COMP623 - Digital Security - 14818 - WIN - 202110

Notifications
Announcements

Module Content
Course Handbook

Assessment & Feedback
Academic Integrity Tutorial
Quote Unquote
Turnitin Student Help

Learning Resources
Reading List
MyBeckett Student Help
Library
Skills For Learning

Module Resources
Module Content
Module Handbook
Quizzes
Report Submission

Take Test: Footprinting

Test Information

Description	
Instructions	
Timed Test	This test has a time limit of 40 minutes.This test will save and be submitted automatically when the time expires. Warnings appear when **half the time**, **5 minutes**, **1 minute**, and **30 seconds** remain.
Multiple Attempts	Not allowed. This Test can only be taken once.
Force Completion	Once started, this test must be completed in one sitting. Do not leave the test before clicking **Save and Submit**. Your answers are saved automatically.

QUESTION 1 — 1 points — Saved

Starting with a single IP address, how could an attacker determine the range of IP addresses used by the company?

- DNS
- (•) Whois
- The dig command
- Domain bruteforcing

QUESTION 2 — 1 points — Saved

Put the stages of attack into the correct order

5. Post-exploitation
4. Exploitation
1. Footprinting
2. Enumeration
3. Scanning

QUESTION 3 — 1 points — Saved

The steps of an attack typically involve this sequence of events:

- Scanning, footprinting, and hacking
- (•) Information gathering, exploitation, and post-exploitation
- Maintaining access, information gathering, and hacking
- Exploitation, information gathering, covering tracks

QUESTION 4 — 1 points — Saved

dig +short google.co.uk

The above command will return what?

- (•) IP address(es) that the domain name resolves to
- The name server(s) used to provide authoritative information about the DNS zone
- Mail server(s)
- IPv6 address(es)
- Domain name(s)
- The results of a DNS zone transfer
- A listing of various types of DNS records

QUESTION 5 — 1 points — Saved

Given a domain name, an attacker could determine IP address(es) using:

- Whois
- Zone transfer
- Subdomain bruteforcing
- (•) The dig command

QUESTION 6 — 1 points — Saved

RIPE and ARIN are examples of:

- Registrars
- Protocols
- (•) Regional internet registries
- Exploits

QUESTION 7 — 1 points — Saved

dig +short -x 130.57.5.70

The above command will return what?

- The name server(s) used to provide authoritative information about the DNS zone
- (•) Domain name(s)
- A listing of various types of DNS records
- The results of a DNS zone transfer
- IP address(es) that the domain name resolves to
- Mail server(s)
- IPv6 address(es)

QUESTION 8 — 1 points — Saved

dig +short leedsmet.ac.uk MX

The above command will return what?

- Domain name(s)
- The results of a DNS zone transfer
- IPv6 address(es)
- A listing of various types of DNS records
- The name server(s) used to provide authoritative information about the DNS zone
- (•) Mail server(s)
- IP address(es) that the domain name resolves to

QUESTION 9 — 1 points — Saved

dig @8.8.8.8 mydomain.co.uk

The above command does what?

- Attempts to use a reverse lookup on 8.8.8.8 to determine which domain name it points to, using mydomain.co.uk as the DNS server
- Attempts a zone transfer on mydomain.co.uk using the 8.8.8.8 server
- (•) Attempts to resolve the IP address for mydomain.co.uk using the DNS server 8.8.8.8
- Attempts to use a reverse lookup on 8.8.8.8 to determine which domain name it points to, and compares the answer to mydomain.co.uk

QUESTION 10 — 1 points — Saved

dig +short google.co.uk AAAA

The above command will return what?

- The name server(s) used to provide authoritative information about the DNS zone
- IP address(es) that the domain name resolves to
- A listing of various types of DNS records
- The results of a DNS zone transfer
- Domain name(s)
- Mail server(s)
- (•) IPv6 address(es)