

# 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

**ford.com** Updated 16 hours ago

Domain Information	
Domain:	ford.com
Registered On:	1988-09-01
Expires On:	2025-08-31
Updated On:	2023-08-01
Status:	client transfer prohibited server delete prohibited server transfer prohibited server update prohibited
Name Servers:	dns005.ford.com dns006.ford.com extdns001.ford.com extdns002.ford.com extdns007.ford.com extdns008.ford.com extdns009.ford.com extdns010.ford.com

Registrar Information	
Registrar:	CSC Corporate Domains, Inc.
IANA ID:	299
Abuse Email:	domainabuse@cscglobal.com
Abuse Phone:	8887802723

Administrative Contact	
Name:	DNS MGR
Organization:	Ford Motor Company
Street:	One American Road
City:	Dearborn
State:	MI
Postal Code:	48126
Country:	US
Phone:	+1.3133223000
Fax:	+1.3133905011
Email:	dnsmgr@ford.com

Technical Contact	
Name:	DNS MGR
Organization:	Ford Motor Company
Street:	One American Road
City:	Dearborn
State:	MI
Postal Code:	48126
Country:	US
Phone:	+1.3133223000
Fax:	+1.3133905011
Email:	dnsmgr@ford.com

related domain names

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

The diagram illustrates DNS record types and their associated TTL values. It is divided into two main sections: a top section for general DNS records and a bottom section for MX records.

**Top Section: General DNS Records**

This section shows a list of DNS record types: A, AAAA, ANY, CAA, CNAME, DNSKEY, DS, **MX** (highlighted in green), NS, PTR, SOA, SRV, TLSA, TSIG, and TXT. Below this list, a table provides the TTL values for each record type:

Record Type	TTL
A	30 minutes
AAAA	30 minutes
ANY	10
CAA	10
CNAME	10
DNSKEY	10
DS	10
MX	30 minutes
NS	10
PTR	10
SOA	10
SRV	10
TLSA	10
TSIG	10
TXT	10

**Bottom Section: MX Records**

This section shows a list of MX records: A, AAAA, ANY, CAA, CNAME, DNSKEY, DS, **MX** (highlighted in green), NS, PTR, SOA, SRV, TLSA, TSIG, and TXT. Below this list, a table provides the TTL values for each MX record type:

Record Type	TTL
A	30 minutes
AAAA	30 minutes
ANY	10
CAA	10
CNAME	10
DNSKEY	10
DS	10
MX	30 minutes
NS	10
PTR	10
SOA	10
SRV	10
TLSA	10
TSIG	10
TXT	10

name

ford.com

A

AAAA

ANY

CAA

CNAME

DNSKEY

D5

**MX**

NS

PTR

SOA

SRV

TLSA

TSIG

TXT

TTL:

30 minutes

EXCHANGE:

exa-00400f03.gslb.phosted.com.

PREFERENCE:

10

MX

TTL:

30 minutes

EXCHANGE:

exb-00400f03.gslb.phosted.com.

PREFERENCE:

20

```

NS

TTL:
30 minutes

TARGET:
extdns010.ford.com.

TTL:
30 minutes

TARGET:
extdns009.ford.com.

TTL:
30 minutes

TARGET:
extdns007.ford.com.

TTL:
30 minutes

TARGET:
dns005.ford.com.

```

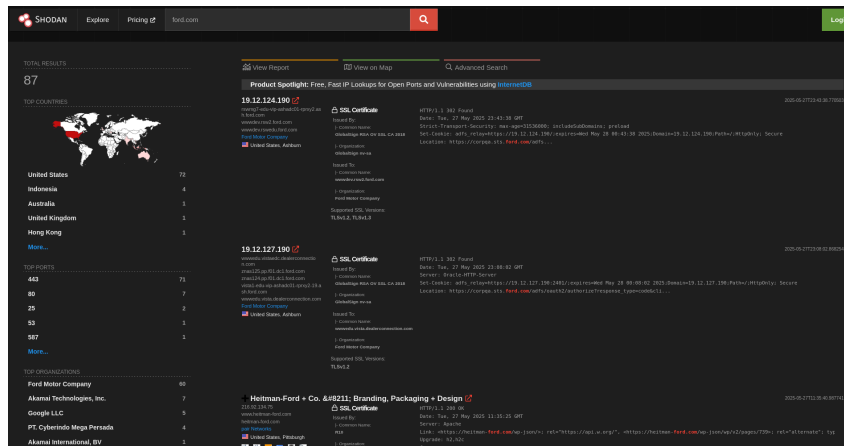
Queried DNS records (A, MX, NS) for ford.com to discover the domain's IP addresses, mail servers, and authoritative name servers. This step reveals critical infrastructure components and aids in mapping the domain's network footprint.

## Subdomain Enumeration

[illegible]

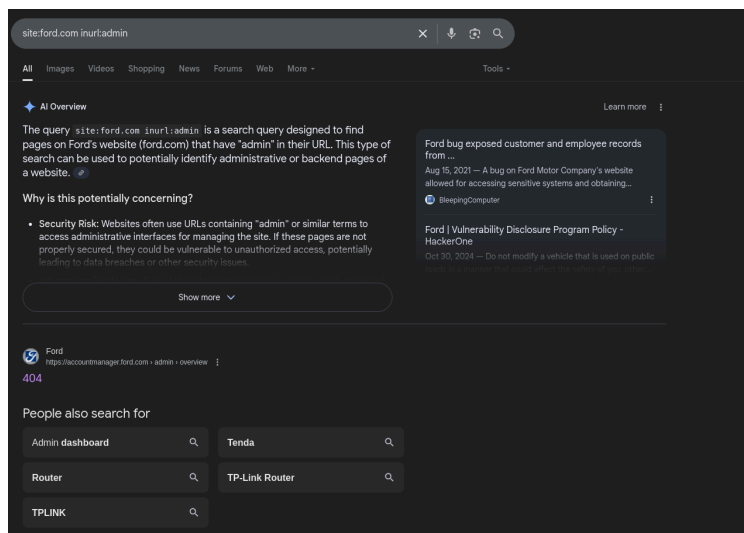
Used certificate transparency logs via crt.sh to identify subdomains related to ford.com. Subdomains often represent distinct services or environments and provide additional targets for further analysis

## 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

```

(test@test)-[~]
$ nmap -sV --script vuln ford.com -oN ford_nmap_vuln_scan.txt

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 20:27 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

(test@test)-[~]
$ █

```

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

```

(test@test)-[~]
$ curl -I https://ford.com

HTTP/1.1 301 Moved Permanently
Date: Wed, 28 May 2025 00:33:28 GMT
Location: https://www.ford.com/
Content-Type: text/html; charset=iso-8859-1

(test@test)-[~]
$ █

```

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
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=2.94SVNNT-SSLXI=7KD=5/278Time=68365847XP=x86_64-pc-linux
SF:gnuxr(HTTPOptions,158,"HTTP/1.1,x20403x20Forbidden\r\nDate:x20Wed,x
SF:2028x20Mayx202025x2000:39:35x20GMT\r\nContent-Length:x20199\r\nCon
SF:nction:x20close\r\nContent-Type:x20text/html;x20charset=iso-8859-1\
SF:r\n\r\n<DOCTYPEx20HTMLx20PUBLICx20\"~//IETF//DTDx20HTMLx202.0//E
SF:N\">\n<html><head>\n<title>403x20Forbidden</title>\n</head><body>\n<h1
SF:Forbidden</h1>\n<p>Youx20don'tx20havex20permissionx20toaccessx20
SF:x20thisx20resource</p>\n</body></html>\n\"%r(Four0hFourRequest,158,\"
SF:HTTP/1.1,x20403x20Forbidden\r\nDate:x20Wed,x2028x20Mayx202025x20
SF:00:39:36x20GMT\r\nContent-Length:x20199\r\nConnection:x20close\r\nCo
SF:ntent-Type:x20text/html;x20charset=iso-8859-1\r\n\r\n<DOCTYPEx20HTM
SF:Lx20PUBLICx20\"~//IETF//DTDx20HTMLx202.0//EN\">\n<html><head>\n<ti
SF:tle>403x20Forbidden</title>\n</head><body>\n<h1>Forbidden</h1>\n<p>You
SF:x20don'tx20havex20permissionx20toaccessx20thisx20resource</p>
SF:p>\n</body></html>\n\"%r(PFSPRequest,178,\"HTTP/1.1,x20400x20Badx20Requ
SF:est\r\nDate:x20Wed,x2028x20Mayx202025x2000:39:47x20GMT\r\nConte
SF:nt-Length:x20226\r\nConnection:x20close\r\nContent-Type:x20text/html
SF;x20charset=iso-8859-1\r\n\r\n<DOCTYPEx20HTMLx20PUBLICx20\"~//IETF
SF://DTDx20HTMLx202.0//EN\">\n<html><head>\n<title>400x20Badx20Reques
SF:t</title>\n</head><body>\n<h1>Badx20Request</h1>\n<p>Yourx20browser\x
SF:20sentx20a\x20requestx20thatx20thisx20serverx20couldx20notx20und
SF:erstand<br>x20/>\n<p>\n</body></html>\n\"%r(HELP,178,\"HTTP/1.1,x204
SF:00x20Badx20Request\r\nDate:x20Wed,x2028x20Mayx202025x2000:40:03\
SF:x20GMT\r\nContent-Length:x20226\r\nConnection:x20close\r\nContent-Typ
SF:e:x20text/html;x20charset=iso-8859-1\r\n\r\n<DOCTYPEx20HTMLx20PUBL
SF:ICx20\"~//IETF//DTDx20HTMLx202.0//EN\">\n<html><head>\n<title>400\x
SF:20Badx20Request</title>\n</head><body>\n<h1>Badx20Request</h1>\n<p>Yo
SF:urx20browserx20sentx20a\x20requestx20thatx20thisx20serverx20coul
SF:d\x20notx20understand<br>x20/>\n<p>\n</body></html>\n\"%r(SSLSSio
SF:nReq,178,\"HTTP/1.1,x20400x20Badx20Request\r\nDate:x20Wed,x2028x20
SF:Mayx202025x2000:40:04x20GMT\r\nContent-Length:x20226\r\nConnection:
SF:x20close\r\nContent-Type:x20text/html;x20charset=iso-8859-1\r\n\r\n<
SF:DOCTYPEx20HTMLx20PUBLICx20\"~//IETF//DTDx20HTMLx202.0//EN\">\n<h
SF:tml><head>\n<title>400x20Badx20Request</title>\n</head><body>\n<h1>Ba
SF:d\x20Request</h1>\n<p>Yourx20browserx20sentx20a\x20requestx20that\x
SF:20thisx20serverx20couldx20notx20understand<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

```
(test@test)-[~]
$ curl -I http://ford.com

HTTP/1.0 302 Moved Temporarily
Location: https://ford.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

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

```
(test@test)-[~]
$ traceroute ford.com

traceroute to ford.com (19.12.97.37), 30 hops max, 60 byte packets
 1  Docsis-Gateway (192.168.1.1)  7.429 ms  7.785 ms  7.687 ms
 2  10.240.166.9 (10.240.166.9)  14.072 ms  14.998 ms  19.279 ms
 3  67.59.230.100 (67.59.230.100)  20.225 ms  20.546 ms  20.456 ms
 4  ool-4353e69e.dyn.optonline.net (67.83.230.156)  22.099 ms  ool-4353e69e.dyn.optonline.net (67.83.230.156)  22.500 ms
 5  63.142.24.8 (63.142.24.8)  22.407 ms  64.15.8.57 (64.15.8.57)  22.266 ms  64.15.8.162 (64.15.8.162)  21.996 ms
 6  64.15.1.92 (64.15.1.92)  21.805 ms  451be0d6.cst.lightpath.net (65.19.120.214)  12.350 ms  rtr4-tg10-1.wan.whplny.cv.net (64.15.0.54)  19.970 ms
 7  * * *
 8  be3363.ccr42.jfk02.atlas.cogentco.com (154.54.3.125)  17.976 ms  be3362.ccr41.jfk02.atlas.cogentco.com (154.54.3.9)  15.512 ms  be3363.ccr42.jfk02.atlas.cogentco.com (154.54.3.125)  14.870 ms
 9  port-channel4985.ccr91.cle04.atlas.cogentco.com (154.54.162.165)  22.468 ms  port-channel4986.ccr92.cle04.atlas.cogentco.com (154.54.162.169)  29.859 ms  port-channel4985.ccr91.cle04.atlas.cogentco.com (154.54.162.165)  29.777 ms
10  be2718.ccr42.ord01.atlas.cogentco.com (154.54.7.129)  34.646 ms  35.821 ms  be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)  36.064 ms
11  be3470.rcr51.be22161-0.ord01.atlas.cogentco.com (154.54.1.102)  35.970 ms  37.515 ms  37.429 ms
12  38.142.191.18 (38.142.191.18)  35.693 ms  37.225 ms  37.147 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

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

```
(test@test)-[~]
$ curl -I ford.com
curl: (6) Could not resolve host: ford.com

(test@test)-[~]
$ curl -I ford.com
HTTP/1.0 302 Moved Temporarily
Location: https://ford.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0

(test@test)-[~]
$
```

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

```
(test@test)-[~]  
$ curl http://ford.com/images/  
  
(test@test)-[~]  
$
```

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

```
(test@test)-[~]  
$ ftp ford.com  
  
Trying 19.12.113.37:21 ...  
$
```

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](https://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](https://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