral, o estabelecimento de conexões TCP da Internet para a rede privativa, a não ser em casos especiais que devem ser tratados separadamente do mecanismo convencional de realização do mapeamento de endereços.
- NAT está associado a sistemas firewall por possibilitar, por definição, a criação de listas de acesso.

8. Um dos conceitos fundamentais para a formação de redes ligadas à Internet com uso de endereçamento IP pertencente ao bloco privativo, conforme especificado na RFC 1918, é a técnica de tradução de endereços de rede NAT (Network Address Translation). Com referência à NAT e aos cuidados e limitações que representam o seu uso, julgue os itens seguintes.

- ~~Uma rede com endereços IP privativos, conectada à Internet por meio de um sistema proxy de rede usando NAT, possui a mesma conectividade com a Internet de uma rede que esteja diretamente ligada à Internet e que utilize endereços IP verdadeiros.~~
- ~~Não há rotas na Internet para os endereços reservados a Internets privativas (bloco privativo). Portanto, um roteador que opere de acordo com as especificações usuais do protocolo IP deve rejeitar a inserção estática ou o manual de uma rota para um endereço IP pertencente a esse conjunto de endereços.~~
- NAT consiste essencialmente de uma técnica de mapeamento de vários endereços privados em um ou mais endereços verdadeiros. Para tanto, deve ser realizado o mapeamento de pacotes que saem da rede privativa para a Internet usando-se números de portas TCP e UDP como elo de ligação com os pacotes de resposta que entram na rede privativa.
- NAT não permite, em geral, o estabelecimento de conexões TCP da Internet para a rede privativa, a não ser em casos especiais que devem ser tratados separadamente do mecanismo convencional de realização do mapeamento de endereços.
- ~~NAT está associado a sistemas firewall por possibilitar, por definição, a criação de listas de acesso.~~

GABARITO

1. C
2. C, E, E
3. C, C, C
4. C
5. E
6. E
7. C
8. E, E, C, C, E