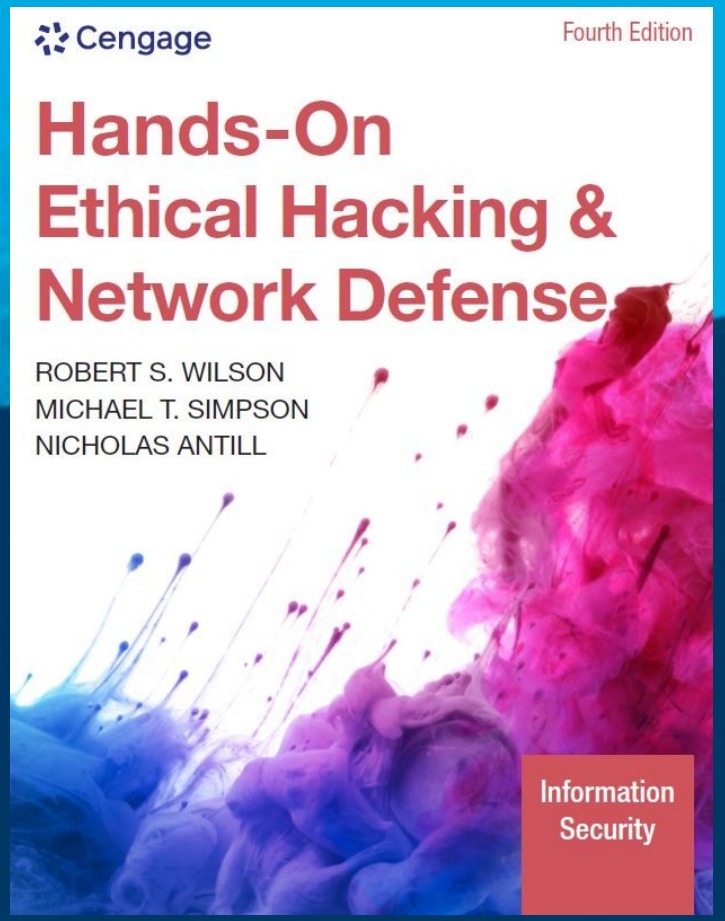


Hands-On Ethical Hacking and Network Defense, Edition 4

Module 4: Footprinting and Social Engineering

CENGAGE

Using Web Tools for Footprinting (1 of 4)

- Many attackers do “case the joint”
  - Look over the location
  - Find weaknesses in security systems
  - Determine what types of locks and alarm systems are used
- As a security tester
  - You must find out as much as you can about an organization that hired you
- **Footprinting** (may also be called reconnaissance)
  - Finding information on a company’s network
  - Passive and nonintrusive

Using Web Tools for Footprinting (2 of 4)

- Active footprinting
  - Actually, prodding the target network in ways that might seem suspicious to network defenders
  - Includes things such as:
    - Port scans
    - DNS zone transfers
    - Interacting with a target's web server
- Security tester uses both passive and active techniques
  - To discover as much as possible about the organization and its network

Summary of Reconnaissance Tools (1 of 4)

Tool	Function
`dig` (Command available on all *nix systems; can be downloaded for Windows platforms from the BIND 9 website. `dig` is contained in the BIND download, so download BIND.)	Perform DNS zone transfers; replaces the `nslookup` command.
Domain Dossier	This web tool is useful in gathering IP and domain information (including whois, DNS, and traceroute).
FOCA	Extract metadata from documents on websites to reveal the document creator's network logon and email address, information on IP addresses of internal devices, and more.
Google and Google Hacking Database (GHDB), also called Google Dorks	Uncover files, systems, sites, and other information about a target using advanced operators and specially crafted queries. Some of these queries can be found at the GHDB (Google Hacking Database).
Google Groups	Search for email addresses in technical or nontechnical

Summary of Reconnaissance Tools (2 of 4)

Tool	Function
Maltego	Discover relevant files, email addresses, and other important information with this powerful graphic user interface (GUI) tool.
`netcat` (command available on all *nix systems; can be downloaded for Windows platforms from the N MAP website)	Read and write data to ports over a network.
Netcraft Site Report	Uncover the underlying technologies that a website operates on.
OSINT Framework	A collection of OSINT tools presented in an interactive web-based mind map that organizes the information visually. You can expand nodes to find collections of tools suited for the task you want to accomplish.

Summary of Reconnaissance Tools (3 of 4)

Tool	Function
SpiderFoot	A tool with a graphical user interface (GUI) that queries more than 100 OSINT sources to grab intelligence on email addresses names, IP addresses, domain names, web servers, and more.
Spyse	Spyse is a cybersecurity search engine. You can use it to search entire domains or individual systems for vulnerabilities, IPs, DNS records, domains, and more. Spyse claims to be "the most complete Internet assets registry for every cybersecurity professional."
TheHarvester	Used for finding email addresses, subdomains, IPs, URLs, employee names, and more. This is a command line only tool.
WayBackMachine	Search through previous versions of the website to uncover historical information about a target.

Summary of Reconnaissance Tools (4 of 4)

Tool	Function
`wget` (command available on all *nix systems; can be downloaded for Windows platforms from Wget for Windows HTML site)	Retrieve HTTP, HTTPS, and FTP files over the Internet.
White Pages	Conduct reverse phone number lookups and retrieve address information.
Whois	Gather IP and domain information.
Zed Attack Proxy	This is a useful website analysis tool that can crawl through remote websites and even produce a list of vulnerabilities for a remote website.

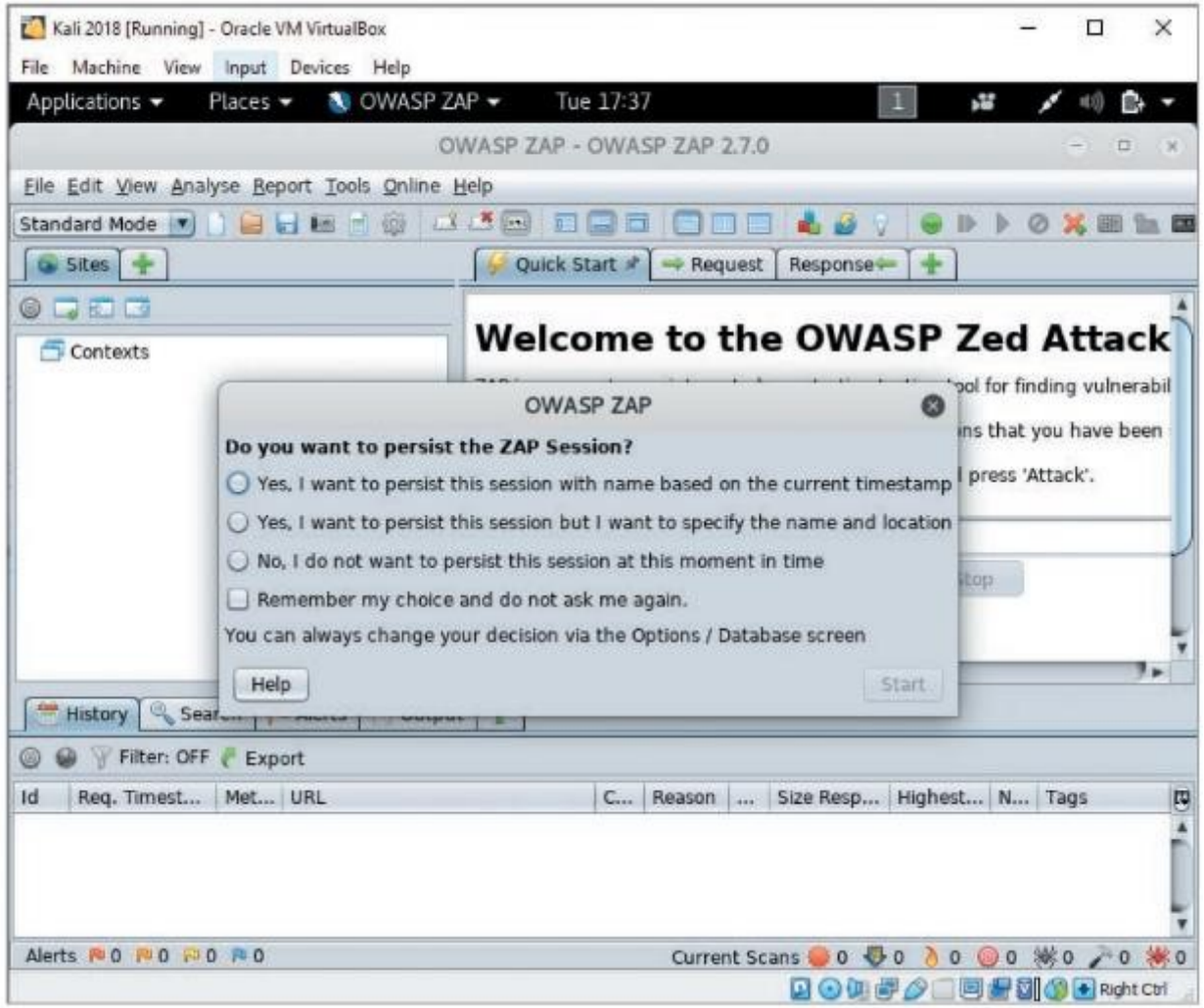
Conducting Competitive Intelligence

- Numerous resources are available to find information legally
  - **Competitive intelligence**
    - Gathering information on a higher level using technology
- Security professionals must:
  - Explain to their clients the methods used by competitors to gather confidential information

Analyzing a Company's Website (1 of 8)

- Webpages are an easy source of critical information
  - Websites are often referred to as web applications
- Many available tools for this type of information gathering
  - Zed Attack Proxy (ZAP)
    - Powerful tool for Linux, macOS, and Windows
    - Requires Java to be installed

Analyzing a Company's Website (2 of 8)



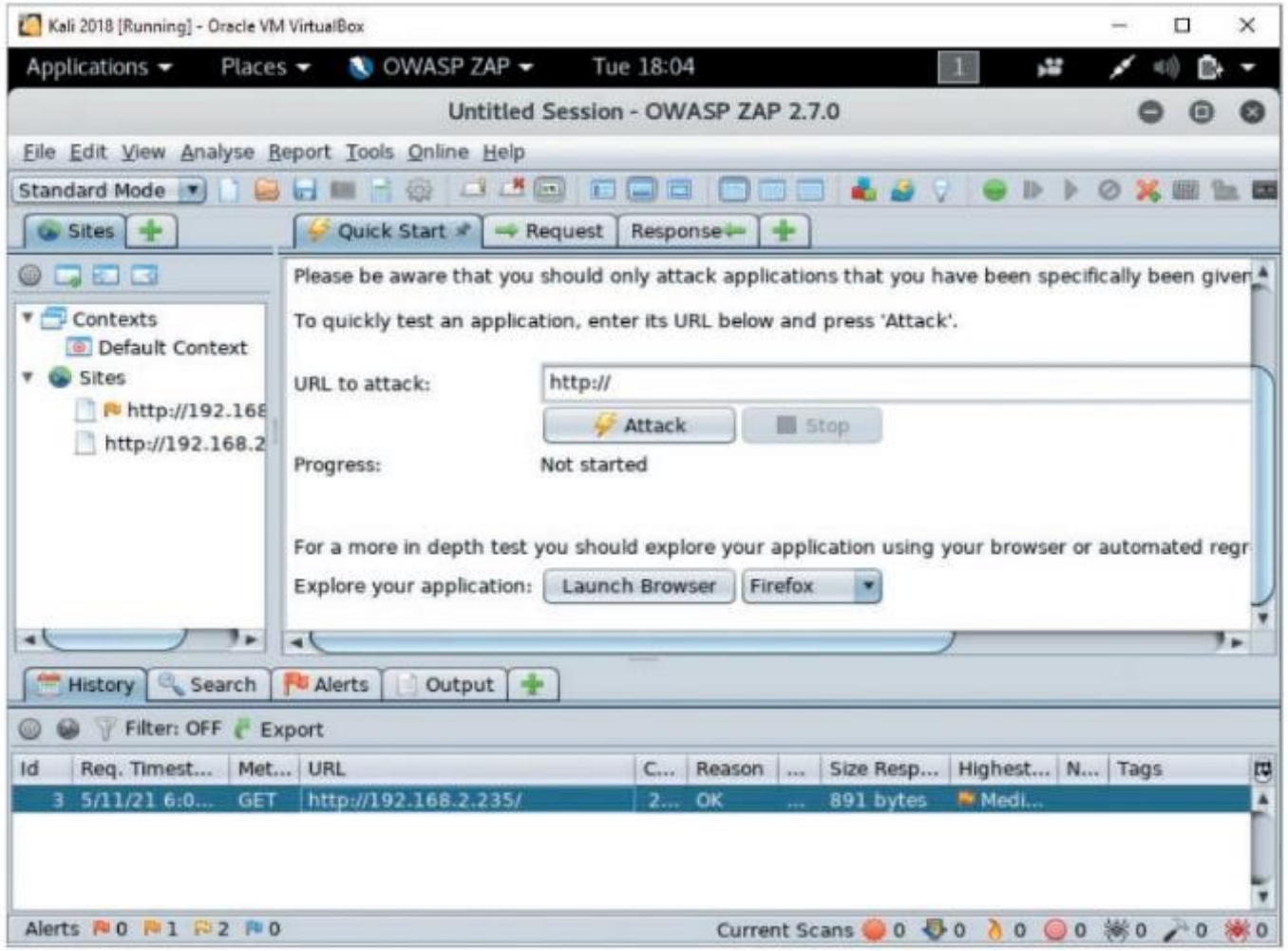
Source: OWASP.ORG

Figure 4-1 ZAP main window

Analyzing a Company's Website (3 of 8)

- ZAP has a feature called Launch Browser on its Quick Start tab
  - Automatically edits the configuration of a web browser
    - To direct traffic through ZAP proxy
  - Allows the ZAP tool to intercept and manipulate traffic sent between your web browser and the target web server
  - To use this feature:
    - Select the Quick Start tab
    - Choose the browser from the drop-down menu
      - Next to the Launch Browser button
    - Click the Launch Browser button

Analyzing a Company's Website (4 of 8)



Source OWASP.ORG

Figure 4-2 ZAP launch browser

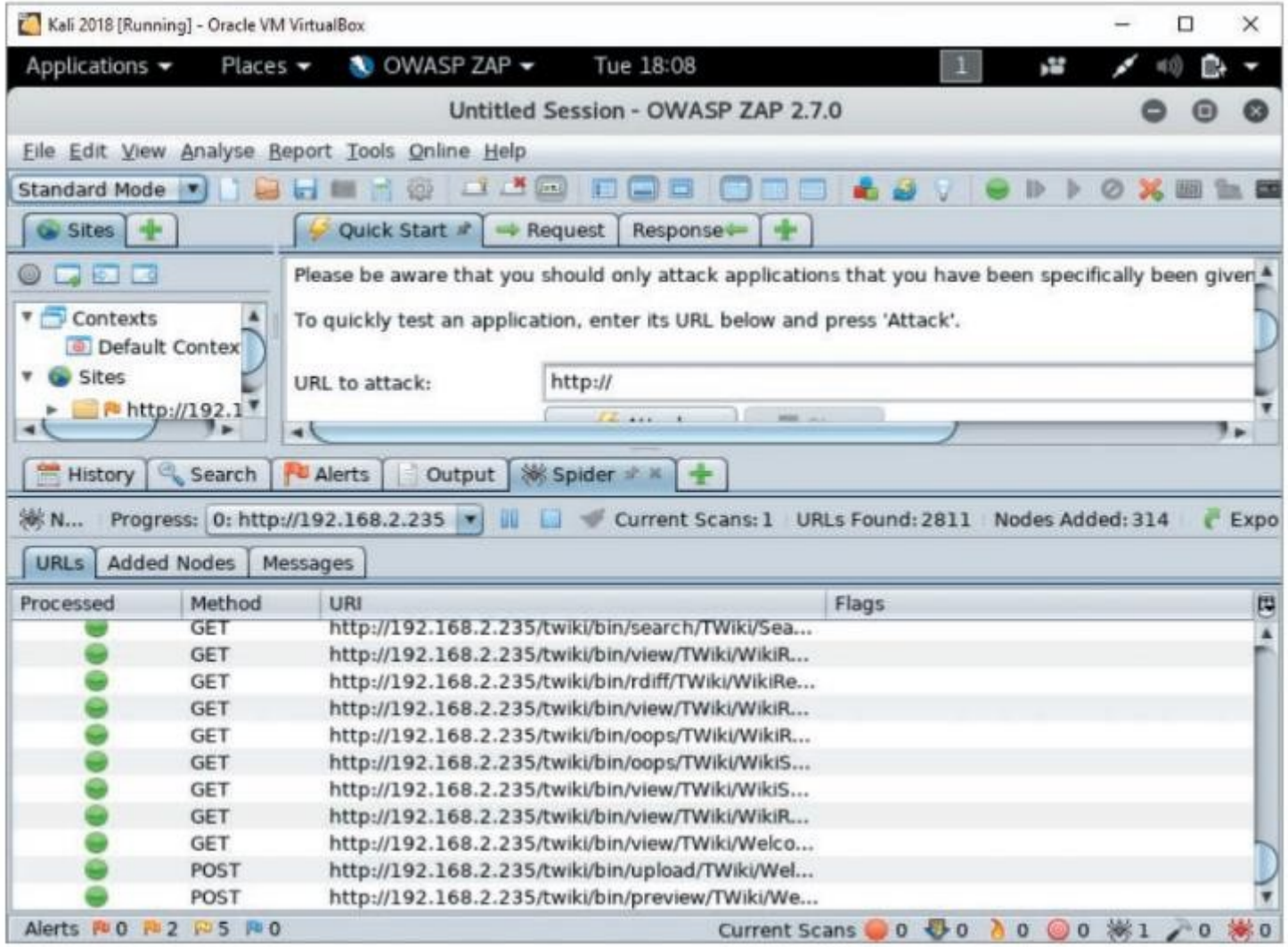
Analyzing a Company's Website (5 of 8)

- Once the browser is configured:
  - The attacker can use the browser to navigate the target site
  - Target site will be listed on the History tab in the lower pane and in the Sites list in the left pane
  - Site can be selected for **spidering**
    - Spidering (or crawling) is an automated way to discover pages of a website by following links
    - Within seconds, the filenames of webpages on the "spidered" site are displayed on the URLs tab

Analyzing a Company's Website (6 of 8)

- After the site has been "spidered":
  - You can actively scan the site using the ZAP Attack feature
    - Sends the web server a series of requests designed to identify vulnerabilities
    - Vulnerabilities will display under the Alerts tab
      - Indicated in the Risk Level column as either High, Medium, Low, or Informational

Analyzing a Company's Website (7 of 8)



Source OWASP.ORG

Figure 4-5 Displaying filenames of content on a website

Analyzing a Company's Website (8 of 8)

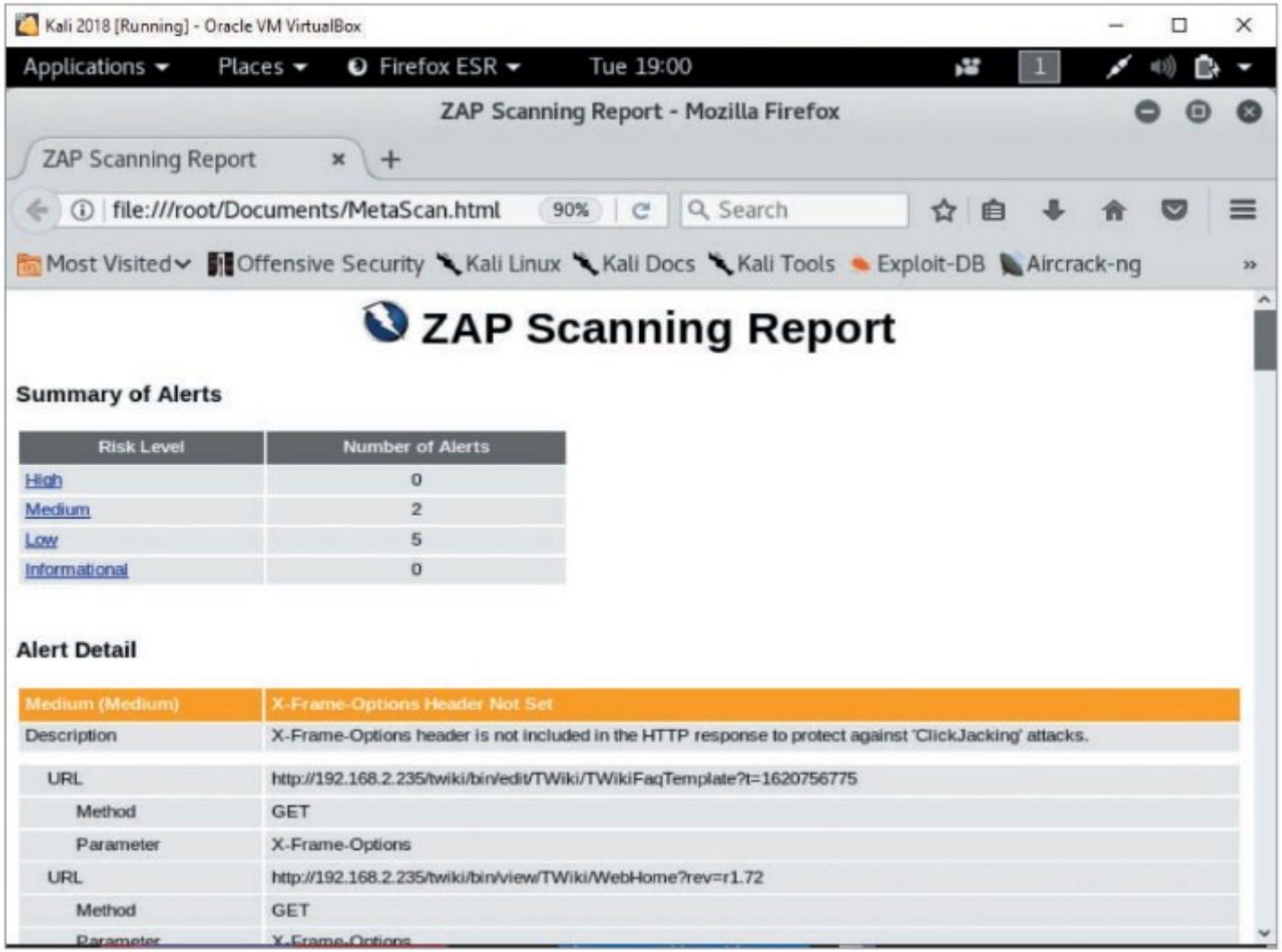


Figure 4-6 ZAP scanning report

Using Other Footprinting Tools

- Whois utility
  - Commonly used web tool
  - Gathers IP address and domain information
  - Unfortunately, attackers can also use this information
  - Gives information on a company's IP addresses
    - And any other domains the company might be part of

Using Email Addresses

- Email address
  - Knowing a user's email address can help retrieve even more information
- Find out a company's email address format
  - You might be able to find other employees' email accounts
    - By acquiring a company phone directory
    - By searching the Internet for any @companyname.com references
- Tool to find corporate employee information
  - Groups

Using HTTP Basics (1 of 3)

- HTTP operates on port 80 and HTTPS operates on port 443
  - Both versions use HTTP commands
  - Security testers can pull information from a web server using these commands
- A basic understanding of HTTP
  - Beneficial for security testers
- Return codes
  - Reveal information about OS used on the computer where a security test is being conducted
- Most basic HTTP method
  - `GET / HTTP/1.1.`

HTTP Client Errors (1 of 2)

Error	Description
400 Bad Request	Request not understood by server
401 Unauthorized	Request requires authentication
402 Payment Required	Reserved for future use
403 Forbidden	Server understands the request but refuses to comply
404 Not Found	Unable to match request
405 Method Not Allowed (Note: Methods are covered later in this module.)	Request not allowed for the resource
406 Not Acceptable	Resource doesn't accept the request
407 Proxy Authentication Required	Client must authenticate with proxy
408 Request Timeout	Request not made by client in allotted time
409 Conflict	Request couldn't be completed because of an inconsistency

HTTP Client Errors (2 of 2)

Error	Description
410 Gone	Resource is no longer available
411 Length Required	Content length not defined
412 Precondition Failed	Request header fields evaluated as false
413 Request Entity Too Large	Request is larger in volume than the server can process
414 Request-URI (uniform resource identifier) Too Long	Request-URI is longer than the server is willing to accept

HTTP Server Errors

Error	Description
500 Internal Server Error	Request couldn’t be fulfilled by the server
501 Not Implemented	Server doesn’t support the request
502 Bad Gateway	Server received invalid response from the upstream server
504 Gateway Timeout	Server didn’t receive a timely response
505 HTTP Version Not Supported	HTTP version not supported by the server

HTTP Methods

Error	Description
GET	Retrieves data by URI
HEAD	Same as the GET method, but retrieves only the header information of an HTML document, not the document body
OPTIONS	Requests information on available options
TRACE	Starts a remote Application-layer loopback of the request message
CONNECT	Used with a proxy that can dynamically switch to a tunnel connection, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS)
DELETE	Requests that the origin server delete the identified resource
PUT	Requests that the entity be stored under the Request-URI
POST	Allows data to be posted (i.e., sent to a web server)

Using HTTP Basics (2 of 3)

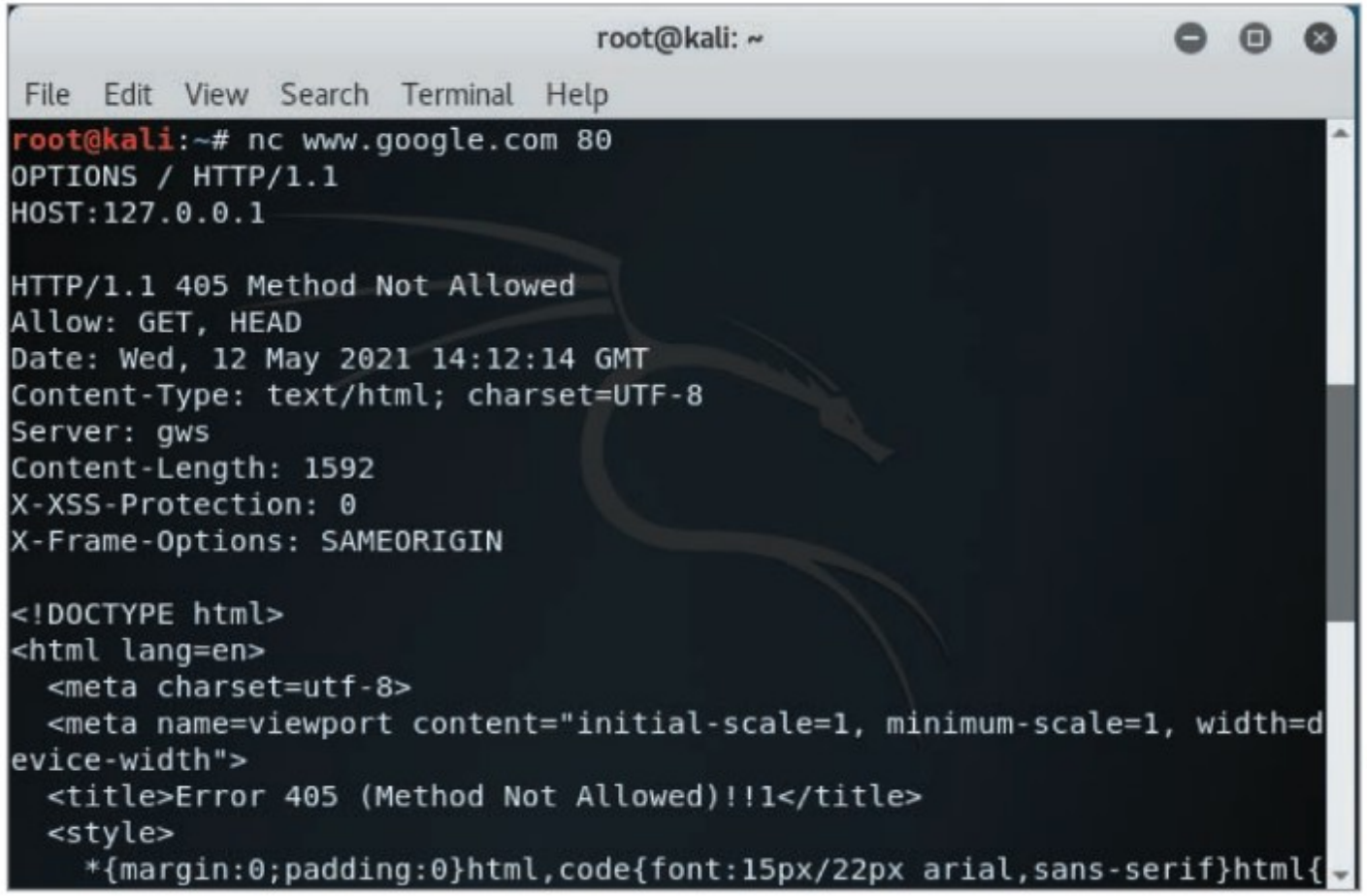


Figure 4-8 Using the OPTIONS HTTP method

Using HTTP Basics (3 of 3)

- If you know HTTP methods:
  - You can send a request to a web server
    - From the generated output, you can determine what OS the web server is using
- Other information can be determined that could be used in an attack
  - Such as vulnerabilities of operating systems (OSs) and other software

Other Methods of Gathering Information

- With just a URL, you can determine the following that a company is using:
  - Web server
  - OS
  - Names of IT personnel
- Other unscrupulous methods:
  - Cookies
  - Web beacons

Detecting Cookies and Web Bugs (1 of 2)

- **Cookie**
  - Text file generated by a web server
  - Stored on a user's browser
  - Information is sent to the web server when the user returns to the website
  - Used to customize webpages
  - Some cookies cause security issues
    - Unscrupulous people might store personal information
    - Can be used to attack a computer or server

Detecting Cookies and Web Bugs (2 of 2)

- **Web bug**
  - 1-pixel ×1-pixel image file
  - Referenced in an <IMG> tag
  - Usually works with a cookie
  - Type of **web beacon**
    - A hidden graphic or piece of code
      - Embedded in a webpage to track user activity and harvest user information
  - Purpose is similar to spyware and adware
  - Comes from third-party companies specializing in data collection
  - Usually match the color of the webpage's background
    - Renders them invisible

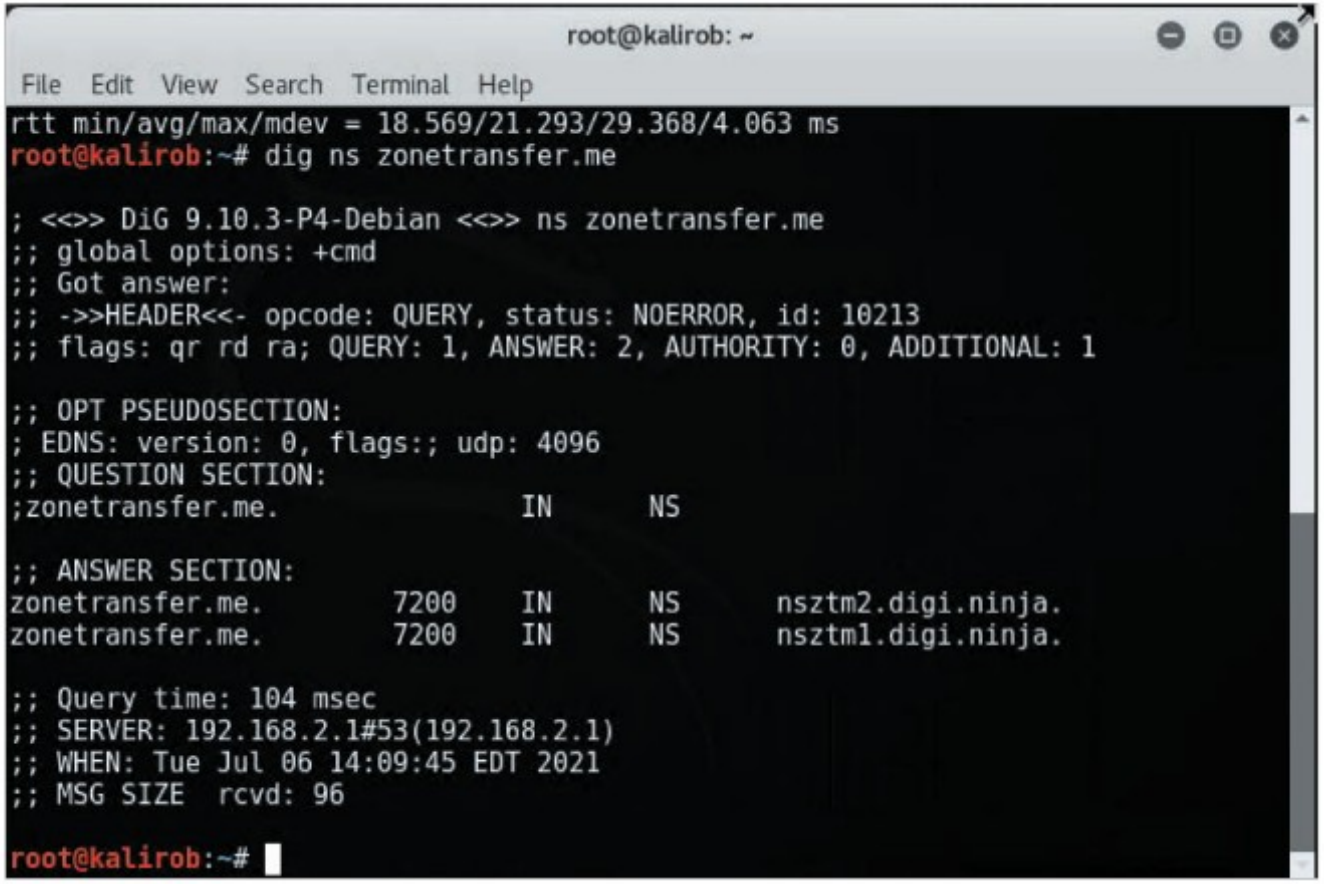
Using Domain Name System Zone Transfers (1 of 3)

- Domain Name System (DNS)
  - Resolves host names to IP addresses and vice versa
  - People prefer URLs to IP addresses
  - DNS is a major area of potential vulnerability for network attacks
    - Uses name servers to resolve names
    - Once you determine what name server a company is using:
      - You can attempt to transfer all the records for which the DNS server is responsible
      - Process is called a **zone transfer**
      - Can be done with the `dig` command

Using Domain Name System Zone Transfers (2 of 3)

- Recommended zone transfer tool
  - The `dig` command
- Determining primary DNS server
  - Start of Authority (S O A) record
    - Shows for which zones or IP addresses the DNS server is responsible
  - Zone transfer gives an organization's network diagram
    - This information can be used to attack other servers or computers that are part of the network infrastructure

Using Domain Name System Zone Transfers (3 of 3)



Source: Kali Linux

Figure 4-14 Using the dig command

Introduction to Social Engineering (1 of 3)

- **Social engineering**: Uses the art of deception to extract valuable information
  - From well-meaning people who are trying to be helpful
  - Art of social engineering is older than computers
  - Uses knowledge of human nature to gather information from people
- Goals
  - Obtain confidential information (passwords)
  - Obtain other personal information
- Tactics used by social engineers
  - Persuasion
  - Intimidation
  - Coercion
  - Extortion/blackmailing

Introduction to Social Engineering (2 of 3)

- Social engineers
  - Probably the biggest security threat to networks
  - The most difficult to protect against
- Main idea
  - “Why try to crack a password when you can simply ask for it?”
    - Users divulge passwords to IT personnel
- Social engineers study human behavior
  - Create a sense of urgency to remain cordial
  - They recognize personality traits
  - Understand how to read body language
  - Can read a person’s tone of voice for clues

Introduction to Social Engineering (3 of 3)

- Techniques to gain information from unsuspecting people
  - Urgency
  - Quid pro quo
  - Status quo
  - Kindness
  - Position
- Security training
  - Train users not to reveal information to outsiders about OSs
  - Employees should confirm identity of the person asking questions
    - Routinely ask the person for a company phone number to call back

The Art of Shoulder Surfing (1 of 2)

- Shoulder surfer
  - Reads what users enter on keyboards
    - Logon names
    - Passwords
    - PINs
- Tools used by shoulder surfers
  - Memorize key positions and typing techniques
  - Know popular letter substitutions
    - $ equals s, @ equals a

The Art of Shoulder Surfing (2 of 2)

- Prevention
  - Avoid typing when:
    - Someone is nearby
    - Someone nearby is talking on cell phone
  - Ensure display screens face away from the door
  - Immediately change password
    - If you suspect someone might have observed you entering your password

The Art of Dumpster Diving (1 of 2)

- Attacker finds information in victim's trash
  - Discarded computer manuals
  - Passwords jotted down
  - Company phone directories
  - Calendars with schedules
  - Financial reports
  - Interoffice memos
  - Company policy
  - Utility bills
  - Resumes

The Art of Dumpster Diving (2 of 2)

- Prevention
  - Educate users
    - The possibility of dumpster diving
    - Proper trash disposal
  - Format disks before disposing them with “disk-cleaning” software that writes binary zeros on all portions of the disks
    - Should be done at least seven times
  - Discard old computer manuals offsite
  - Shred documents before disposal

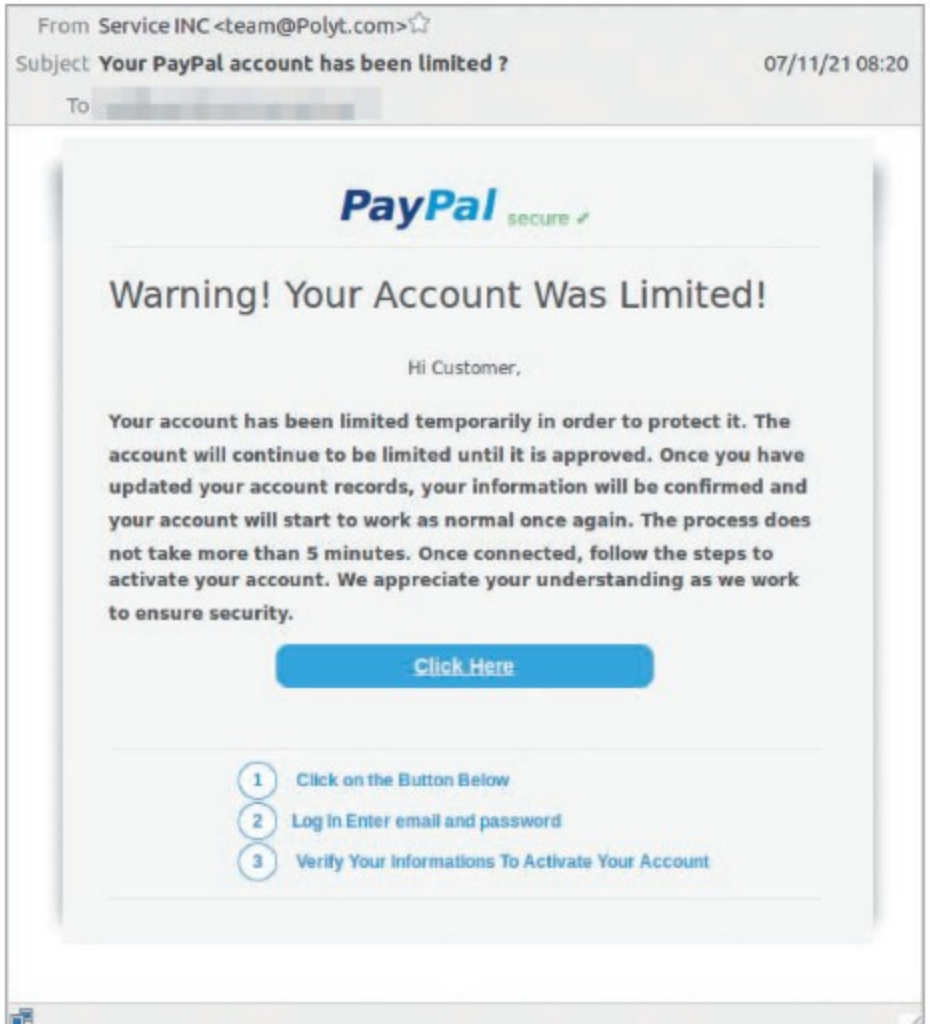
The Art of Piggybacking

- Trailing closely behind an employee cleared to enter restricted areas
- How it works:
  - Watch authorized personnel enter an area
  - Quickly join them at security entrance
  - Exploit desire to be polite and helpful
  - Attacker wears a fake badge or security card
- Prevention
  - Use turnstiles
  - Train personnel to notify security about strangers
  - Do not hold secured doors open for anyone
    - Even people you know
  - All employees must use access cards to enter a restricted area

Phishing (1 of 2)

- **Phishing** emails
  - “Update your account details” is a typical subject line
  - Usually framed as an urgent request to visit a website
    - The website is a fake
    - The money you lose is real
- **Spear phishing**
  - Combines social engineering with exploiting vulnerabilities
  - Attack is directed at specific people in an organization
    - Comes from someone the recipient knows
    - Mentions topics of mutual interest

Phishing (2 of 2)



mailguard.com.au

Figure 4-15 Phishing email message