

9. How does the email's claim that "Over 92% of employees have already completed the verification" attempt to pressure the recipient into responding to the email?
- (A) By framing the request as routine HR communication that seems safe, showing the use of familiarity
 - (B) By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity
 - (C) By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority
 - (D) By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus
10. Which of the following is the most likely impact if the recipient responds to this email with the requested information?
- (A) An adversary could use the recipient's personal details to impersonate them.
 - (B) An adversary could use the recipient's device as a foothold and move laterally on the network compromising other devices.
 - (C) An adversary could infect the recipient's device with malicious code hidden in the reply email.
 - (D) An adversary could disrupt the entire payroll system by disabling access for all employees.
11. A natural gas company's help desk receives reports from employees that the company's website is intermittently crashing when they try to log in. The cybersecurity analyst reviews the server's access logs and finds the following entries.

```
[22/Oct/2025:10:11:02] "GET /index.html HTTP/1.1" 200 4521
[22/Oct/2025:10:11:07] "GET /about.html HTTP/1.1" 200 3890
[22/Oct/2025:10:11:10] "GET ../../../../etc/passwd HTTP/1.1" 403 721
[22/Oct/2025:10:11:12] "GET ../../../../etc/shadow HTTP/1.1" 403 654
```

Which of the following application attacks is indicated in the log file?

- (A) Buffer overflow attack
 - (B) Cross site scripting attack
 - (C) Directory traversal attack
 - (D) SQL injection attack
18. Which of the following types of attacks occurred when the adversary submitted a string that included ' OR '1'='1';--?
- (A) SQL injection attack
 - (B) Buffer overflow attack
 - (C) Cross site scripting attack
 - (D) Directory traversal attack