Exame simulado

Edição 201701

Conteúdo

Introdução	4
Exame simulado	5
Gabarito de respostas	14
Avaliação	28

Introdução

Este é o modelo de exame de EXIN Ethical Hacking Foundation (EHF.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame consiste de 40 questões de múltipla escolha. Cada questão de múltipla escolha possui um certo número de alternativas de resposta, entre as quais apenas uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale um ponto. Para passar você deve obter 26 pontos ou mais.

O tempo permitido para este exame é de 60 minutos.

Boa sorte!

Exame simulado

1 / 40
Qual é a meta principal de um Hacker Ético?

A) Evitar a detecção
B) Determinar o retorno sobre o investimento (ROI) das medidas de segurança
C) Resolver vulnerabilidades de segurança
D) Testar controles de segurança

2 / 40
Quais são exemplos de sniffers de redes?

A) Bash, Nano, VI
B) Nmap, Metasploit, Nessus
C) Wireshark, Tshark, TCPdump

3 / 40
Um hacker ético é contratado por uma organização para obter acesso remoto à sua rede interna. Ele não recebeu nenhuma informação sobre a rede interna da organização.

Que tipo de teste está sendo realizado?

A) testes black box
B) testes grey box
C) testes white box

4 / 40
Qual é a função do shell R57?

A) Implementação de uma versão baseada na web do Metasploit
B) Visualização e transferência de arquivos
C) Visualização das webcams de visitantes para o site

5 / 40
Cristina adicionou um apóstrofo após um parâmetro ?id= na URL de uma página da web. Agora, ela vê um erro, informando que houve um erro de sintaxe.

O que Cristina encontrou?

A) Uma vulnerabilidade de Cross-Site Scripting
B) Uma exploração de banco de dados PostgreSQL
C) Uma injeção SQL

6 / 40
Um site usa um conteúdo gerado dinamicamente. Recorrendo a uma técnica específica, é possível roubar as credenciais de login do usuário.

Qual técnica é abordada aqui?

A) Sequestro de sessão
B) Injeção SQL
C) Cross Site Scripting (XSS)

7 / 40
O que pode ser utilizado para criar uma conexão entre sua máquina e o site no qual seu shell R57 está sendo executado?

A) Função de avaliação
B) Shell de conexão retroativa
C) Comando Incluir

8 / 40
No Meterpreter, você encontrou um arquivo interessante chamado passwords.xls. Você deseja recuperar esse arquivo dentro do Meterpreter, mas não tem certeza sobre como fazer isso.

O que você deve usar?

A) O comando 'download' dentro do Meterpreter
B) O VNC, pois é o caminho mais rápido para copiar dados
C) Não é possível fazer o download de arquivos a partir do shell Meterpreter

9 / 40
Você encontrou um sistema ativo no endereço IP 192.168.10.113.

Qual comando nmap permite detectar o sistema operacional deste alvo?

A) `nmap -O 192.168.10.113`
B) `nmap -Os 192.168.10.113`
C) `nmap -os 192.168.10.113`

10 / 40
Uma varredura de serviço, incluindo impressão digital, mostrou que uma máquina de destino está executando o Apache 2.2.14.

Qual poderia ser o passo seguinte para verificar se esse serviço é vulnerável?

A) Verificar recursos on-line, como o Exploit-DB, OSVDB para vulnerabilidades conhecidas.
B) Use o Kismet para determinar o nível de configuração e correção do Apache.
C) Use o netcat para obter acesso à máquina por meio deste serviço.

11 / 40
Você conhece os nomes de uma tabela e colunas de um banco de dados. Você precisa utilizar Injeção de SQL para recuperar mais informações.

O que você deve usar?

A) UNION GET
B) UNION SELECT
C) UNION CONCAT

12 / 40
Um hacker está tentando captar o tráfego a partir de seu adaptador de rede sem fio.

O que o adaptador de rede dele deve procurar no Wireshark?

A) eth0
B) l0
C) wlan0

13 / 40
Antes de iniciar o penetration test em um cliente, o penetration tester deve estar sempre preparado para qualquer questão jurídica.

O que ele deve fazer para evitar a responsabilidade legal?

A) Verificar, no ambiente do cliente, se há alguma vulnerabilidade que possa causar problemas antes do penetration test.
B) Assinar um contrato com o cliente antes de executar o penetration test.
C) Conversar com o cliente antes do teste e assegurar-se de que é necessário que o teste seja um teste black box, grey box ou white box.

14 / 40
Em que ponto do processo de Hackeamento Ético é mais provável que o invasor utilize uma ferramenta de varredura de portas?

A) Execução do ataque
B) Preparação do ataque
C) Coleta de informações
D) Elaboração de um relatório

15 / 40
Para que serve um c99shell?

A) É uma ferramenta de linha de comandos que permite conexões remotas a um servidor de banco de dados.
B) É um backdoor PHP que permite upload, exclusão e execução de arquivos.
C) É um malware utilizado para provocar falhas em servidores que executam o Microsoft Windows Server 2008 R2.

16 / 40
Uma hacker conseguiu seguir parcialmente o processo de cracking de uma chave WEP. Ela criou um pacote ARP que agora deve ser injetado em direção ao access point.

Qual aplicativo ela deve usar para injetar o pacote ARP?

A) airbase-ng
B) aireplay-ng
C) wesside-ng

17 / 40
Um pentetration tester deseja saber quais endereços IP estão ativos na rede no momento. Ele usa o nmap para fazer isso.

Qual opção nmap ele precisa para realizar esse teste?

A) -sU
B) -sO
C) -sP

18 / 40
Um cliente afirmou haver criado um filtro que diferenciava maiúsculas de minúsculas para o 'script' o qual era inserido de todas as formas para evitar um PoC de XSS.

Como você pode evitar isso?

A) `<sCrIPt>alert(1);</ScRiPT>`
B) `<javascript>alert(1);</script>`
C) `<img src=x onerror=alert(1)>`

19 / 40
Uma hacker conseguiu encontrar uma vulnerabilidade de XSS. Agora, ela quer assumir o controle das sessões.

Em qual opção ela conseguirá obter a informação desejada?

A) document.session
B) session.cookie
C) document.cookie

20 / 40
Ao criar uma PoC de XSS, qual é a função que fornece uma janela pop-up?

A) `popup()`
B) `alert()`
C) `window.popup()`

21 / 40
Uma Ethical Haker é convidada para fazer a varredura de uma máquina, mas só é autorizada a verificar se as portas TCP/IP 21, 22, 80 e 443 estão abertas.

O que ela deve fazer?

A) `nmap -vv -A -p 21,22,80,https <target>`
B) `nmap -vv -p 21,22,80,443 <target>`
C) `nmap -sV ftp, ssh, http, https <target>`

22 / 40
A URL do site contém 'index.php?page=home.php'. O parâmetro da página permite que URLs remotas sejam aprovadas e ele as carrega.

Qual seria um exemplo disso?

A) Inclusão de Arquivos Remotos
B) Injeção de Arquivos Remotos
C) Representação de Arquivos Remotos

23 / 40
Alguém violou um site e conseguiu manter isso em segredo. O hackeamento não fazia parte da tarefa e não havia autorização para isso.

Que nome damos a esse indivíduo?

A) Hacker black hat
B) Hacktivista
C) ScriptKiddie
D) Hacker white hat

24 / 40
Você está realizando um teste de invasão e é convidado a testar a força de autenticação de um dispositivo de armazenamento. Você não recebeu o endereço IP do host, mas lhe disseram que o sistema envia uma mensagem de broadcast a cada cinco minutos.

O que você poderia usar para encontrar o endereço IP do host?

A) Ncrack
B) Netdiscover
C) Wireshark

25 / 40
Um Hacker Ético é solicitado a executar um teste de invasão para um cliente, e tudo o que recebeu foi uma URL.

Que tipo de teste é esse?

A) Teste de invasão black box
B) Teste de hackeamento black hat
C) Teste de invasão white box

26 / 40
Os penetration testers usam shells para se comunicar e encontrar vulnerabilidades em sistemas. Um tipo de shells são os assim chamados 'shells bind'. Em determinados cenários, são ineficazes.

Por quê isso ocorre?

A) O firewall bloqueará qualquer tráfego em uma porta na qual o bind shell tentar se comunicar.
B) O Windows 7 e superior não pode mais executar comandos shell se o usuário não for um administrador.
C) Os bind shells somente são executados em sistemas operacionais baseados em terminais.

27 / 40
Um penetration tester está testando um aplicativo da web. Para verificar se há vulnerabilidades, ele decide verificar se injeções SQL são possíveis.

Qual caractere normalmente é utilizado pelo penetration tester?

A) Sinal de cifrão
B) Ponto e vírgula
C) Aspa simples

28 / 40
Você não tem certeza do endereço MAC de sua rede Wi-Fi.

Após ser orientado a usar o Airodump-NG, qual rede você deve procurar?

A) BSSID
B) ESSID
C) SSID

29 / 40
Você está tentando descobrir qual de seus adaptadores de rede conectados suporta Wi-Fi.

Qual comando você deve usar na janela do terminal?

A) `iwconfig`
B) `wificards`
C) `wireshark`

30 / 40
O que é ESSID?

A) O endereço MAC de um cliente conectado
B) O endereço MAC de um access point do destino
C) Nome da rede

31 / 40
Um testador está realizando um teste de invasão em um servidor web. Ela começa o teste com um ataque de obtenção de banners. Ela já verificou que o servidor web está executando uma versão do Linux. No entanto, o banner HTTP relata que ele está executando a versão 8 do IIS.

Que tipo de defesa o administrador do servidor web está usando?

A) Redirecionamento de pastas
B) Ofuscação de portas
C) Redirecionamento do processo
D) Forjamento de serviço

32 / 40
Você salvou a saída de uma varredura Nmap no formato XML.

O que você deve usar para importar os resultados da varredura dentro do Metasploit?

A) `db_import`
B) `nmap_import`
C) `scan_import`

33 / 40
O Metasploit usa diversos módulos para testar se há vulnerabilidades. Um desses módulos permite que o penetration tester use explorações automatizadas do navegador.

Qual é o nome desse módulo utilizado no Metasploit?

A) browser_exploiter
B) browser_autopwn
C) metasploit_autopwn

34 / 40
Um hacker ético está tentando invadir um site por meio de uma Injeção SQL. Ele também alterou o cabeçalho HTTP do User-Agent, enviado por seu navegador.

O que ele pode conseguir com essa ação?

A) Ele adquire uma conexão SSL correspondente.
B) Ele obtém o melhor desempenho do site para que ele responda mais rapidamente a suas solicitações.
C) Ele impede que a perícia revele seu navegador real que foi utilizado durante o ataque.

35 / 40
Um administrador de rede percebeu um pouco de tráfego suspeito na rede da empresa. Ele decide investigar. Após realizar o ping com sucesso na origem do tráfego, ele usa um utilitário para encontrar o endereço MAC associado.

Qual utilitário ele usa?

A) ARP
B) DNSSpoof
C) PSExec

36 / 40
No Metasploit Framework (msf) é possível usar vários exploits. Depois de selecionar um exploit para usar contra uma vítima, em alguns casos, é obrigatório selecionar um alvo.

Um pentester selecionou e iniciou um exploit. A seguinte mensagem de erro é mostrada no terminal: "Exploit falhou: um destino não foi selecionado"

Como isso pode ser corrigido?

A) Configurando a variável RHOST para fornecer um endereço de destino
B) Verificando os destinos disponíveis digitando `'show targets'` e, então, selecionando um destino digitando `'set TARGET x'`
C) Digitando `'check'` se o destino estiver vulnerável

37 / 40
Quando se observam os arquivos de log no servidor web, Pete quer saber qual navegador foi utilizado durante o ataque contra o site dele. Pete deve procurar informações que geralmente são enviadas por meio do cabeçalho <answer>.

Qual cabeçalho `<answer>` está relacionado com isso?

A) Aceitar-Idioma:
B) Host:
C) User-Agent:

38 / 40
Uma empresa sofreu um ataque de DDoS. Eles têm o endereço IP do invasor e desejam entrar em contato com seu Provedor de Serviços de Internet para denunciar um abuso.

O que eles devem fazer?

A) Pesquisa de DNS
B) Pesquisa de localização por GeoIP
C) Pesquisa WHOIS

39 / 40

Um penetration tester está realizando uma varredura no ambiente de rede de seu cliente com uma ferramenta. Essa ferramenta tem as seguintes propriedades:

- Ela usa uma classificação para mostrar o impacto de uma vulnerabilidade.
- Ela detecta todos os tipos de vulnerabilidades em vários sistemas operacionais como Windows, Linux e Mac OS.
- Ela é capaz de detectar bots, cavalos de troia e outros malwares que podem ser instalados em computadores conectados à rede.

Qual é o nome da ferramenta que o penetration tester está usando?

A) nessus
B) nmap
C) nikto

40 / 40

Qual é o nome dos módulos do Metasploit que **não** são utilizados para fins de exploração?

A) auxiliares
B) payloads
C) shellcodes

Gabarito de respostas

1 / 40
Qual é a meta principal de um Hacker Ético?

A) Evitar a detecção
B) Determinar o retorno sobre o investimento (ROI) das medidas de segurança
C) Resolver vulnerabilidades de segurança
D) Testar controles de segurança

A) Incorreto. Evitar a detecção faz parte do Hackeamento Ético, mas não da meta principal.
B) Incorreto. O cálculo do ROI faz parte da seleção de controle e da mitigação de riscos.
C) Incorreto. O Hackeamento Ético significa encontrar e documentar vulnerabilidades, mas não resolvê-las.
D) Correto. A função principal dos Hackers Éticos é testar a segurança.

2 / 40
Quais são exemplos de sniffers de redes?

A) Bash, Nano, VI
B) Nmap, Metasploit, Nessus
C) Wireshark, Tshark, TCPdump

A) Incorreto. Estas são ferramentas Linux/UNIX de edição de textos
B) Incorreto. Estas são ferramentas de exploração integradas (Metasploit, Nessus) e ferramenta de varredura (Nmap).
C) Correto. Estas são ferramentas de sniffing (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 7.)

3 / 40
Um hacker ético é contratado por uma organização para obter acesso remoto à sua rede interna. Ele não recebeu nenhuma informação sobre a rede interna da organização.

Que tipo de teste está sendo realizado?

A) testes black box
B) testes grey box
C) testes white box

A) Correto. O hacker ético não sabe nada sobre a rede interna. Ele simula ser um hacker black hat (chapéu preto), trabalhando de fora da empresa.
B) Incorreto. Nesse caso, o hacker ético recebe o mínimo de informações.
C) Incorreto. Em um teste white box, todas as informações relevantes sobre o sistema/rede estão disponíveis para o hacker.

4 / 40
Qual é a função do shell R57?

A) Implementação de uma versão baseada na web do Metasploit
B) Visualização e transferência de arquivos
C) Visualização das webcams de visitantes para o site

A) Incorreto. Não existe uma versão baseada na Web do Metasploit que você pode usar out-of-the-box. Metasploit é uma estrutura que faz uso de banco de dados para a exploração da vulnerabilidade.
B) Correto. Isto é uma função do Shell R57.
C) Incorreto. Isto não é possível com o Shell R57. Isto pode ser feito com uma ferramenta em combinação com Metasploit.

5 / 40
Cristina adicionou um apóstrofo após um parâmetro ?id= na URL de uma página da web. Agora, ela vê um erro, informando que houve um erro de sintaxe.

O que Cristina encontrou?

A) Uma vulnerabilidade de Cross-Site Scripting
B) Uma exploração de banco de dados PostgreSQL
C) Uma injeção SQL

A) Incorreto. Usar um apóstrofo [’] para fechar a consulta de SQL fará com que o aplicativo apresente um erro de sintaxe de SQL (se houver uma vulnerabilidade de SQLi).
B) Incorreto. Usar um apóstrofo [’] para fechar a consulta de SQL fará com que o aplicativo apresente um erro de sintaxe de SQL (se houver uma vulnerabilidade de SQLi).
C) Correto. Usar um apóstrofo [’] para fechar a consulta de SQL fará com que o aplicativo apresente um erro de sintaxe de SQL (se houver uma vulnerabilidade de SQLi).

6 / 40
Um site usa um conteúdo gerado dinamicamente. Recorrendo a uma técnica específica, é possível roubar as credenciais de login do usuário.

Qual técnica é abordada aqui?

A) Sequestro de sessão
B) Injeção SQL
C) Cross Site Scripting (XSS)

A) Incorreto. O sequestro de sessão é algo que o hacker pode tentar depois de usar o XSS.
B) Incorreto. A injeção SQL está criando novas consultas e tentando obter informações particulares do banco de dados.
C) Correto. O código XSS permite introduzir o código javascript em um site sem que o usuário perceba. O código pode mostrar uma janela de login falsa que envia as credenciais ao hacker. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 14, Paragraph Cross-Site Scripting.)

7 / 40
O que pode ser utilizado para criar uma conexão entre sua máquina e o site no qual seu shell R57 está sendo executado?

A) Função de avaliação
B) Shell de conexão retroativa
C) Comando Incluir

A) Incorreto. A função eval não tem nada a ver com o shell R57. Isso não solicita nada.
B) Correto. O R57 também é chamado de “Shell de conexão retroativa”. É utilizado para enviar malwares, spam, etc.
C) Incorreto. O R57 também é chamado de “Shell de conexão retroativa”. É utilizado para enviar malwares, spam, etc.

8 / 40
No Meterpreter, você encontrou um arquivo interessante chamado passwords.xls. Você deseja recuperar esse arquivo dentro do Meterpreter, mas não tem certeza sobre como fazer isso.

O que você deve usar?

A) O comando 'download' dentro do Meterpreter
B) O VNC, pois é o caminho mais rápido para copiar dados
C) Não é possível fazer o download de arquivos a partir do shell Meterpreter

A) Correto. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 13.)
B) Incorreto. O VNC é utilizado para se conectar a um PC remoto e compartilhar uma tela, por exemplo.
C) Incorreto. O hacker pode se conectar a um computador remoto e fazer download de arquivos.

9 / 40
Você encontrou um sistema ativo no endereço IP 192.168.10.113.

Qual comando nmap permite detectar o sistema operacional deste alvo?

A) `nmap -O 192.168.10.113`
B) `nmap -Os 192.168.10.113`
C) `nmap -os 192.168.10.113`

A) Correto. O -O tenta obter as informações sobre o sistema operacional utilizado. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 5.)
B) Incorreto. O -Os não é nem mesmo um parâmetro para o nmap.
C) Incorreto. O -os não é nem mesmo um parâmetro para o nmap.

10 / 40
Uma varredura de serviço, incluindo impressão digital, mostrou que uma máquina de destino está executando o Apache 2.2.14.

Qual poderia ser o passo seguinte para verificar se esse serviço é vulnerável?

A) Verificar recursos on-line, como o Exploit-DB, OSVDB para vulnerabilidades conhecidas.
B) Use o Kismet para determinar o nível de configuração e correção do Apache.
C) Use o netcat para obter acesso à máquina por meio deste serviço.

A) Correto. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 6, Paragraph Nessus, Subparagraph Researching Vulnerabilities and Paragraph Web Application Scanning.)
B) Incorreto. O Kismet é uma ferramenta de vulnerabilidade de wi-fi.
C) Incorreto. O Netcat não é uma ferramenta para verificar vulnerabilidades.

11 / 40
Você conhece os nomes de uma tabela e colunas de um banco de dados. Você precisa utilizar Injeção de SQL para recuperar mais informações.

O que você deve usar?

A) UNION GET
B) UNION SELECT
C) UNION CONCAT

A) Incorreto. O operador SQL UNION combina o resultado de duas ou mais instruções SELECT.
B) Correto. O operador SQL UNION combina o resultado de duas ou mais instruções SELECT.
C) Incorreto. A função CONCAT é utilizada para concatenar duas sequências de caracteres para formar uma única sequência (quando temos apenas um campo para receber os dados).

12 / 40
Um hacker está tentando captar o tráfego a partir de seu adaptador de rede sem fio.

O que o adaptador de rede dele deve procurar no Wireshark?

A) eth0
B) l0
C) wlan0

A) Incorreto. eth0 é sempre um adaptador de Ethernet com fio. wlan0 é a única opção de adaptador sem fio.
B) Incorreto. wlan0 é a única opção de adaptador sem fio.
C) Correto. wlan0 é a única opção de adaptador sem fio (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 7).

13 / 40
Antes de iniciar o penetration test em um cliente, o penetration tester deve estar sempre preparado para qualquer questão jurídica.

O que ele deve fazer para evitar a responsabilidade legal?

A) Verificar, no ambiente do cliente, se há alguma vulnerabilidade que possa causar problemas antes do penetration test.
B) Assinar um contrato com o cliente antes de executar o penetration test.
C) Conversar com o cliente antes do teste e assegurar-se de que é necessário que o teste seja um teste black box, grey box ou white box.

A) Incorreto. A análise do ambiente do cliente ocorre após a assinatura de todos os documentos legais, como, por exemplo, o Acordo de Não Divulgação (NDA). Usar ferramentas de hackeamento não torna isso legal ou não.
B) Correto. Assinar um contrato. Dessa forma, ambas as partes (o ethical hacker e o cliente) sabem o que esperar um do outro. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 0.)
C) Incorreto. Embora seja necessário fazer isso, nada tem a ver com questões jurídicas.

14 / 40
Em que ponto do processo de Hackeamento Ético é mais provável que o invasor utilize uma ferramenta de varredura de portas?

A) Execução do ataque
B) Preparação do ataque
C) Coleta de informações
D) Elaboração de um relatório

A) Incorreto. Este é o ataque real. A varredura de portas é a coleta de informações.
B) Incorreto. Esta fase usa as informações da varredura de portas para selecionar os alvos.
C) Correto. A varredura de portas faz parte do reconhecimento ativo e da varredura.
D) Incorreto. Este é o resumo dos resultados. A varredura de portas está coletando dados que alimentam o relatório.

15 / 40
Para que serve um c99shell?

A) É uma ferramenta de linha de comandos que permite conexões remotas a um servidor de banco de dados.
B) É um backdoor PHP que permite upload, exclusão e execução de arquivos.
C) É um malware utilizado para provocar falhas em servidores que executam o Microsoft Windows Server 2008 R2.

A) Incorreto. Não é utilizado para conexões remotas a um servidor de banco de dados.
B) Correto. É um shell backdoor que pode ser carregado via upload para um site com o objetivo de obter acesso aos arquivos armazenados nesse site. Após o upload, o hacker pode usá-lo para editar, excluir ou fazer download de quaisquer arquivos no site ou fazer upload de arquivos.
C) Incorreto. O c99shell pode ser classificado como um malware, mas definitivamente não é.

16 / 40
Uma hacker conseguiu seguir parcialmente o processo de cracking de uma chave WEP. Ela criou um pacote ARP que agora deve ser injetado em direção ao access point.

Qual aplicativo ela deve usar para injetar o pacote ARP?

A) airbase-ng
B) aireplay-ng
C) wesside-ng

A) Incorreto. Airbase é uma ferramenta de múltiplas finalidades para atacar clientes.
B) Correto. Aireplay injetará pacotes captados ou criados em uma rede sem fio.
C) Incorreto. wesside é uma ferramenta de cracking de WEP, mas não injeta pacotes captados.

17 / 40
Um pentetration tester deseja saber quais endereços IP estão ativos na rede no momento. Ele usa o nmap para fazer isso.

Qual opção nmap ele precisa para realizar esse teste?

A) -sU
B) -sO
C) -sP

A) Incorreto. O -sU é utilizado para fazer a varredura de UDP.
B) Incorreto. O -sO tenta determinar quais protocolos IP (TCP, UDP, ICMP) são suportados por um sistema.
C) Correto. O -sP verifica os endereços IP ativos na rede. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 5.)

18 / 40
Um cliente afirmou haver criado um filtro que diferenciava maiúsculas de minúsculas para o 'script' o qual era inserido de todas as formas para evitar um PoC de XSS.

Como você pode evitar isso?

A) `<sCrIPt>alert(1);</ScRiPT>`
B) `<javascript>alert(1);</script>`
C) `<img src=x onerror=alert(1)>`

A) Incorreto. Este script não será executado porque o formulário do cliente realiza verificações em scripts que diferenciam entre maiúsculas e minúsculas.
B) Incorreto. Isto não será executado porque o script não pode ser executado no formulário.
C) Correto. Isso será executado. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 14.)

19 / 40
Uma hacker conseguiu encontrar uma vulnerabilidade de XSS. Agora, ela quer assumir o controle das sessões.

Em qual opção ela conseguirá obter a informação desejada?

A) document.session
B) session.cookie
C) document.cookie

A) Incorreto. O document.cookie é o único lugar onde uma sessão é armazenada.
B) Incorreto. O document.cookie é o único lugar onde uma sessão é armazenada.
C) Correto. O document.cookie é o único lugar onde uma sessão é armazenada.

20 / 40
Ao criar uma PoC de XSS, qual é a função que fornece uma janela pop-up?

A) `popup()`
B) `alert()`
C) `window.popup()`

A) Incorreto. Pop-up () não é um método javascript correto.
B) Correto. alert() disparará o evento de alerta que gerará uma janela pop-up.
C) Incorreto. Isso não fará nada.

21 / 40
Uma Ethical Haker é convidada para fazer a varredura de uma máquina, mas só é autorizada a verificar se as portas TCP/IP 21, 22, 80 e 443 estão abertas.

O que ela deve fazer?

A) `nmap -vv -A -p 21,22,80,https <target>`
B) `nmap -vv -p 21,22,80,443 <target>`
C) `nmap -sV ftp, ssh, http, https <target>`

A) Incorreto. Não é possível fazer a varredura de um tipo específico, como https ou ssh. O testador precisará saber quais portas são utilizadas.
B) Correto. Verificando as portas, é possível ver quais serviços (https, ssh, etc.) estão em execução.
C) Incorreto. Não é possível fazer a varredura de um tipo específico, como https ou ssh. O testador precisará saber quais portas são utilizadas.

22 / 40
A URL do site contém 'index.php?page=home.php'. O parâmetro da página permite que URLs remotas sejam aprovadas e ele as carrega.

Qual seria um exemplo disso?

A) Inclusão de Arquivos Remotos
B) Injeção de Arquivos Remotos
C) Representação de Arquivos Remotos

A) Correto. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 14, Paragraph Remote File Inclusion.)
B) Incorreto. Este não é o termo correto.
C) Incorreto. Este não é o termo correto.

23 / 40
Alguém violou um site e conseguiu manter isso em segredo. O hackeamento não fazia parte da tarefa e não havia autorização para isso.

Que nome damos a esse indivíduo?

A) Hacker black hat
B) Hacktivista
C) ScriptKiddie
D) Hacker white hat

A) Correto. Alguém que realiza hackeamento sem permissão é chamado de hacker black hat (chapéu preto).
B) Incorreto. Tipo de hacker válido, mas não coincide com a descrição.
C) Incorreto. Tipo de hacker válido, mas não coincide com a descrição.
D) Incorreto. Tipo de hacker válido, mas não coincide com a descrição.

24 / 40
Você está realizando um teste de invasão e é convidado a testar a força de autenticação de um dispositivo de armazenamento. Você não recebeu o endereço IP do host, mas lhe disseram que o sistema envia uma mensagem de broadcast a cada cinco minutos.

O que você poderia usar para encontrar o endereço IP do host?

A) Ncrack
B) Netdiscover
C) Wireshark

A) Incorreto. O Ncrack é uma ferramenta de craqueamento de autenticação de redes de alta velocidade.
B) Incorreto. O Netdiscover é uma ferramenta de reconhecimento de endereços ativos/passivos, desenvolvida principalmente para redes sem fio sem o servidor dhcp, quando você está realizando wardriving.
C) Correto. O Wireshark pode ser utilizado para descobrir o endereço IP.

25 / 40
Um Hacker Ético é solicitado a executar um teste de invasão para um cliente, e tudo o que recebeu foi uma URL.

Que tipo de teste é esse?

A) Teste de invasão black box
B) Teste de hackeamento black hat
C) Teste de invasão white box

A) Correto. São fornecidas informações mínimas ao testador de invasão durante um teste black box.
B) Incorreto. Um black hat é um tipo de hacker, e não um tipo de teste.
C) Incorreto. Detalhes moderados a avançados são fornecidos ao testador de invasão durante um teste white box.

26 / 40
Os penetration testers usam shells para se comunicar e encontrar vulnerabilidades em sistemas. Um tipo de shells são os assim chamados 'shells bind'. Em determinados cenários, são ineficazes.

Por quê isso ocorre?

A) O firewall bloqueará qualquer tráfego em uma porta na qual o bind shell tentar se comunicar.
B) O Windows 7 e superior não pode mais executar comandos shell se o usuário não for um administrador.
C) Os bind shells somente são executados em sistemas operacionais baseados em terminais.

A) Correto. Um bind shell orienta a máquina selecionada como alvo a abrir um shell de comando e a rastrear uma porta local. A máquina selecionada para o ataque conecta-se, então, à máquina selecionada como alvo na porta de rastreamento. Entretanto, com o advento dos firewalls, a eficácia dos shells bind foi reduzida, pois qualquer firewall configurado corretamente bloqueará o tráfego para uma porta aleatória como 4444. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 4, Paragraph Types of shells.)
B) Incorreto. Bind shells nada têm a ver com o usuário ser administrador.
C) Incorreto. Bind shells nada têm a ver com o usuário ser administrador.

27 / 40
Um penetration tester está testando um aplicativo da web. Para verificar se há vulnerabilidades, ele decide verificar se injeções SQL são possíveis.

Qual caractere normalmente é utilizado pelo penetration tester?

A) Sinal de cifrão
B) Ponto e vírgula
C) Aspa simples

A) Incorreto. Este não é o caractere a ser utilizado.
B) Incorreto. Em geral, este é o último caractere a ser utilizado.
C) Correto. Um teste típico de vulnerabilidades de injeção SQL é usar a aspa simples para encerra a consulta SQL. Se houver vulnerabilidade na injeção SQL, adicionar a aspa simples deve fazer o aplicativo gerar um erro de SQL, pois a consulta já estará encerrada como parte do código subjacente, e a aspa simples adicional tornará a sintaxe de SQL incorreta. Esse erro indica que podemos injetar consultas SQL no banco de dados do site usando o parâmetro testado. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 14, Paragraph Testing for SQL Injection Vulnerabilities.)

28 / 40
Você não tem certeza do endereço MAC de sua rede Wi-Fi.

Após ser orientado a usar o Airodump-NG, qual rede você deve procurar?

A) BSSID
B) ESSID
C) SSID

A) Correto. O BSSID é o equivalente sem fio a um endereço MAC (Lit. Penetration Testing, A Hands-On Introduction to Hacking.)
B) Incorreto. O ESSID é o nome de rede de difusão amigável, e não o endereço MAC.
C) Incorreto. Isto é semelhante ao ESSID e não ao endereço MAC.

29 / 40
Você está tentando descobrir qual de seus adaptadores de rede conectados suporta Wi-Fi.

Qual comando você deve usar na janela do terminal?

A) `iwconfig`
B) `wificards`
C) `wireshark`

A) Correto. iwconfig exibe a configuração de todos os adaptadores sem fio conectados.
B) Incorreto. Isto não é um comando.
C) Incorreto. Wireshark não será executado em uma janela de terminal (Lit. Penetration Testing, A Hands-On Introduction to Hacking.)

30 / 40
O que é ESSID?

A) O endereço MAC de um cliente conectado
B) O endereço MAC de um access point do destino
C) Nome da rede

A) Incorreto. ESSID é baseado em AP, e não no cliente.
B) Incorreto. BSSID é o endereço MAC de um access point.
C) Correto. ESSID é o nome amigável de um AP (Lit. Penetration Testing, A Hands-On Introduction to Hacking).

31 / 40
Um testador está realizando um teste de invasão em um servidor web. Ela começa o teste com um ataque de obtenção de banners. Ela já verificou que o servidor web está executando uma versão do Linux. No entanto, o banner HTTP relata que ele está executando a versão 8 do IIS.

Que tipo de defesa o administrador do servidor web está usando?

A) Redirecionamento de pastas
B) Ofuscação de portas
C) Redirecionamento do processo
D) Forjamento de serviço

A) Incorreto. O redirecionamento de pastas não tem nada a ver com os servidores web.
B) Incorreto. Não houve nenhuma modificação das portas na explicação da pergunta, e a ofuscação de portas não teria nenhum efeito sobre o banner ou a versão do sistema operacional.
C) Incorreto. Redirecionamento de processo não existe. O redirecionamento de palavras pode atrair candidatos não qualificados, o que é uma ótima distração.
D) Correto. O IIS não pode ser executado em Linux, e a Avril já verificou que o Linux é o sistema operacional. Então, o banner é falso.

32 / 40
Você salvou a saída de uma varredura Nmap no formato XML.

O que você deve usar para importar os resultados da varredura dentro do Metasploit?

A) `db_import`
B) `nmap_import`
C) `scan_import`

A) Correto. O comando 'db_import' é utilizado para importar os resultados da varredura no banco de dados do Metasploit.
B) Incorreto. O comando 'nmap_import' é utilizado para executar um Nmap contra as metas, e os resultados da varredura seriam, então, armazenados automaticamente no banco de dados.
C) Incorreto. O comando 'db_import' é utilizado para importar os resultados da varredura no banco de dados do Metasploit.

33 / 40
O Metasploit usa diversos módulos para testar se há vulnerabilidades. Um desses módulos permite que o penetration tester use explorações automatizadas do navegador.

Qual é o nome desse módulo utilizado no Metasploit?

A) browser_exploiter
B) browser_autopwn
C) metasploit_autopwn

A) Incorreto. Não está no metasploit.
B) Correto. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 10.)
C) Incorreto. O metasploit_autopwn geralmente é às vezes confundido com o browser_autopwn, mas o metasploit_autopwn é um módulo diferente que tenta explorar portas abertas nos sistemas.

34 / 40
Um hacker ético está tentando invadir um site por meio de uma Injeção SQL. Ele também alterou o cabeçalho HTTP do User-Agent, enviado por seu navegador.

O que ele pode conseguir com essa ação?

A) Ele adquire uma conexão SSL correspondente.
B) Ele obtém o melhor desempenho do site para que ele responda mais rapidamente a suas solicitações.
C) Ele impede que a perícia revele seu navegador real que foi utilizado durante o ataque.

A) Incorreto. O cabeçalho HTTP não tem nenhuma relação com as conexões SSL.
B) Incorreto. O desempenho não tem nada a ver com os cabeçalhos HTTP.
C) Correto. Alterar o cabeçalho HTTP muda as informações registradas pelo servidor sobre a conexão e, portanto, o ataque (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 14).

35 / 40
Um administrador de rede percebeu um pouco de tráfego suspeito na rede da empresa. Ele decide investigar. Após realizar o ping com sucesso na origem do tráfego, ele usa um utilitário para encontrar o endereço MAC associado.

Qual utilitário ele usa?

A) ARP
B) DNSSpoof
C) PSExec

A) Correto. O ARP mostra os endereços MAC de todos os endereços IP dos quais o tráfego de rede foi recebido. (Lit. Pentration Testing, A Hands-On Introduction to Hacking. Chapter 7.)
B) Incorreto. O DNSSpoof não fornece informações sobre endereços MAC.
C) Incorreto. O PSExec não fornece informações sobre endereços MAC.

36 / 40
No Metasploit Framework (msf) é possível usar vários exploits. Depois de selecionar um exploit para usar contra uma vítima, em alguns casos, é obrigatório selecionar um alvo.

Um pentester selecionou e iniciou um exploit. A seguinte mensagem de erro é mostrada no terminal: "Exploit falhou: um destino não foi selecionado"

Como isso pode ser corrigido?

A) Configurando a variável RHOST para fornecer um endereço de destino
B) Verificando os destinos disponíveis digitando `'show targets'` e, então, selecionando um destino digitando `'set TARGET x'`
C) Digitando `'check'` se o destino estiver vulnerável

A) Incorreto. O RHOST só é utilizado para definir o parâmetro do host remoto.
B) Correto. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 4, Paragraph Finding Metasploit Modules, Subparagraph The Module Database.)
C) Incorreto. “check” não é uma opção válida.

37 / 40
Quando se observam os arquivos de log no servidor web, Pete quer saber qual navegador foi utilizado durante o ataque contra o site dele. Pete deve procurar informações que geralmente são enviadas por meio do cabeçalho <answer>.

Qual cabeçalho `<answer>` está relacionado com isso?

A) Aceitar-Idioma:
B) Host:
C) User-Agent:

A) Incorreto. O User-Agent informa a um servidor web o tipo e a versão do navegador do cliente.
B) Incorreto. O User-Agent informa a um servidor web o tipo e a versão do navegador do cliente.
C) Correto. O User-Agent informa a um servidor web o tipo e a versão do navegador do cliente (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 7)

38 / 40
Uma empresa sofreu um ataque de DDoS. Eles têm o endereço IP do invasor e desejam entrar em contato com seu Provedor de Serviços de Internet para denunciar um abuso.

O que eles devem fazer?

A) Pesquisa de DNS
B) Pesquisa de localização por GeoIP
C) Pesquisa WHOIS

A) Incorreto. Isto é utilizado apenas para obter tabelas DNS.
B) Incorreto. Isto mostra apenas informações de geolocalização para o endereço IP.
C) Correto. O WHOIS mostra toda as informações existentes para saber sobre o endereço IP.

39 / 40
Um penetration tester está realizando uma varredura no ambiente de rede de seu cliente com uma ferramenta. Essa ferramenta tem as seguintes propriedades:

- Ela usa uma classificação para mostrar o impacto de uma vulnerabilidade.
- Ela detecta todos os tipos de vulnerabilidades em vários sistemas operacionais como Windows, Linux e Mac OS.
- Ela é capaz de detectar bots, cavalos de troia e outros malwares que podem ser instalados em computadores conectados à rede.

Qual é o nome da ferramenta que o penetration tester está usando?

A) nessus
B) nmap
C) nikto

A) Correto. O Nessus é um verificador de vulnerabilidades que usa todos os itens apresentados na pergunta. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 6, Paragraph Nessus.)
B) Incorreto. O Nmap não realiza a varredura de vulnerabilidades. É um verificador de versão.
C) Incorreto. O Nikto é um verificador apenas para aplicativos da web.

40 / 40
Qual é o nome dos módulos do Metasploit que **não** são utilizados para fins de exploração?

A) auxiliares
B) payloads
C) shellcodes

A) Correto. Alguns módulos não utilizados para fins de exploração são conhecidos como módulos auxiliares; eles incluem verificadores, fuzzers e até mesmo módulos de negação de serviço. Uma boa regra prática para se ter em mente é que módulos de exploração usam payload e módulos auxiliares, não. (Lit. Penetration Testing, A Hands-On Introduction to Hacking. Chapter 4, Paragraph Using an Auxiliary Module.)
B) Incorreto. Payloads são o mesmo que shellcode e são utilizadas para explorar.
C) Incorreto. Shellcodes são a mesma coisa que payloads e são utilizados para explorar.

Avaliação

A tabela a seguir mostra as respostas corretas às questões apresentadas neste exame simulado.

Questão	Resposta	Questão	Resposta
1	D	**21**	B
2	C	**22**	A
3	A	**23**	A
4	B	**24**	C
5	C	**25**	A
6	C	**26**	A
7	B	**27**	C
8	A	**28**	A
9	A	**29**	A
10	A	**30**	C
11	B	**31**	D
12	C	**32**	A
13	B	**33**	B
14	C	**34**	C
15	B	**35**	A
16	B	**36**	B
17	C	**37**	C
18	C	**38**	C
19	C	**39**	A
20	B	**40**	A

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER