

1. Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- A. Rainbow table
- B. Dictionary
- C. Password spraying
- D. Pass-the-hash

Answer: C

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

Answer: C

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80 200 200  
[02/Feb/2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

- A. Secure cookies
- B. Input validation
- C. Code signing
- D. Stored procedures

Answer: B

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

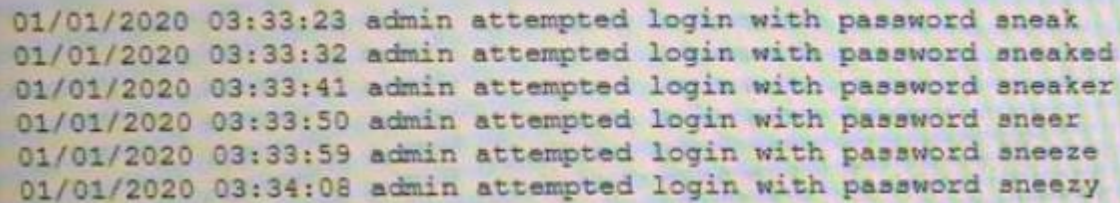
No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

Answer: B

A security analyst is reviewing logs on a server and observes the following output:



```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

Answer: C