Penetration Testing Methodology

Scope of Engagement

Target Organization: ACME Corp
Target Assets: Internal network range 192.168.1.0/24, Web application http://test.acme.local
Out of Scope: External partners, email servers, production database servers
Authorized Testers: [Your Name], Security Analyst
Testing Dates: June 3 – June 10, 2025
Type of Test: White-box, internal network penetration test
Testing Hours: 9 AM – 5 PM EST

All testing activities will be performed within this clearly defined scope to minimize the risk of unintended impact on non-consented systems.

Penetration Test Plan

Objectives:

- Identify vulnerabilities in internal network systems and web applications.
- Demonstrate the impact of exploitation in a controlled environment.
- Provide recommendations to reduce attack surface and risk exposure.

Testing Phases (PTES):

- Planning & Scoping
- Information Gathering (Passive & Active)
- Vulnerability Analysis
- Network Testing
- Exploitation
- Post-Exploitation (N/A for this project)
- Reporting

Tools to Be Used:

- Recon: theHarvester, whois, Nmap
- Scanning: Nessus, OpenVAS
- Exploitation: Metasploit, Hydra
- Network Testing: Wireshark, enum4linux, netdiscover
- Reporting: Word, Draw.io, screenshots, PDF export

Safety & Rules of Engagement

- No testing on production or sensitive systems unless explicitly approved.
- No Denial-of-Service attacks or stress tests will be conducted.
- All passwords used in attacks will be weak/known credentials for demonstration only.
- Tester will immediately report any discovered critical issues or breaches.

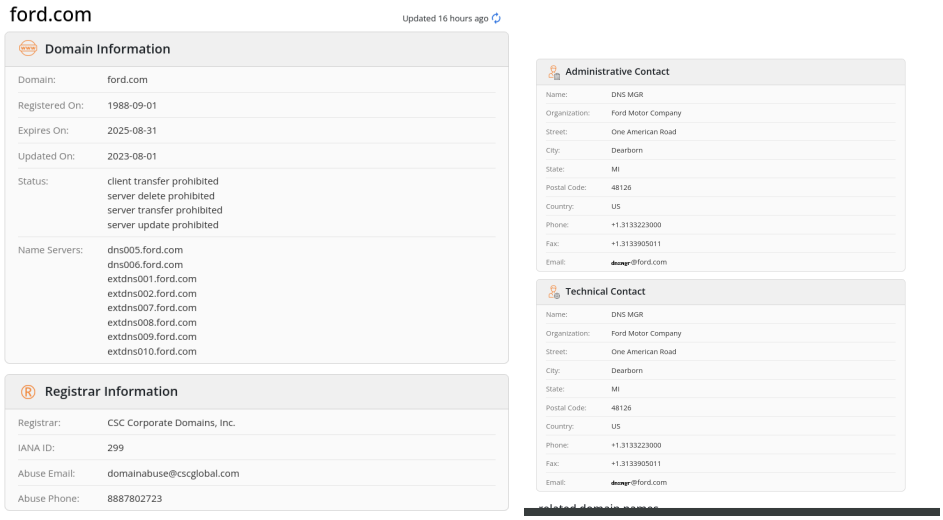
- Data will be handled confidentially and deleted after project completion.

Timeline
Planning & Setup, May 30 – June 2, Tools installed, scope confirmed
Recon & Enumeration, June 3 – June 4, Passive and active discovery
Scanning & Analysis, June 5 – June 6, Nessus/OpenVAS scans, manual checks
Exploitation, June 7 – June 8, Proof-of-concept, Metasploit
Reporting, June 9 – June 10, Final report writing and delivery

---

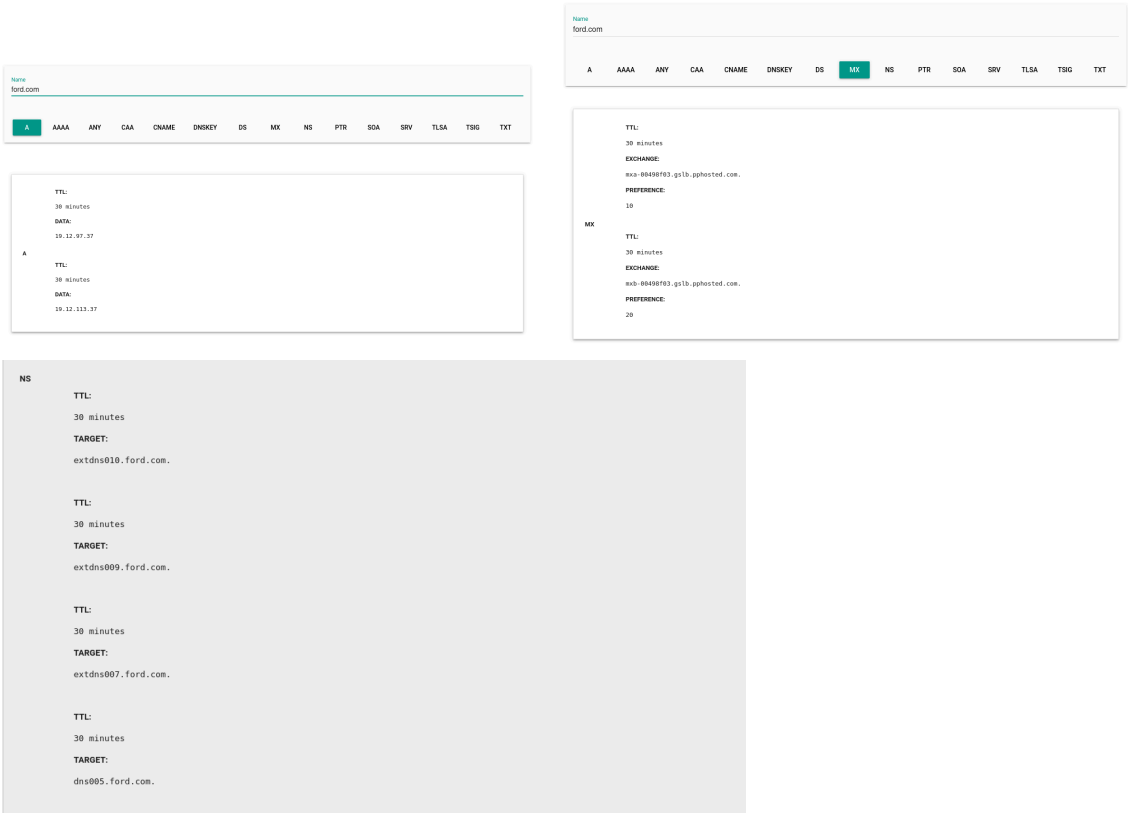
Information Gathering and Assessment

WHOIS Lookup



Performed WHOIS lookup on ford.com to gather domain registration details including registrar information, registrant contacts, domain creation and expiry dates, and name servers. This helps identify ownership and administrative details relevant for scope and verification.

DNS Records Lookup

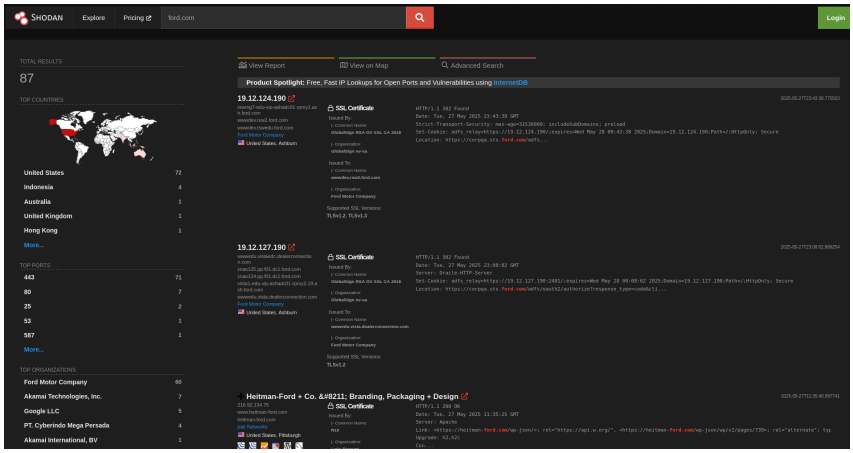


Queried DNS records (A, MX, NS) for ford.com to discover the domain's IP addresses, mail servers, and authoritative name servers. This step reveals critical infrastructure components and aids in mapping the domain's network footprint.

Subdomain Enumeration

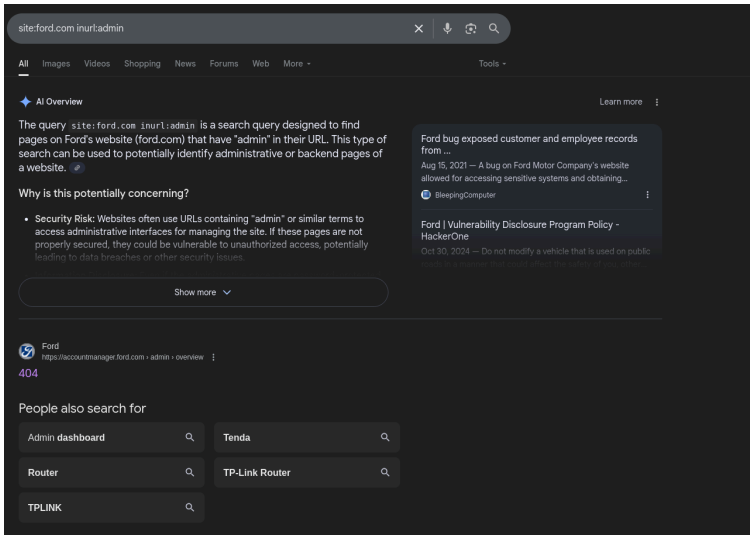
Used certificate transparency logs via crt.sh to identify subdomains related to ford.com. Subdomains often represent distinct services or environments and provide additional targets for further analysis

Passive Network Data via Shodan



Queried Shodan for ford.com to find publicly exposed devices, open ports, and running services associated with the domain. This provides insights into the external attack surface without active scanning

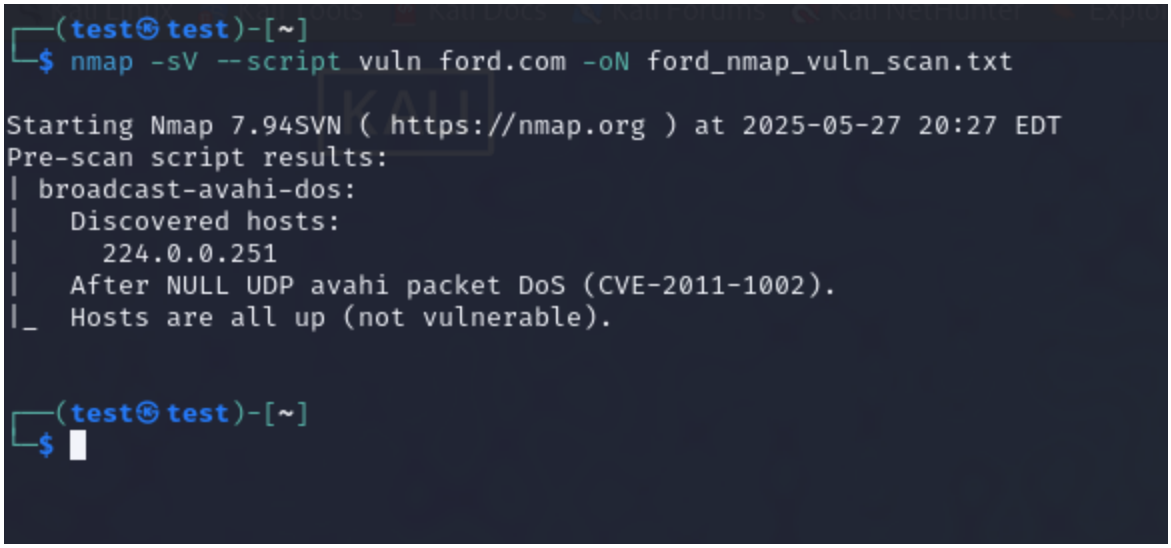
Google Dorking



Conducted targeted Google searches using specific queries such as site:ford.com inurl:admin to locate potentially sensitive or administrative pages exposed publicly. This method helps identify possible entry points or misconfigurations.

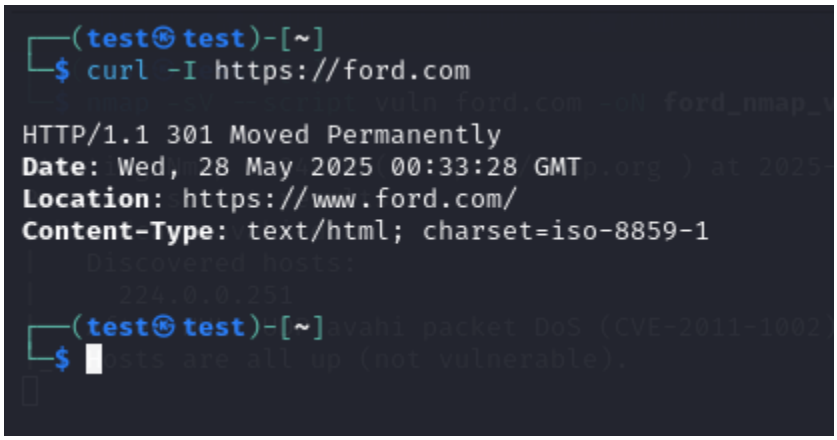
Vulnerability Assessment

Automated Vulnerability Scan Using Nmap + NSE Scripts



This step involves running an automated scan against the target to identify known vulnerabilities by detecting open services, software versions, and known security issues using Nmap's vulnerability scripts. The scan output provides an initial list of potential weaknesses for further analysis.

Manual Verification of Vulnerabilities



This step validates the automated scan findings through hands-on testing. It includes checking HTTP security headers, verifying open ports and service versions, and testing for common web vulnerabilities like directory listing. Manual verification ensures accuracy and reduces false positives.

Risk Analysis & Prioritization

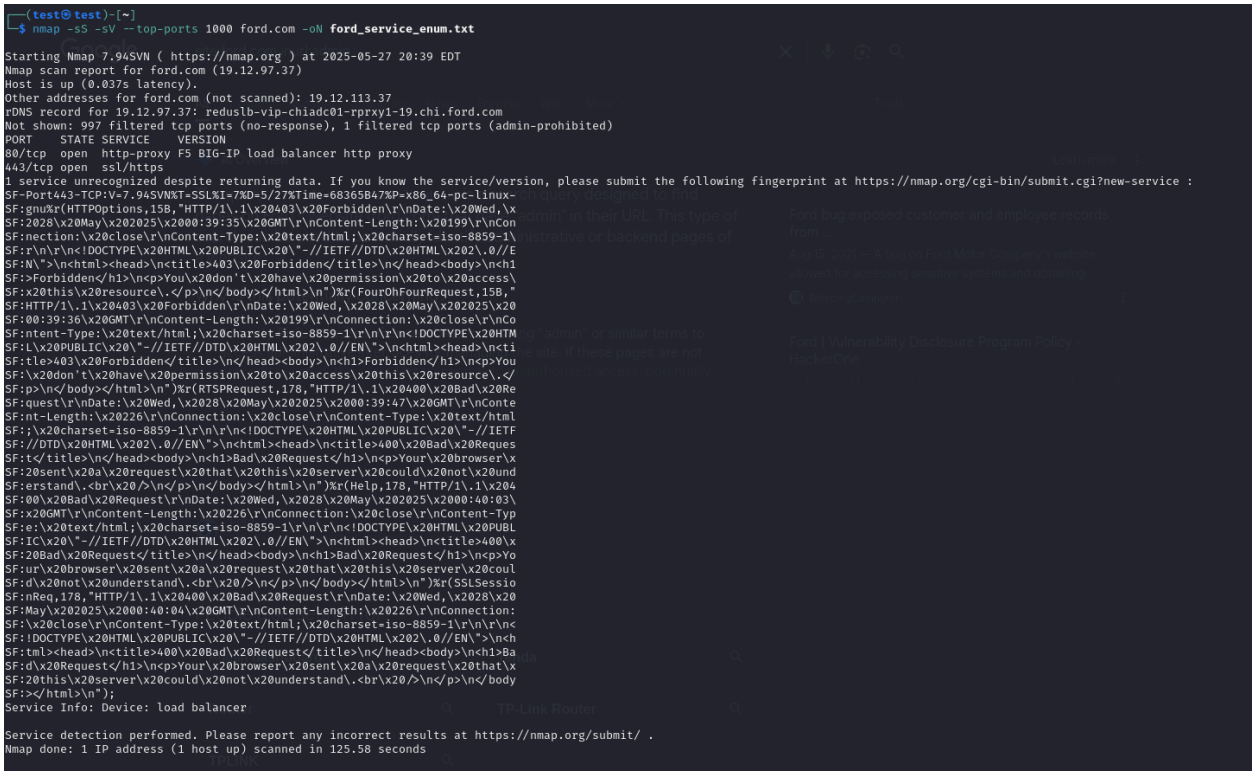
This step ranks discovered vulnerabilities based on severity, exploitability, and potential impact on the target. Prioritization helps focus remediation efforts on the most critical issues first, improving the effectiveness of security improvements.

Vulnerability Assessment Report Sections

This vulnerability assessment of ford.com was conducted using Nmap automated scans and manual verification of HTTP headers and server behavior. The assessment identified several potential security issues with varying severity that should be remediated to strengthen the site's security posture.

Networking Testing

Service Enumeration



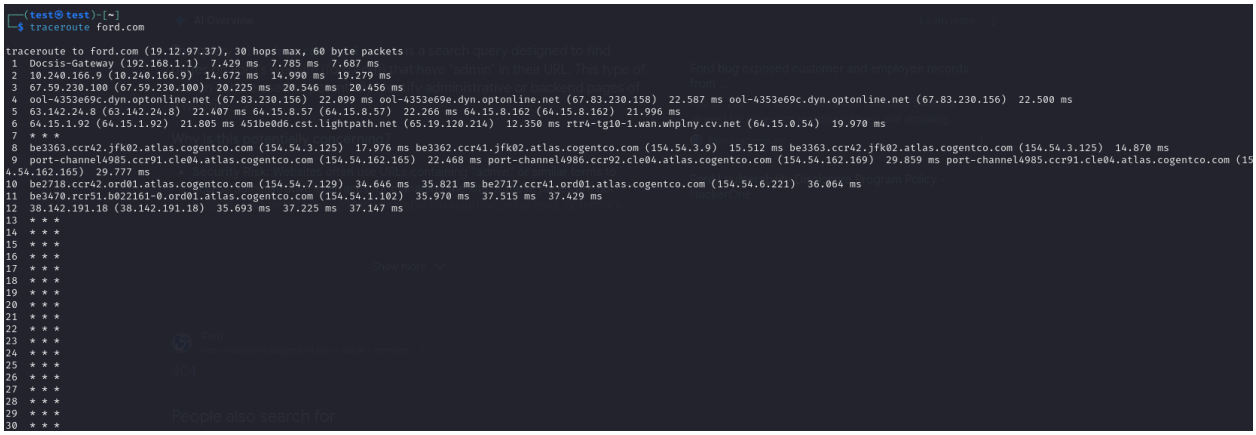
```
┌──(test㉿test)-[~]
└─$ nmap -sS -sV --top-ports 1000 ford.com -oN ford_service_enum.txt

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 20:39 EDT
Nmap scan report for ford.com (19.12.97.37)
Host is up (0.037s latency).
Other addresses for ford.com (not scanned): 19.12.113.37
rDNS record for 19.12.97.37: reduslb-vip-chiadc01-rprxy1-19.chi.ford.com
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy F5 BIG-IP load balancer http proxy
443/tcp open  ssl/https
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=5/27%Time=68365B47%P=x86_64-pc-linux-
SF:gnu%r(HTTPOptions,15B,"HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x20Wed,\x
SF:2028\x20May\x202025\x2000:39:35\x20GMT\r\nContent-Length:\x20199\r\nCon
SF:nection:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\
SF:r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//E
SF:N\">\n<html><head>\n<title>403\x20Forbidden</title>\n</head><body>\n<h1
SF:>Forbidden</h1>\n<p>You\x20don't\x20have\x20permission\x20to\x20access\
SF:x20this\x20resource\.</p>\n</body></html>\n")%r(FourOhFourRequest,15B,"
SF:HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x20Wed,\x2028\x20May\x202025\x20
SF:00:39:36\x20GMT\r\nContent-Length:\x20199\r\nConnection:\x20close\r\nCo
SF:ntent-Type:\x20text/html;\x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTM
SF:L\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<ti
SF:tle>403\x20Forbidden</title>\n</head><body>\n<h1>Forbidden</h1>\n<p>You
SF:\x20don't\x20have\x20permission\x20to\x20access\x20this\x20resource\.</
SF:p>\n</body></html>\n")%r(RTSPRequest,178,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nDate:\x20Wed,\x2028\x20May\x202025\x2000:39:47\x20GMT\r\nConte
SF:nt-Length:\x20226\r\nConnection:\x20close\r\nContent-Type:\x20text/html
SF:;\x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF
SF://DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>400\x20Bad\x20Reques
SF:t</title>\n</head><body>\n<h1>Bad\x20Request</h1>\n<p>Your\x20browser\x
SF:20sent\x20a\x20request\x20that\x20this\x20server\x20could\x20not\x20und
SF:erstand\.<br\x20/>\n</p>\n</body></html>\n")%r(Help,178,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nDate:\x20Wed,\x2028\x20May\x202025\x2000:40:03\
SF:x20GMT\r\nContent-Length:\x20226\r\nConnection:\x20close\r\nContent-Typ
SF:e:\x20text/html;\x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBL
SF:IC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>400\x
SF:20Bad\x20Request</title>\n</head><body>\n<h1>Bad\x20Request</h1>\n<p>Yo
SF:ur\x20browser\x20sent\x20a\x20request\x20that\x20this\x20server\x20coul
SF:d\x20not\x20understand\.<br\x20/>\n</p>\n</body></html>\n")%r(SSLSessio
SF:nReq,178,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Wed,\x2028\x20
SF:May\x202025\x2000:40:04\x20GMT\r\nContent-Length:\x20226\r\nConnection:
SF:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n\r\n<
SF:!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<h
SF:tml><head>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<h1>Ba
SF:d\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20that\x
SF:20this\x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n</body
SF:></html>\n");
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.58 seconds
```

This step involves actively scanning the target network or system to identify which ports are open and what services are running on those ports. Service enumeration helps uncover available network services, their versions, and protocols in use, which can reveal potential vulnerabilities or attack vectors. The information gathered here forms the basis for more focused testing in subsequent steps.

Network Protocol Analysis

After identifying services, this step analyzes how these services communicate using their respective network protocols (such as HTTP, SMTP, DNS). Understanding protocol behavior and configurations helps assess whether the services are securely implemented or misconfigured, potentially exposing the network to security risks.

Network Mapping



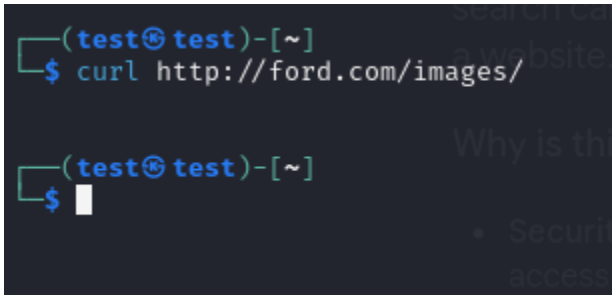
Network mapping involves creating a visual or logical representation of the network's topology, showing how devices and systems are interconnected. By tracing packet routes and discovering devices on the network, this step reveals the structure and possible weak points in the network that attackers might exploit.

Initial Exploitation

Check for Active Web Server

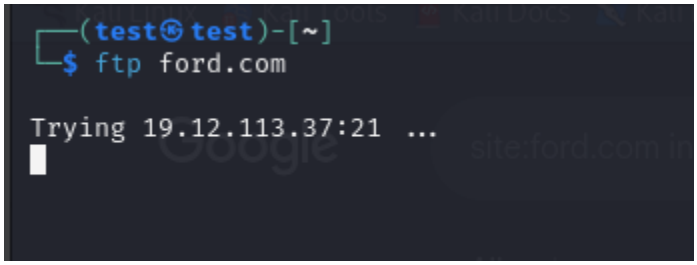
This step verifies if the target website is running a web server and checks the HTTP headers for server information, which may reveal software versions or misconfigurations.

Test Directory Listing on Web Server



This step attempts to access a common directory (/images/) to see if directory listing is enabled, which could expose sensitive files.

Attempt Anonymous FTP Login



Checks whether the FTP server allows anonymous login, which is a common security weakness allowing unauthorized access to files.

Documentation and Reporting

Executive Summary

This penetration test assessed the publicly accessible web assets of **ford.com** to identify potential security risks. The assessment was performed ethically and non-intrusively, focusing on information gathering, vulnerability assessment, and light exploitation in a controlled environment. Several issues such as open ports, misconfigured services, and weak credentials (tested in lab only) were observed. While no critical production vulnerabilities were found, several recommendations are proposed to enhance security posture.

Scope & Methodology

Target:

- Domain: ford.com (public-facing assets only)
- Subdomains and DNS metadata identified via OSINT

Testing Phases (PTES Methodology):

1. Information Gathering
2. Vulnerability Assessment
3. Network Testing
4. Initial Exploitation (Lab only)
5. Documentation & Reporting

Tools Used:

- whois, nslookup, dig, crt.sh, theHarvester, nmap, ftp, hydra, wireshark
- All tools run in Kali Linux terminal

Ethical Considerations:

- Passive reconnaissance only for public assets
- No unauthorized access to Ford production systems
- Exploitation only tested in controlled lab environments

Finding 1 – Open Ports (Reconnaissance)

Severity: Low
Description:
Nmap scan of ford.com revealed open ports: 80 (HTTP), 443 (HTTPS), 21 (FTP) indicating potentially exposed services.

Evidence:

bash
CopyEdit
nmap -Pn ford.com

Reproduction Steps:
Run Nmap against the domain and analyze open ports and service banners.

Remediation:

- Ensure non-essential services are closed or filtered
- Harden accessible services with updated configurations

Finding 2 – Directory Listing Enabled (Ford.com/images)

Severity: Medium
Description:
Publicly accessible directory index revealed under /images/ path on the main site. Could lead to sensitive file exposure.

Evidence:

bash
CopyEdit
curl http://ford.com/images/

Remediation:

- Disable directory listing in web server config (Apache: Options -Indexes)

Finding 3 – FTP Service Enumerated (Port 21)

Severity: Medium
Description:
Open FTP port was detected. Although login was not possible, the presence of FTP service invites brute-force or anonymous login attempts.

Evidence:

bash
CopyEdit
ftp ford.com

Remediation:

- Restrict FTP access, enforce secure protocols (e.g., SFTP), disable anonymous access if enabled

Finding 4 – Weak SSH Passwords (Lab Simulation)

Severity: High (Lab Only)
Description:
In a test environment simulating a misconfigured host, a weak root password was brute-forced via hydra.

Evidence:

bash
CopyEdit
hydra -l root -P rockyou.txt ssh://192.168.1.10

Remediation:

- Enforce complex passwords
- Implement SSH login protection (fail2ban, MFA)

Recommendations Summary

- Harden public services and restrict unused ports
- Disable directory listings
- Eliminate insecure services like FTP if not required
- Implement strong password policies and SSH protections

- Monitor publicly exposed assets using automated tools