Cheatography

Configuration Testing Cheat Sheet

by binca via cheatography.com/44948/cs/13307/

Scanning with Nmap

Actively scans a target by sending packets to each port on a target and then based on the response reports whether the port is "open", "-closed" or "filtered"

Slow scans are less likely to be noticed

TCP SYN scans are stealthier than TCP connect scans since Nmap only sends a SYN packet and does not complete the TCP connection. While IDS detects these by default, alerts for this scan are often ignored.

Can perform OS (**-O**) detection with 2nd gen engine

Service version (**-sV**) detection enables Nmap to look at a banner, a "nudge" is sent if absent, and match responses to signatures in `nmap-service-probes`

Combined OS and service version detection using the **-A** flag.

Can define ports to be scanned or it will choose from default range.

The GUI of Nmap is **Zenmap**

Server Profiling

Identifying server software and versions can help guide attacks

Software serving hTTP, SSL support, type of virtual server, whether there is a load balancer.

Other sites may reside at the same IP address. Look at the host: header or pulling the default page can provide this information.

Note: Load balancers introduce complexity since some tie a session to a particular server. It is important to understand how the site implements persistence.

Server Version

Beyond web servers there are also database servers and client servers.

Server type and version can help determine vulnerability to attack and the methods.

Attempt to gather this information in multiple ways.

Software Configuration

Underlying server OS and network services.

Web server daemon configuration

Available features such as PHP, HTTP Request Methods

Presence of default pages

Netcat for Server and Method Detection

Netcat can be used to connect to a server to retrieve pages and inspect response data.

"X-Powered-By" and "Server" are very useful.

Header data may reveal server version although this data can be falsified.

Can manually or script HTTP commands into Netcat and send them to a host.

Bash cscript to iterate through HTTP Methods

```
#!/bin/bash
for method in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "$method / HTTP/1.1\r\nHost: domain\r\n\r\n"
| nc domain 80
done
```

HTTP Request Methods of Interest to Testers

PUT	Place files on server
DELETE	Removing files
CONNECT	Tunnel with HTTP
TRACE	Echo request as seen by server, including changes made by intermediary servers
OPTIONS	List supported methods

Several tools can identify HTTP request methods available.

Default Pages

Sign of poor management

Can be used to identify server software

Documentation is commonly left on servers

Try to access via IP address instead of hostname, this bypasses name-based virtual hosting

Many tools can discover default pages, Nikto is particularly great.

Nikto

Perl program uses "database" of items to scan for on server including comparing favicon.ico files (MD5 hashed)

Contains widely used server-side scripts and programs known to be vulnerable response strings from servers

Discovers default pages

May produce false positives due to how missing pages are handled

Syntax: `nikto -h [hostname]`