



# 312-50V11<sup>Q&As</sup>

Certified Ethical Hacker v11 Exam

**Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/312-50v11.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Distributed assessment
- B. Wireless network assessment
- C. Most-based assessment
- D. Application assessment

Correct Answer: B

Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

---

### QUESTION 2

You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

- A. hping2 host.domain.com
- B. hping2 --set-ICMP host.domain.com
- C. hping2 -i host.domain.com
- D. hping2 -1 host.domain.com

Correct Answer: D

---

### QUESTION 3

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers



E. Have subnet diversity between DNS servers

Correct Answer: BCDE

#### QUESTION 4

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Correct Answer: A

#### QUESTION 5

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

- A. Proxy scanner
- B. Agent-based scanner
- C. Network-based scanner
- D. Cluster scanner

Correct Answer: B

Knowing when to include agents into your vulnerability management processes isn't an easy decision. Below are common use cases for agent-based vulnerability scanning to assist you build out your combined scanning strategy.

**Intermittent or Irregular Connectivity:** Vulnerability management teams are now tasked with scanning devices that access the company network remotely using public or home-based Wi-Fi connections. These connections are often unreliable and intermittent leading to missed network-based scans. Fortunately, the scanning frequency of agents doesn't require a network connection. The agent detects when the device is back online, sending scan data when it's ready to communicate with the VM platform.

**Connecting Non-Corporate Devices to Corporate Networks:** With the increased use of private devices, company networks are more exposed to malware and infections thanks to limited IT and security teams' control and visibility. Agent-based scanning gives security teams insight into weaknesses on non-corporate endpoints, keeping them informed about professional hacker is potential attack vectors in order that they can take appropriate action.

**Endpoints Residing Outside of Company Networks:** Whether company-issued or BYOD, remote assets frequently hook up with the web outside of traditional network bounds. An agent that resides on remote endpoints conducts regular, authenticated scans checking out system changes and unpatched software. The results are then sent back to the VM platform and combined with other scan results for review, prioritization, and mitigation planning.



VCE & PDF

PassApply.com

<https://www.passapply.com/312-50v11.html>

2024 Latest passapply 312-50V11 PDF and VCE dumps Download

---

[Latest 312-50V11 Dumps](#)

[312-50V11 VCE Dumps](#)

[312-50V11 Exam Questions](#)