Exame Simulado

Fundamentos de Ethical Hacking EXIN

Edição Augusto 2015

EXIN | ETHICAL HACKING

Conteúdo

Introdução	4
Exame simulado	5
Gabarito de respostas	12
Avaliação	23

Introdução

Este é o modelo de exame que consiste de 20 questões de múltipla escolha.

O exame real consiste de 40 questões de múltipla escolha.

Cada questão de múltipla escolha possui um número de possíveis respostas, onde somente uma é a resposta correta.

O número máximo de pontos que pode ser obtido neste exame simulado é 20. Cada questão correta corresponde a um ponto. Para ser aprovado você precisa acertar 13 (65%) ou mais pontos.

O tempo máximo permitido para a realização do exame é de 20 minutos.

Nenhum direito será derivado desta informação.

Boa sorte!

Exame simulado

1 de 20

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 de 20

Alguém violou um site e conseguiu manter isso em segredo. O hacking 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

3 de 20

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 black hat Hacking
C. Teste de invasão white box

4 de 20

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

5 de 20

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.

6 de 20

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:

7 de 20

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`

8 de 20

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

9 de 20

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

10 de 20

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

11 de 20

Uma testadora de invasão 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>`

12 de 20

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`

13 de 20

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.

14 de 20

Ao digitar a exploração no Metasploit, o módulo de exploração não funciona e gera um erro que informa que o 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

15 de 20

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

16 de 20

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

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

17 de 20

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)>`

18 de 20

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

19 de 20

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

20 de 20

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

Gabarito de respostas

1 de 20

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. (EXIN, ECCouncil, Curso CEHv8)
B. Incorreto. O cálculo do ROI faz parte da seleção de controle e da mitigação de riscos. (ECCouncil, Curso CEHv8)
C. Incorreto. O Hackeamento Ético significa encontrar e documentar vulnerabilidades, mas não resolvê-las. (ECCouncil, Curso CEHv8)
D. Correto. A função principal dos Hackers Éticos é testar a segurança (EXIN, ECCouncil CEHv8)

2 de 20

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.
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.

3 de 20

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.

4 de 20

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 (Testes de invasão, capítulo 7).

5 de 20

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 (Testes de invasão, capítulo 14).

6 de 20

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 (Testes de invasão, capítulo 7)

7 de 20

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 (Testes de invasão)

8 de 20

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 (Testes de invasão)
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.

9 de 20

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.

10 de 20

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 (Testes de invasão).

11 de 20

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.
B. Correto.
C. Incorreto.

12 de 20

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.

13 de 20

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.
B. Incorreto.
C. Incorreto.

14 de 20

Ao digitar a exploração no Metasploit, o módulo de exploração não funciona e gera um erro que informa que o 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.
B. Correto.
C. Incorreto.

15 de 20

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.

16 de 20

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.
B. Correto.
C. Incorreto.

17 de 20

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.
B. Incorreto.
C. Correto.

18 de 20

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.
B. Incorreto.
C. Incorreto.

19 de 20

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.
B. Correto.
C. Incorreto.

20 de 20

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.
B. Correto.
C. Incorreto.

Avaliação

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

Número	Resposta	Pontos
1	D	1
2	A	1
3	A	1
4	C	1
5	C	1
6	C	1
7	A	1
8	A	1
9	B	1
10	C	1
11	B	1
12	A	1
13	A	1
14	B	1
15	D	1
16	B	1
17	C	1
18	A	1
19	B	1
20	B	1

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER