Web Application Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

Fingerprinting the web server

Fingerprinting

- ✓ Web server fingerprinting is the task of identifying the type and version of web server that a target is running on.
- ✓ While web server fingerprinting is often encapsulated in automated testing tools, it is important for researchers to understand the fundamentals of how these tools attempt to identify software, and why this is useful.

Fingerprinting

- ✓ Accurately discovering the type of web server that an application runs on can enable security testers to determine if the application is vulnerable to attack.
- ✓ In particular, servers running older versions of software without up-to-date security patches can be susceptible to known version-specific exploits.

Fingerprinting

- ✓ Accurately discovering the type of web server that an application runs on can enable security testers to determine if the application is vulnerable to attack.
- ✓ In particular, servers running older versions of software without up-to-date security patches can be susceptible to known version-specific exploits.

Test Objectives

- ✓ Determine the version and type of a running web server to enable further discovery of any known vulnerabilities.

- ✓ Techniques used for web server fingerprinting include banner grabbing, eliciting responses to malformed requests, and using automated tools to perform more robust scans that use a combination of tactics.
- ✓ The fundamental premise on which all these techniques operate is the same.

- ✓ They all strive to elicit some response from the web server which can then be compared to a database of known responses and behaviors, and thus matched to a known server type.

- ✓ Telnet nfsu.ac.in 80

  GET HTTP/1.0

Telnet is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the internet). Using telnet client software on your computer, you can make a connection to a telnet server (that is, the remote host).

NetCat

- ✓ Netcat is one of the most versatile networking tools for system administrators – it is called the Swiss army knife of Networking.
- ✓ This tool can be used for creating any connections over TCP or UDP protocol which makes it an excellent debugging tool. It helps the user investigate connections directly by connecting to them.

NetCat

- ✓ Netcat can also perform port scanning, file transfer, and sometimes it might be used by the hackers or penetration testers for creating a backdoor into a system.

- ✓ nc –v nfsu.ac.in 80

  GET /POST/ HEAD/DELETE/OPTIONS HTTP/1.0

  press enter

Or

- ✓ nc –v nfsu.ac.in 80

  GET /POST/ HEAD/DELETE/OPTIONS HTTP/1.1

  press enter

Or

- ✓ nc –v nfsu.ac.in 80

  GET /POST/ HEAD/DELETE/OPTIONS SANTA CLOUS/1.1

  press enter

- httprint is a web server fingerprinting tool.
- It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. httprint can also be used to detect web enabled devices which do not have a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings and it is very easy to add signatures to the signature database.

- httprint -h <host> -s signatures.txt
- Httprint –h www.net-square.com –s usr/share/httpring/signatures.txt

*if error comes that signature file or corrupted signature file the download the signature file from

https://net-square.com/httprint.html

- Download : from
- Screenshots and reports : Download - signatures.txt
- And replace downloaded signatures.txt the same at /usr/share/httprint/
- And try again

HTTPrint - Windows

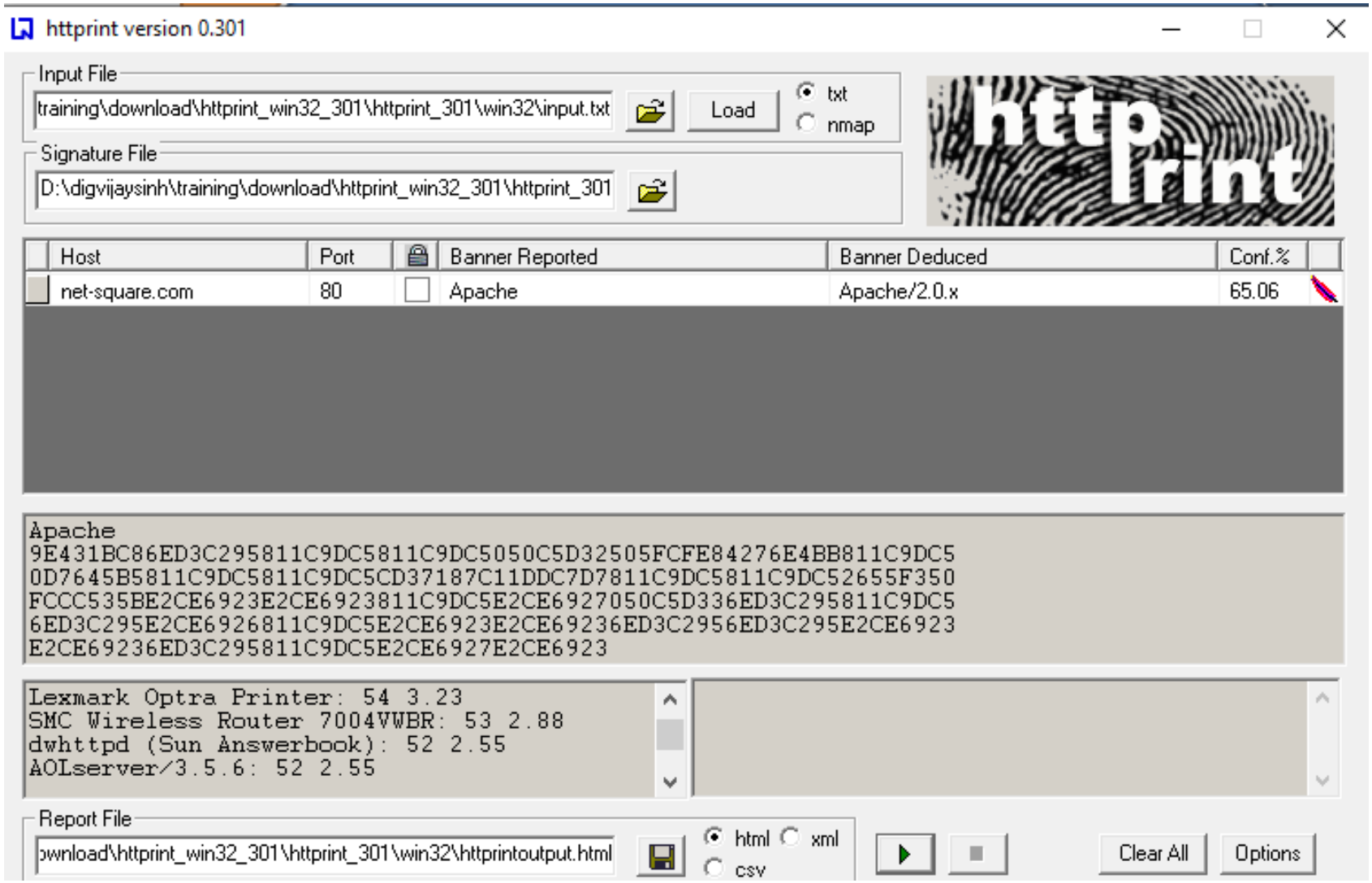
- For windows and GUI
- Download the HTTprint GUI version from
- https://net-square.com/httprint.html and download the Win32 GUI and cmd line version
- Unzip and start GUI using httprint_gui.exe
- It has input.txt file available in the httprint_win32_301\httprint_301\win32
- Provide the name of the sites for which you would like to perform fingerprinting

- # inputs for httprint can be:# - individual IP addresses (default port 80)# - http://servername:[port]/# - https://servername:[port]/# - IP ranges xx.xx.xx.xx-yy.yy.yy.yy#

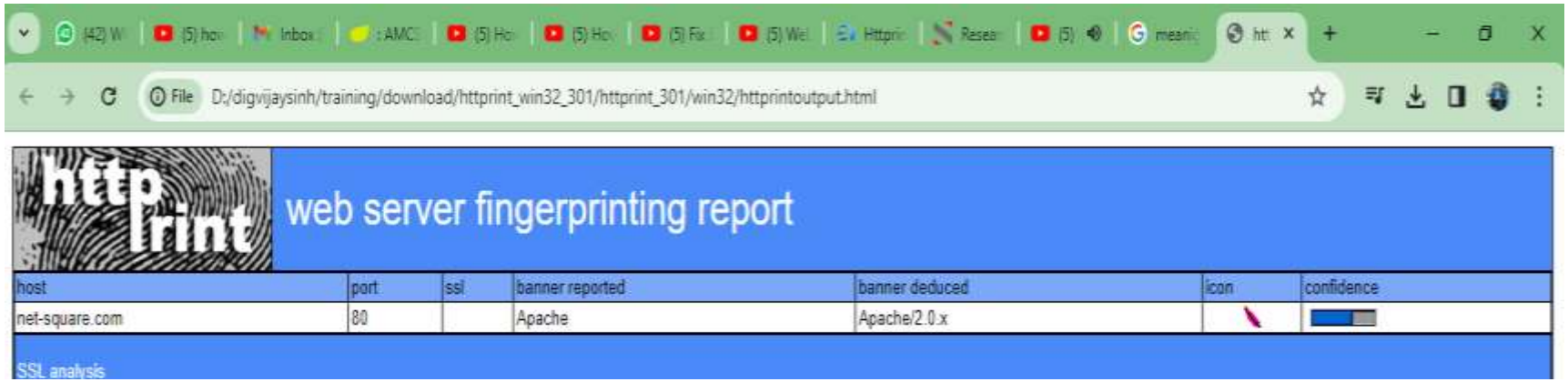
http://net-square.com

- and load the file if you want you can provide the nmap file output also
- Chose the report type : xml or html or csv
- Report will be generated in the same directory

HTTPrint - Windows



HTTPrint – Report



Recon-ng

- Recon-ng is a powerful open-source tool used for reconnaissance, also known as information gathering, in the realm of cybersecurity.
- Developed by Tim Tomes, recon-ng is designed to aid security professionals, penetration testers, and ethical hackers in collecting, organizing, and analyzing data about potential targets. It provides a modular framework that allows users to extend its functionality through the addition of custom modules, making it highly versatile and adaptable to various scenarios.

Recon-ng -Key Features:

- Modular Architecture: Recon-ng is built on a modular architecture, allowing users to easily extend its capabilities by adding custom modules. These modules enable reconnaissance across different platforms and services, including social media, domain information, network infrastructure, and more.
- Automated Information Gathering: Recon-ng automates the process of information gathering, saving time and effort for security professionals. It retrieves data from various sources such as public databases, search engines, and social media platforms, providing comprehensive insights into potential targets.

Recon-ng -Key Features:

- Data Organization and Analysis: The tool organizes the collected data into a structured format, making it easier for users to analyze and interpret the information effectively. This structured approach enhances the reconnaissance process and facilitates informed decision-making during security assessments.
- Integration with Other Tools: Recon-ng can be integrated with other cybersecurity tools and frameworks, enhancing its functionality and interoperability within complex security environments. Integration with tools like Metasploit and Maltego enables seamless collaboration and workflow automation.

Recon-ng -Key Features:

- Command-Line Interface (CLI): Recon-ng features a command-line interface that offers flexibility and control over the reconnaissance process. Users can execute commands, load modules, and manage the reconnaissance workflow efficiently through the CLI, making it suitable for both novice and experienced security professionals.
- Extensive Documentation and Community Support: Recon-ng benefits from extensive documentation and a supportive community of security professionals and developers. Users can find resources, tutorials, and guidance to effectively utilize the tool and address any challenges they encounter during reconnaissance activities.

Recon-ng -Typical Use Cases:

- Penetration Testing: Security professionals use recon-ng during penetration testing engagements to gather intelligence about target systems, networks, and organizations. The tool helps identify potential vulnerabilities and assess the security posture of the target environment.
- Vulnerability Assessment: Recon-ng aids in conducting comprehensive vulnerability assessments by collecting information about systems, services, and infrastructure components. This data assists in identifying potential security weaknesses and prioritizing remediation efforts.

Recon-ng -Typical Use Cases:

- Threat Intelligence Gathering: Organizations leverage recon-ng to gather threat intelligence and monitor for potential security threats and indicators of compromise (IOCs). By analyzing data from various sources, security teams can stay informed about emerging threats and take proactive measures to mitigate risks.
- Digital Footprint Analysis: Recon-ng enables organizations to analyze their digital footprint and understand how they are perceived online. By collecting data from social media platforms, websites, and public databases, businesses can assess their online presence and address any privacy or security concerns.

Recon-ng -Typical Use Cases:

- Competitive Intelligence: Companies may use recon-ng to gather competitive intelligence by monitoring competitors' online activities, analyzing their digital footprint, and identifying potential strategic advantages or vulnerabilities.

- **recon/domains-hosts/hackertarget - Module**
- Recon-ng: show
- Marketplace search
- Marketplace search search-keywork

  Example: Marketplace search hacker

  Check status is installed or non installed

  If it is non-installed then
- Marketplace install recon/domains-hosts/hackertarget

  to load the module
- Modules load hackertarget

[hackertareget]> info

- [hackertareget]> show

this will provide the name of the framework which will store to scanning results i.e., host framework item will store the host details of the harckertarget modules scanning result.

- [hackertareget]> options set source rapid7.com
- [hackertareget]> source -> repid7.com
- [hackertareget]> input
- [hackertareget]> run
- [hackertareget]> show hosts

Recon-ng -Command

- [hackertareget]> db
- [hackertareget]> db delete hosts

  rowids (INT): enter the no of raw of hosts
- [hackertareget]> show hosts

Recon-ng -Command

- **recon/domains-hosts/netcraft**
- Marketplace install recon/domains-hosts/netcraft
- Module load recon/domains-hosts/netcraft
- [netcraft] > info
- Options set source nfsu.ac.in
- Input
- Run
- show

- **recon/domains-hosts/brute_hosts**
- Marketplace install recon/domains-hosts/brute_hosts
- Module load recon/domains-hosts/brute_hosts [netcraft] > info
- Options set source nfsu.ac.in
- Input
- Run
- show hosts

- **doscovery/info_disclosure/interesting_files**
- Marketplace install doscovery/info_disclosure/interesting_files
- Module load doscovery/info_disclosure/interesting_files
- [netcraft] > info
- Options set source nfsu.ac.in
- Input
- Run
- Show hosts

References

- ✓ https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server
- ✓ https://nooblinux.com/how-to-use-netcat/

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in