Footprinting & Social Engineering

By: Melissa Genovese

May 2, 2022

https://www.freepik.com/vectors/safe-money Safe money vector created by vectorpocket - www.freepik.com

Footprinting

Just like bank robbers would scout a place before committing a crime to get a full picture (to minimize chances of being caught) so should we get a full picture of an organizations network to understand any vulnerabilities.

Some things to keep in mind:

- The word “reconnaissance” could also be heard in place of “footprinting.”
- Passive footprinting is legal information gathering.
- Active reconnaissance will likely get you noticed as it can include DNS zone transfers, interacting with web servers, and port scans.

https://www.freepik.com/vectors/internet created by vectorjuice - www.freepik.com

OSINT (Open Source Intelligence) Tools

Free and open source- a few of my favorites:

Tool	Function
FOCA www.elevenpaths.com/labstools/foca/index.html	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.
Maltego www.maltego.com	Discover relevant files, email addresses, and other important information with this powerful graphic user interface (GUI) tool.
Netcraft Site Report https://sitereport.netcraft.com	Uncover the underlying technologies that a website operates on.
WayBackMachine https://archive.org/web	Search through previous versions of the website to uncover historical information about a target.

Did you know?

- That the Department of Defense (DoD) employees are trained to look out for terrorists' groups specifically looking for information on them. These groups gather tiny bits of intelligence to create a larger picture through rather simple means of:

  - Facebook
  - LinkedIn
  - Twitter
  - Other social media accounts

https://www.freepik.com/vectors/hacker-hacking Hacker hacking vector created by freepik - www.freepik.com

Competitive Intelligence

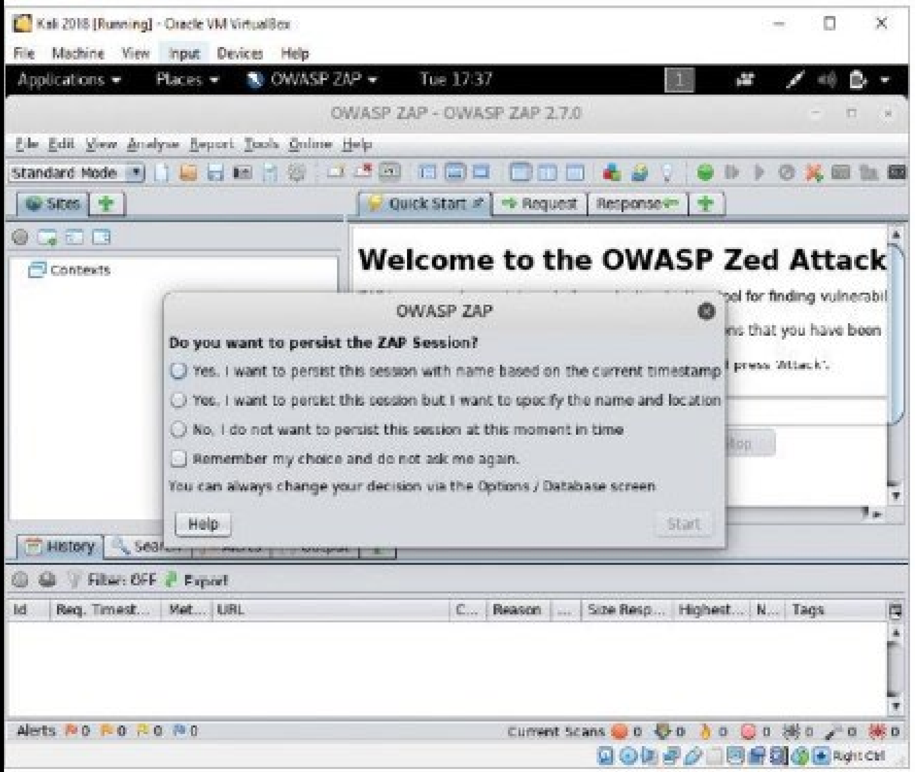
- A practice that companies have been doing for a long time.
- As a security professional, you should be able to tell an organization what their competitors can gather from them so they can limit what is made public. This keeps information private and confidential.

Analyzing a Company's Website

- An attack usually starts on a company's website, which is an easy info grab.
- Websites are called web applications.
- Web applications are programs that reside on web servers.
- A website is a program.
- Many free tools are available for Linux, macOS, and windows to gather information about a company's website.
- ** WARNING ** Only scan websites when you have explicit permission, as it is an attack.

Zed Attack Proxy (ZAP)

- An HTTP proxy that processes HTTP requests between the browser and the user.
- Can be downloaded for free at www.zaproxy.org.
- A tool to gather information about a companies and any potential vulnerabilities.
- You can download a virtual box appliance called Metasploitable2 and is intended as a target for a scan https://sourceforge.net/projects/metasploitable/files/Metasploitable2.
- Need to have java downloaded www.java.com.


Kali 2018 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places OWASP ZAP Tue 17:37
OWASP ZAP - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
History
Sear
Filter: OFF
Export
Id
Req. Timest...
Met...
URL
C...
Reason
...
Size Resp...
Highest...
N...
Tags
Alerts 0 0 0 0
Current Scans 0 0 0 0 0 0 0
Right Ctrl
Help
Start

Welcome to the OWASP Zed Attack

OWASP ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

○ No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

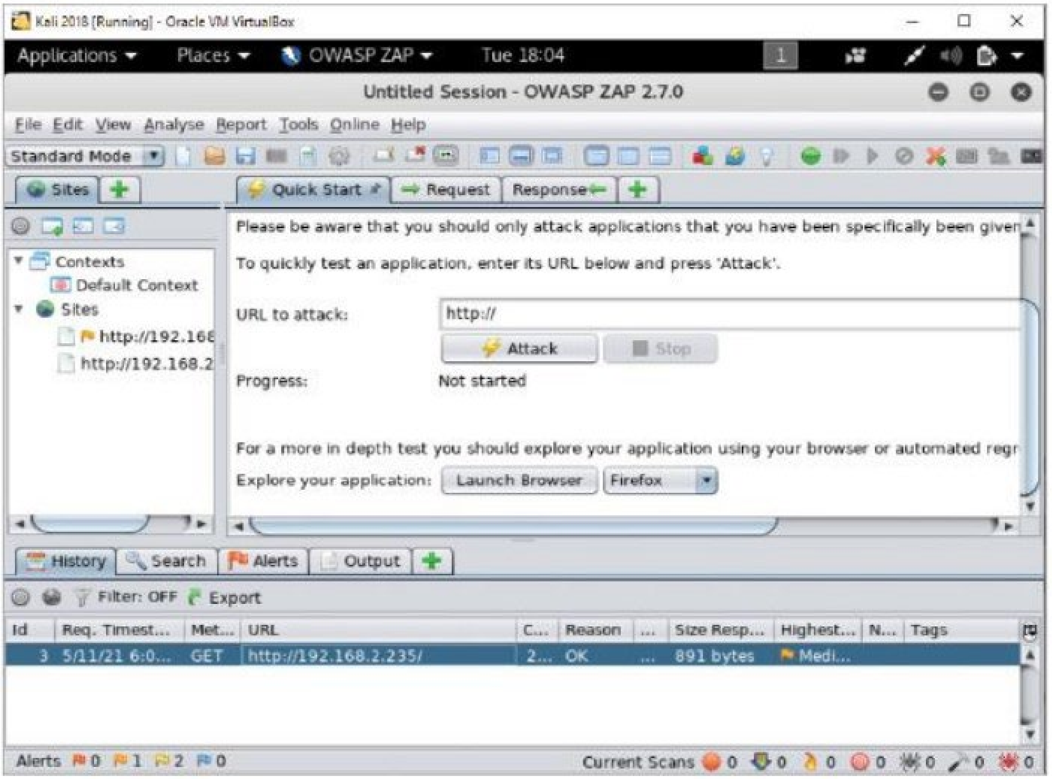
Source: OWASP.ORG

ZAP main window

Zed Attack Proxy (ZAP)

- ZAP has a feature, “Launch Browser” on Quick Start tab that configures for browser traffic to direct to ZAP proxy.

- To launch feature, select Quick Start tab, choose the browser you want to use from drop-down menu (next to Launch Browser button) then click on Launch Browser button.



Please be aware that you should only attack applications that you have been specifically been given

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regr

Explore your application: Launch Browser Firefox

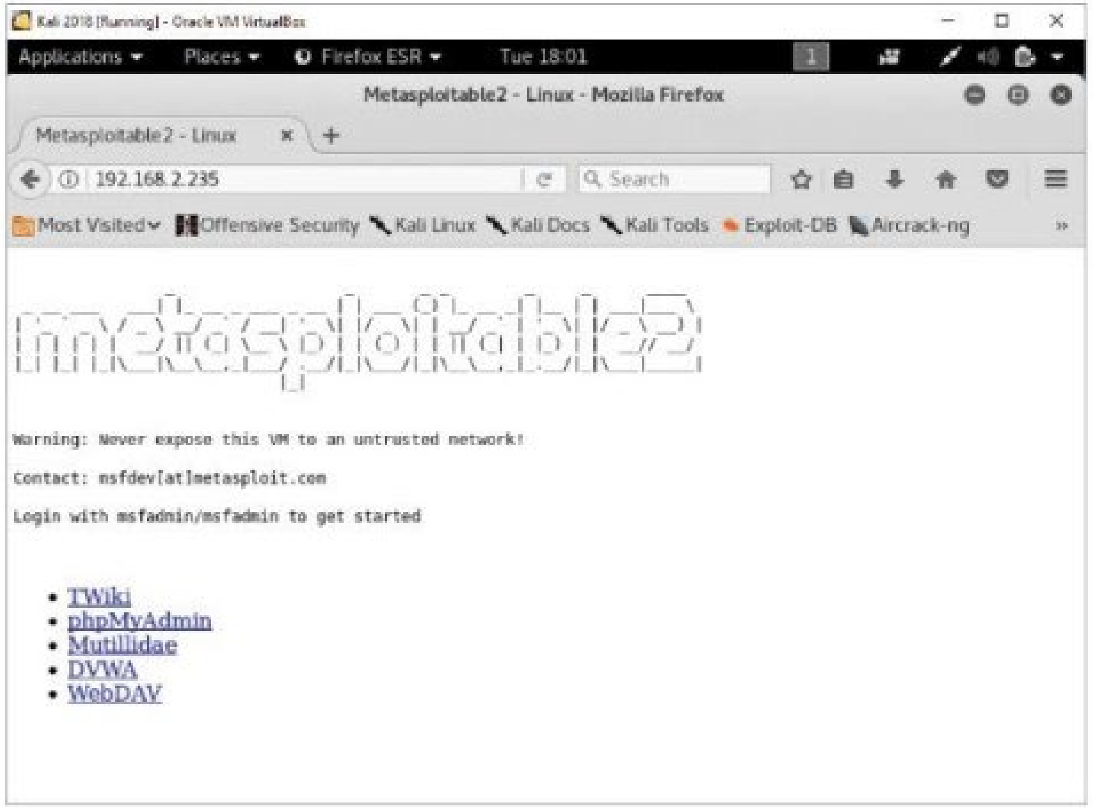
Id	Req. Timest...	Met...	URL	C...	Reason	...	Size Resp...	Highest...	N...	Tags
3	5/11/21 6:0...	GET	http://192.168.2.235/	2...	OK	...	891 bytes	Medi...		

Source OWASP.ORG

ZAP Launch Browser

Zed Attack Proxy (ZAP)

- After configuration, you can use ZAP to navigate to target site.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

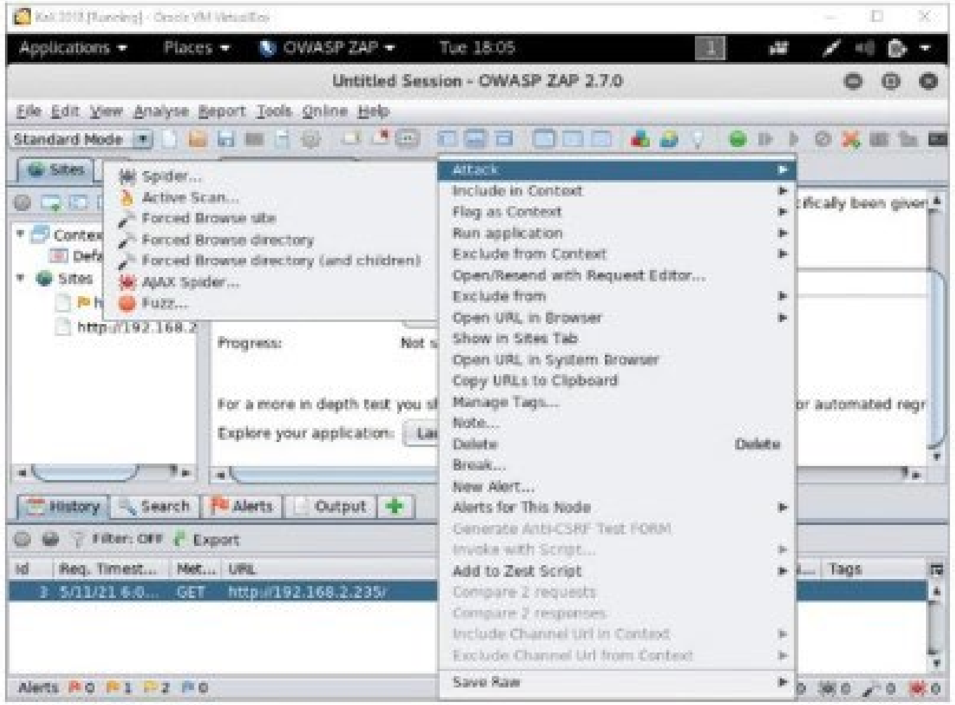
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Source OWASP.ORG

Target website open in ZAP-launched browser

Zed Attack Proxy (ZAP)

- The target website will now be in the History tab.
- Right-click on the site, point to Attack in the shortcut menu, then click “Spider.”
- A pop-up window will appear and click “Start Scan” to begin spidering of the site.

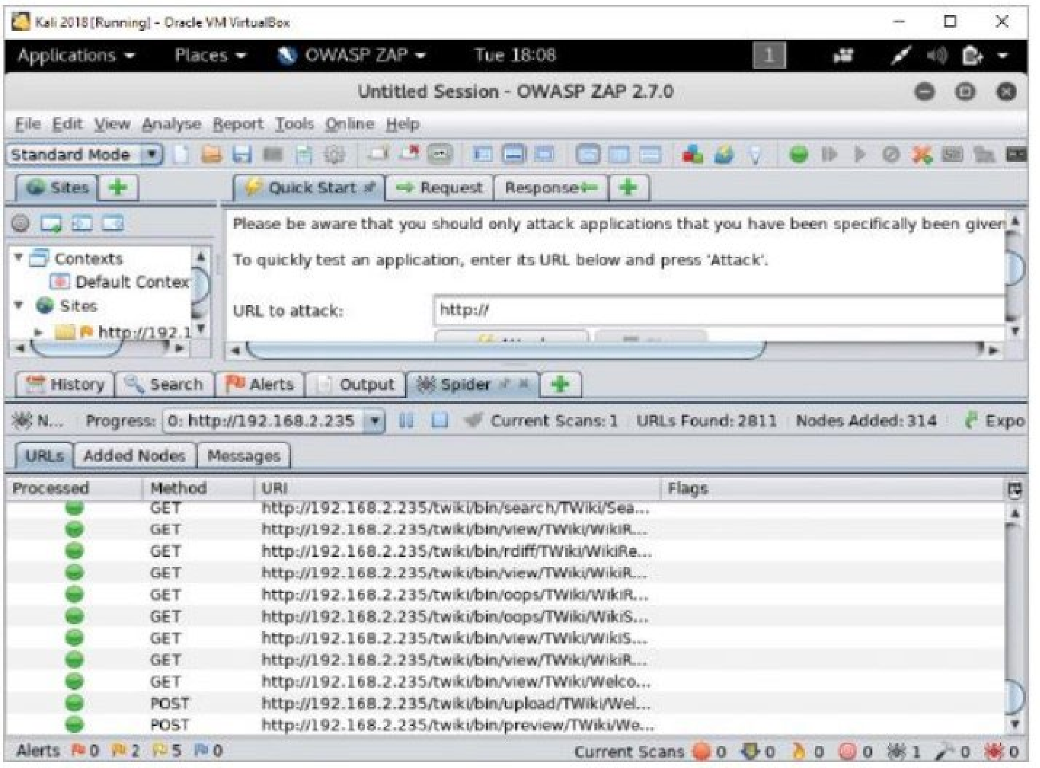


Source OWASP.ORG

Executing a spider (crawl) of targeted website

Zed Attack Proxy (ZAP)

- Spidering (or crawling) is a way to map a website, it explores every nook and is not an attack.



Please be aware that you should only attack applications that you have been specifically been given

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

Progress: 0: http://192.168.2.235 Current Scans: 1 URLs Found: 2811 Nodes Added: 314

Processed	Method	URI	Flags
●	GET	http://192.168.2.235/twiki/bin/search/TWiki/Sea...	
●	GET	http://192.168.2.235/twiki/bin/view/TWiki/WikiR...	
●	GET	http://192.168.2.235/twiki/bin/rdiff/TWiki/WikiRe...	
●	GET	http://192.168.2.235/twiki/bin/view/TWiki/WikiR...	
●	GET	http://192.168.2.235/twiki/bin/oops/TWiki/WikiR...	
●	GET	http://192.168.2.235/twiki/bin/oops/TWiki/WikiS...	
●	GET	http://192.168.2.235/twiki/bin/view/TWiki/WikiS...	
●	GET	http://192.168.2.235/twiki/bin/view/TWiki/WikiR...	
●	GET	http://192.168.2.235/twiki/bin/view/TWiki/Welco...	
●	POST	http://192.168.2.235/twiki/bin/upload/TWiki/Wel...	
●	POST	http://192.168.2.235/twiki/bin/preview/TWiki/We...	

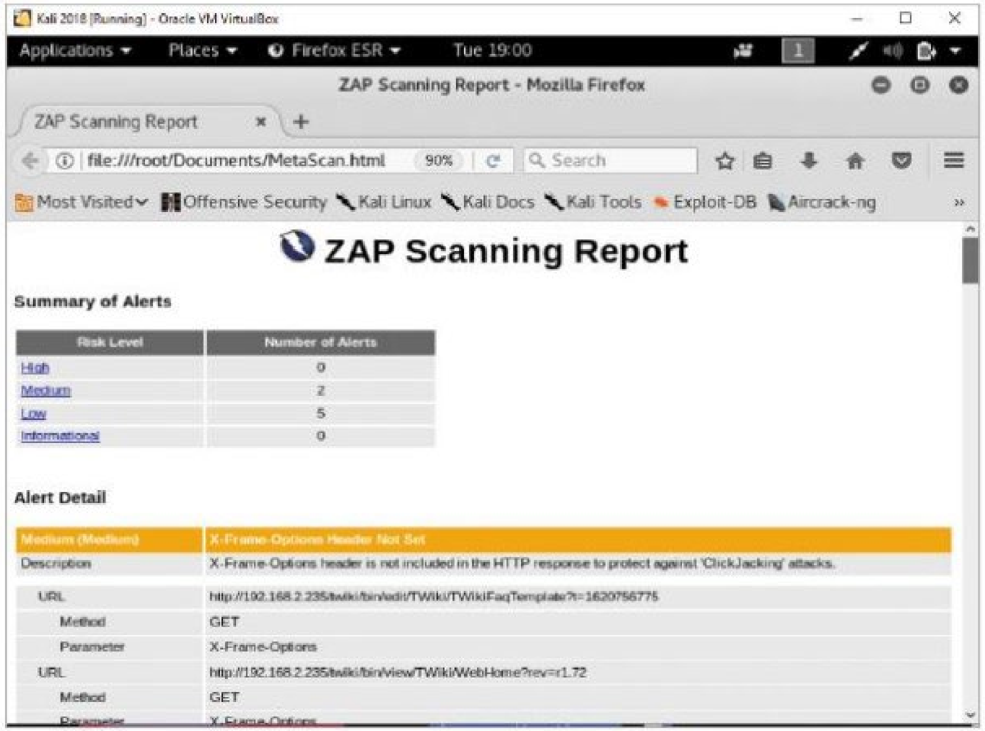
Alerts 0 2 5 0 Current Scans 0 0 0 0 1 0 0

Source OWASP.ORG

Displaying filenames of content on a website

Zed Attack Proxy (ZAP)

- After conducting the spidering, you can then use the ZAP attack.
- It is an active attack that consists of two steps: spidering and then sending a series of requests specifically to seek out vulnerabilities on the web server.
- Once complete you can view the vulnerabilities in the Alerts tab and even export to an HTML report.



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	5
Informational	0

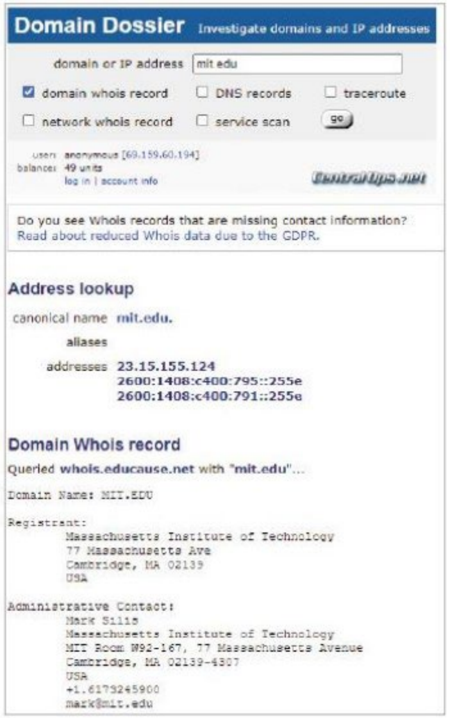
Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://192.168.2.235/twiki/bin/edit/TWiki/TWikiFaqTemplate?t=1620756775
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.2.235/twiki/bin/view/TWiki/WebHome?rev=r1.72
Method	GET
Parameter	X-Frame-Options

Source OWASP.ORG

ZAP Scanning Report

Domain Dossier



Domain Dossier Investigate domains and IP addresses

domain or IP address: mit edu

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan go

user: anonymous [69.159.60.194]
balance: 49 units
log in | account info

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name mit.edu.

aliases

addresses 23.15.155.124
2600:1408:c400:795::255e
2600:1408:c400:791::255e

Domain Whois record

Queried whois.educause.net with "mit.edu"...

```
Domain Name: MIT.EDU

Registrant:
        Massachusetts Institute of Technology
        77 Massachusetts Ave
        Cambridge, MA 02139
        USA

Administrative Contact:
        Mark Silis
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6173245900
        mark@mit.edu
```

Source: centralops.net

Viewing information with the Domain Dossier Whois utility

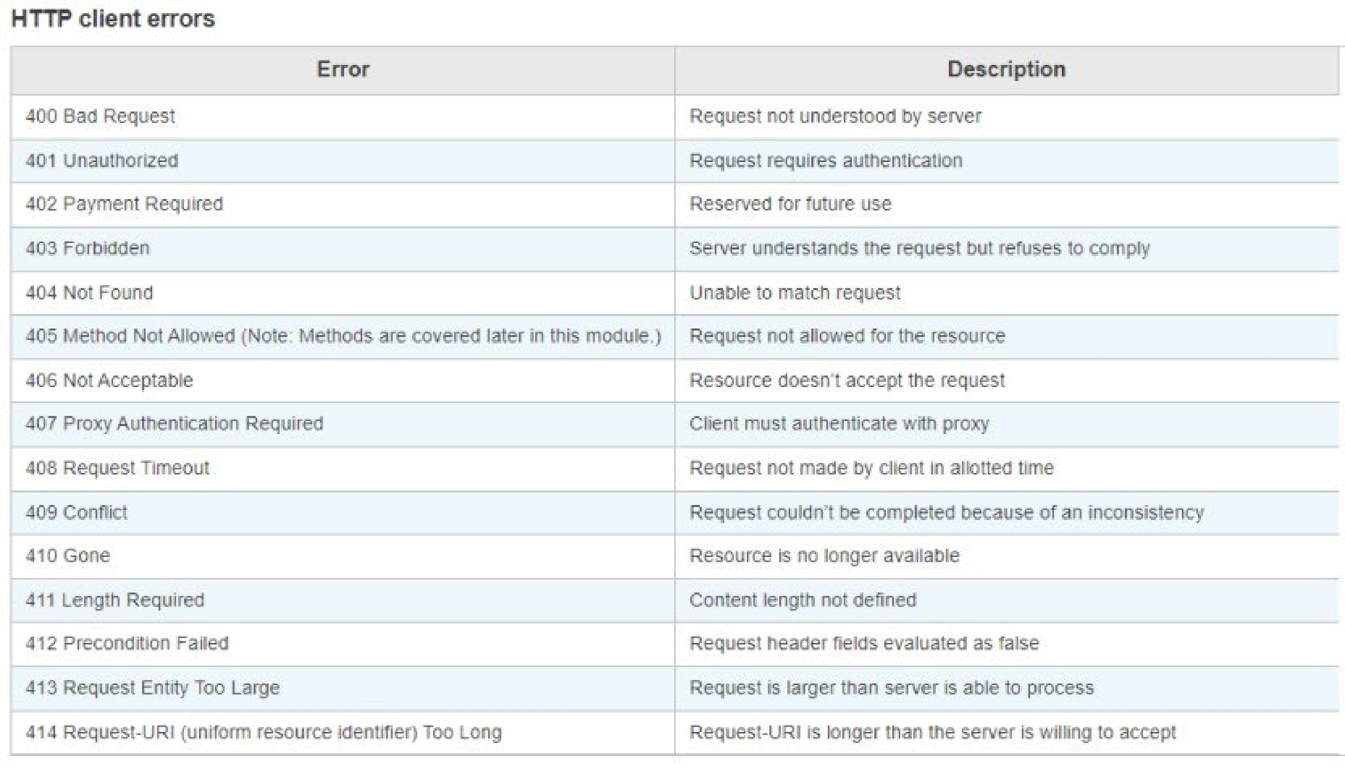
- Domain Dossier and whois.domaintools.com Whois function is passive reconnaissance and a useful footprinting tool to know.

- You can gain knowledge about network configuration that could be used in an attack.

1. Go to https://centralops.net/co/domaindossier.aspx.
2. Type mit.edu in the IP address text box, check domain whois record check box, click "go."
3. Scroll to view the displayed information.

Using HTTP Basics

Because HTTP uses port 80 and HTTPS uses 443, you can learn a lot about a web server by understanding error codes.

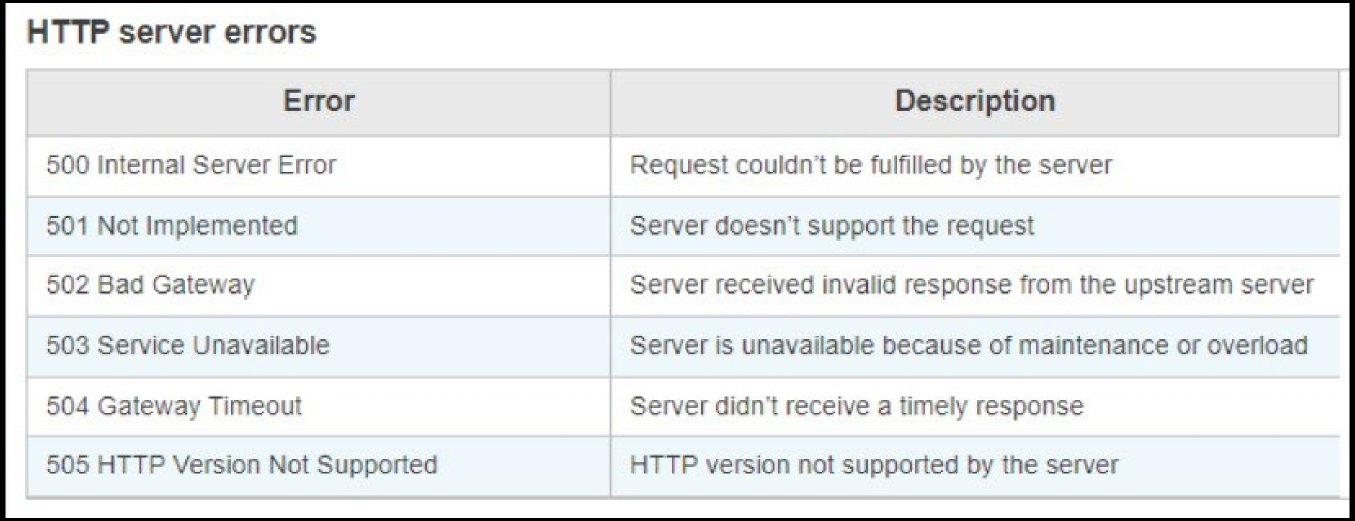


HTTP client errors

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
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 than server is able to process
414 Request-URI (uniform resource identifier) Too Long	Request-URI is longer than the server is willing to accept

Using HTTP Basics

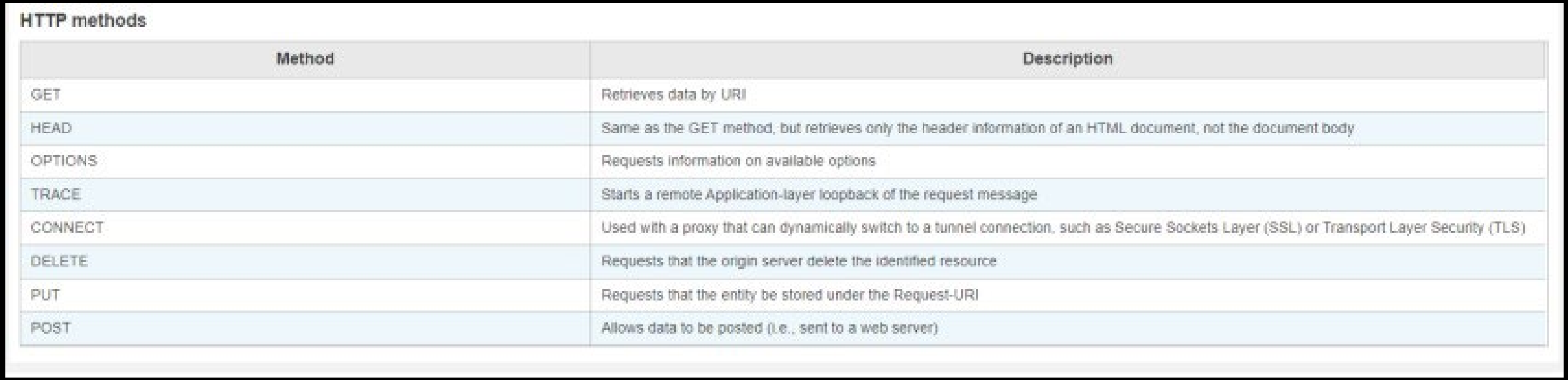
By understand HTTP server error codes, you could possibly learn the OS that the computer is using.



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
503 Service Unavailable	Server is unavailable because of maintenance or overload
504 Gateway Timeout	Server didn't receive a timely response
505 HTTP Version Not Supported	HTTP version not supported by the server

- Learning HTTP methods is helpful, and though it is not necessary to understand everything , learning the basic GET HTTP/1.1 helps.
- By learning HTTP methods, you can send requests to a web server and determine the OS being used, which is a first step to learning about any vulnerabilities.



HTTP methods

Method	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 Methods

- A valid place to start is by using nc command to connect to port 80 (as most likely vulnerable) then use HTTP methods to probe.

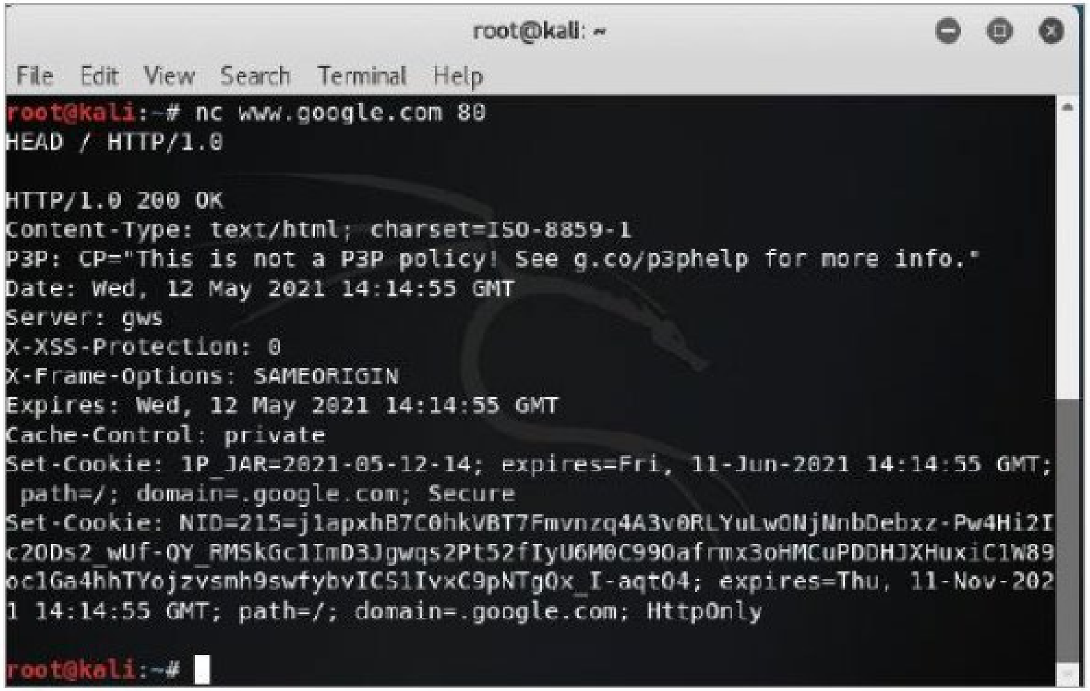
1. Use a computer with Kali Linux installed.

2. In the terminal type “nc www.google.com 80” and hit Enter.

3. Then type OPTIONS / HTTP/1.1 and hit Enter.

4. Then type HOST:127.0.0.1 and hit Enter twice for header information.

** Notice what the HEAD method produced, that the connection was closed. Not surprising, as it is Google. **



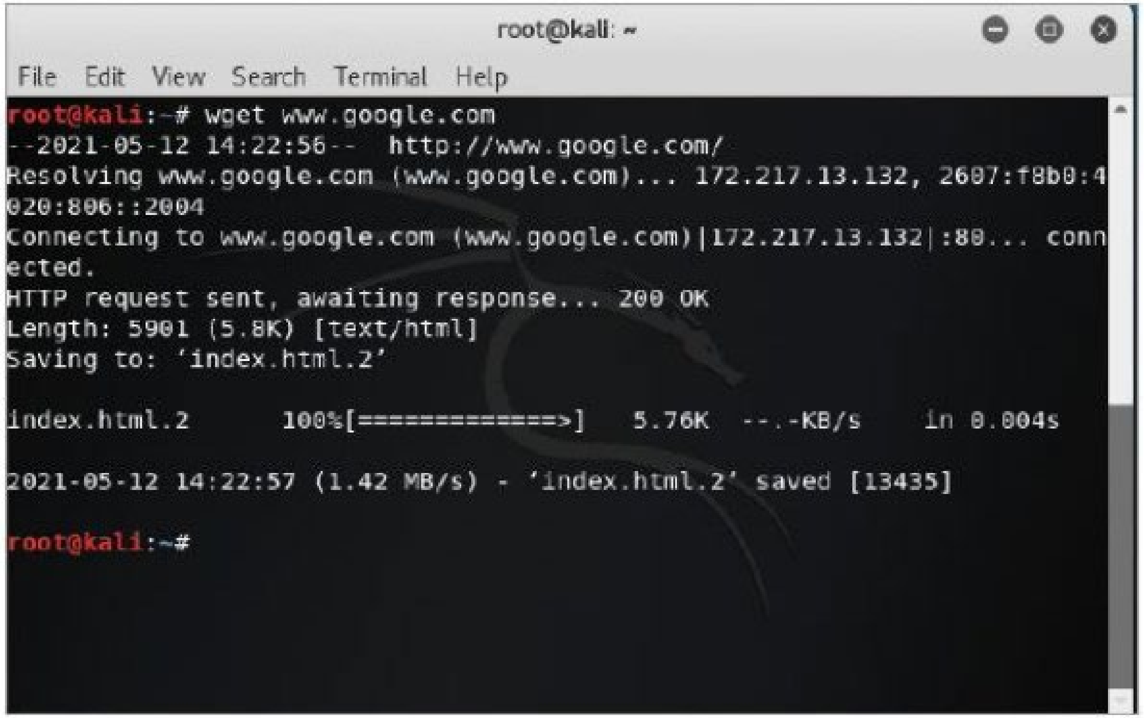
```
root@kali:~# nc www.google.com 80
HEAD / HTTP/1.0

HTTP/1.0 200 OK
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Wed, 12 May 2021 14:14:55 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Wed, 12 May 2021 14:14:55 GMT
Cache-Control: private
Set-Cookie: 1P_JAR=2021-05-12-14; expires=Fri, 11-Jun-2021 14:14:55 GMT;
 path=/; domain=.google.com; Secure
Set-Cookie: NID=215=j1apxhB7C0hkVBT7Fmvnzq4A3v0RLYuLwONjNnbDebxz-Pw4Hi2I
c2ODs2_wUf-QY_RMSkGc1ImD3Jgwqs2Pt52fIyU6M0C99OafrmX3oHMCuPDDHJXHuxiC1W89
oc1Ga4hhTYojzvsmh9swfybvICS1IvxC9pNTgOx_I-aqtO4; expires=Thu, 11-Nov-202
1 14:14:55 GMT; path=/; domain=.google.com; HttpOnly

root@kali:~# 
```

Source: Kali Linux

Using the HEAD HTTP method

Using HTTP Methods

- Next, type “wget www.google.com” and hit Enter. It will download the index page from the website in HTML code.



```
root@kali:~# wget www.google.com
--2021-05-12 14:22:56--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.13.132, 2607:f8b0:4
020:806::2004
Connecting to www.google.com (www.google.com)|172.217.13.132|:80... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: 5901 (5.8K) [text/html]
Saving to: ‘index.html.2’

index.html.2      100%[==============>]   5.76K  --.-KB/s    in 0.004s

2021-05-12 14:22:57 (1.42 MB/s) - ‘index.html.2’ saved [13435]

root@kali:~#
```

Source: Kali Linux

Using the WGET HTTP method

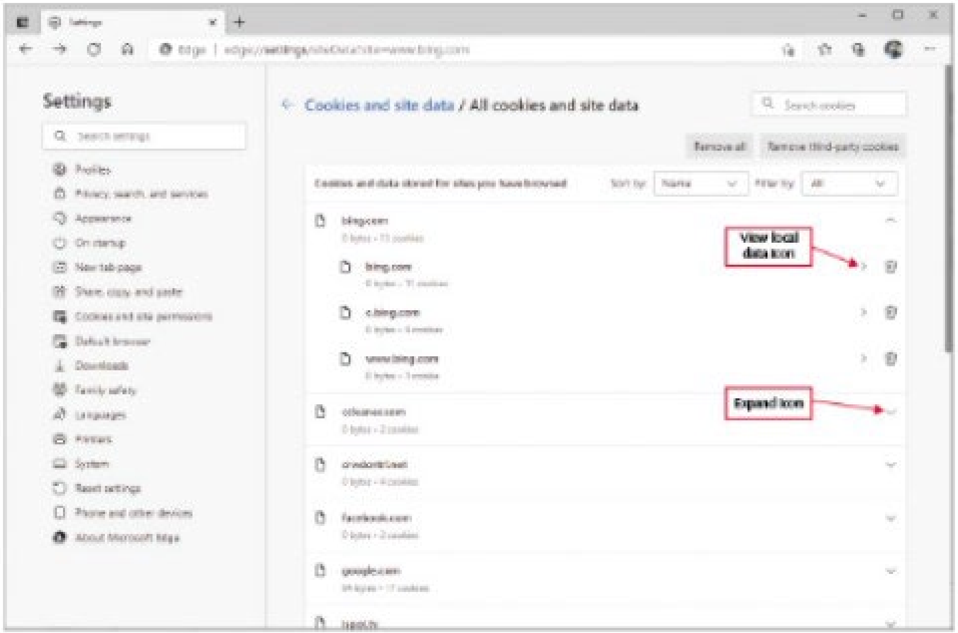
Detecting Cookies and Web Bugs

Photo by Lisa Fotios: https://www.pexels.com/photo/macro-photography-of-pile-of-3-cookie-230325/

- A cookie is a text file generated by a web server and stored on a user's browser. Security issues can arise because some information stored in a cookie could be used to attack a computer or server.
- A web bug is a 1-pixel x 1-pixel image file referenced in an <IMG> tag, and it usually works with a cookie.
- Web beacon is a hidden graphic or piece of code embedded in a webpage to track user activity and harvest information (one kind is JavaScript).
- Good idea to have a tool to detect web bugs and JavaScript web beacons or to look through webpages to see if any exist.

Discovering Cookies in Webpages

1. Using Windows, open Microsoft Edge.
2. Click Settings and more button (upper-right corner) and click Settings.
3. Click on Cookies and site permission and then click Manage and delete cookies and site data.
4. Click See all cookies and site data link in which cookies will be displayed depending on what websites you have visited using the browser.



Source: Microsoft

Edge browser cookies and site data

Discovering Cookies in Webpages

5. Click on the expand icon of a listed website to view specific cookie groups.

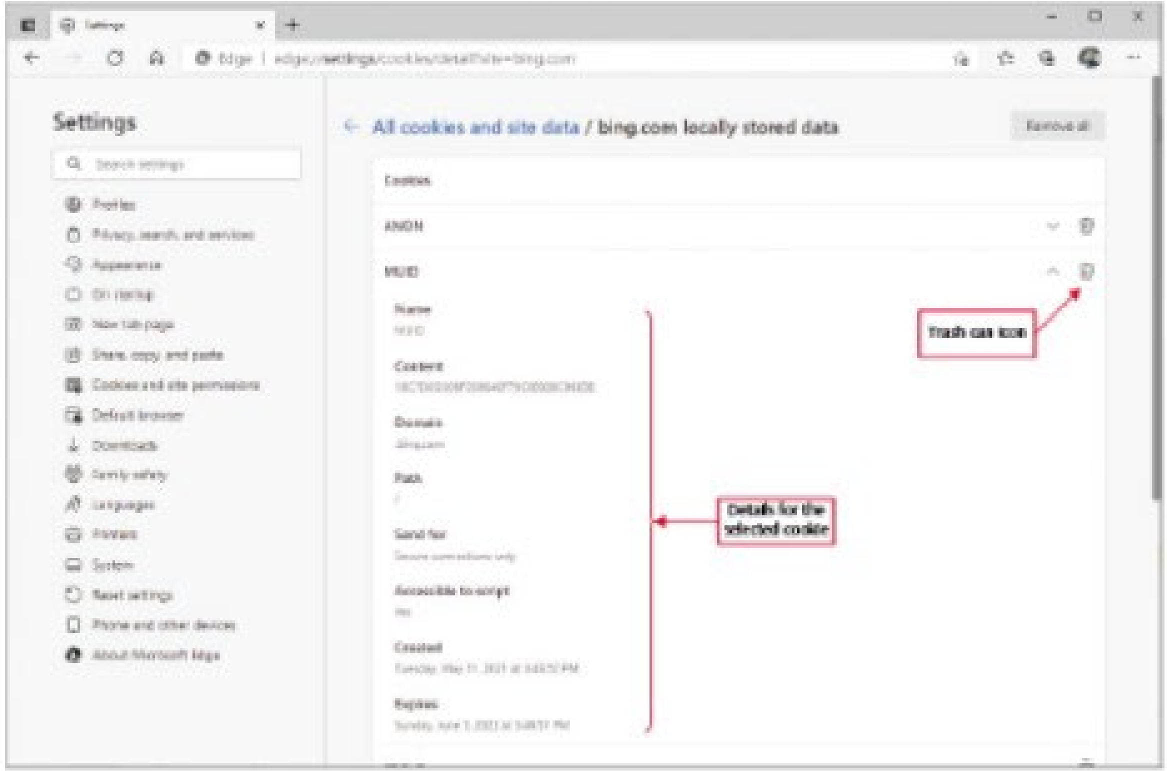
6. Click the View local data icon to display the specific cookies in the group.

7. Click expand icon to see the data stored in the cookie and you can delete the cookies if you wish.

8. Check to see if you have cookies from Amazon.com, if so, delete them.

9. Open www.amazon.com and search for shoes.

10. Refresh the cookie page and expand the amazon.com entry and see if it contains any personal information.



All cookies and site data / bing.com locally stored data

Cookies

ANON

MUID

Name
MUID

Content
[illegible]

Domain
.bing.com

Path
/

Send for
Secure connections only

Accessible to script
No

Created
Tuesday, May 11, 2021 at 3:43:52 PM

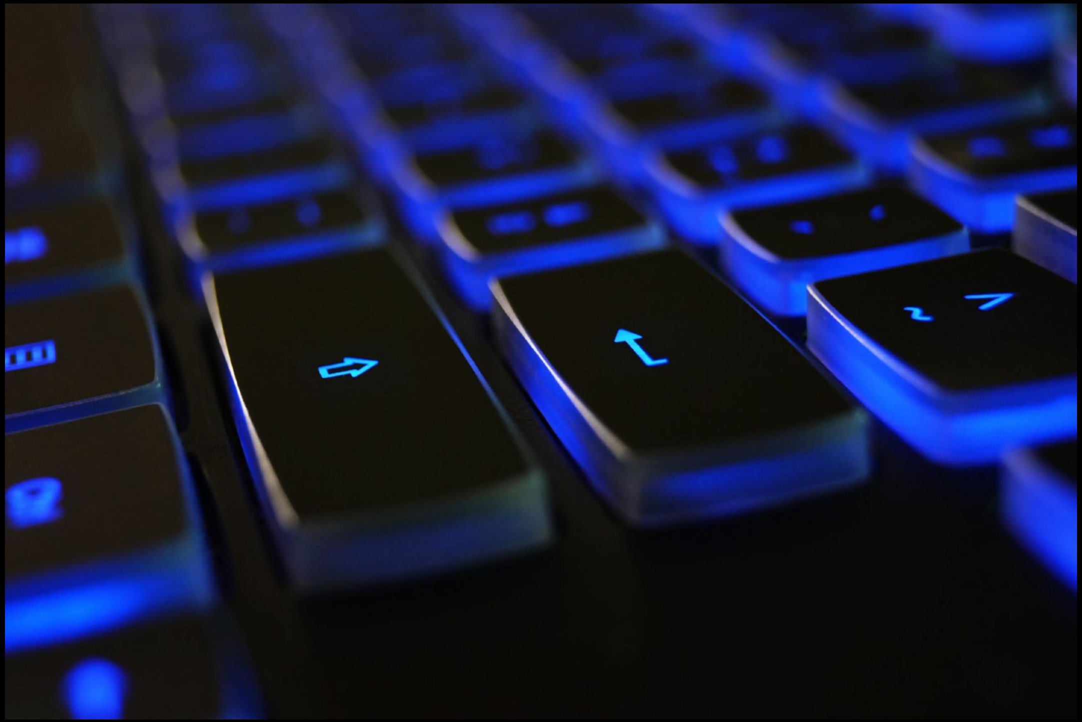
Expires
Sunday, June 5, 2022 at 3:48:51 PM

Trash can icon

Details for the selected cookie

Source: Microsoft

Examining Web Beacons and Privacy



- Web beacons are considered to be more invasive, and it is good to understand how companies use them to gather information.

1. Open a browser in Windows and go to https://en.Wikipedia.org/wiki/web_beacon.

2. Read article, taking note of methods used.

3. Search the web using the term "web beacons" combined with names of social media companies and take note of findings in results and you will be shocked to see what is being monitored.

Photo by Marta Branco: https://www.pexels.com/photo/closeup-photo-of-black-and-blue-keyboard-1194713/

Using Domain Name System Zone Transfers

- Domain Name System (DNS) is used to resolve hostnames to IP addresses and vice-versa, but it is vulnerable to network attacks.
- A zone transfer is a process by which when you determine what name server a company is using, you can attempt to transfer all the records for which the DNS server is responsible.
- Zone transfers are done with the dig command.
- Look for a DNS server containing a SOA record
- SOA records show which zones or IP addresses the DNS server is responsible.
- After finding the primary DNS server, do another zone transfer to see all host computers on the company network (gives you a diagram, great for footprinting).
- This can be used to attack servers or computers on the same network infrastructure.

Photo by panumas nikhomkhai: https://www.pexels.com/photo/close-up-photo-of-mining-rig-1148820/

Identifying IP Addresses by Using Zone Transfers

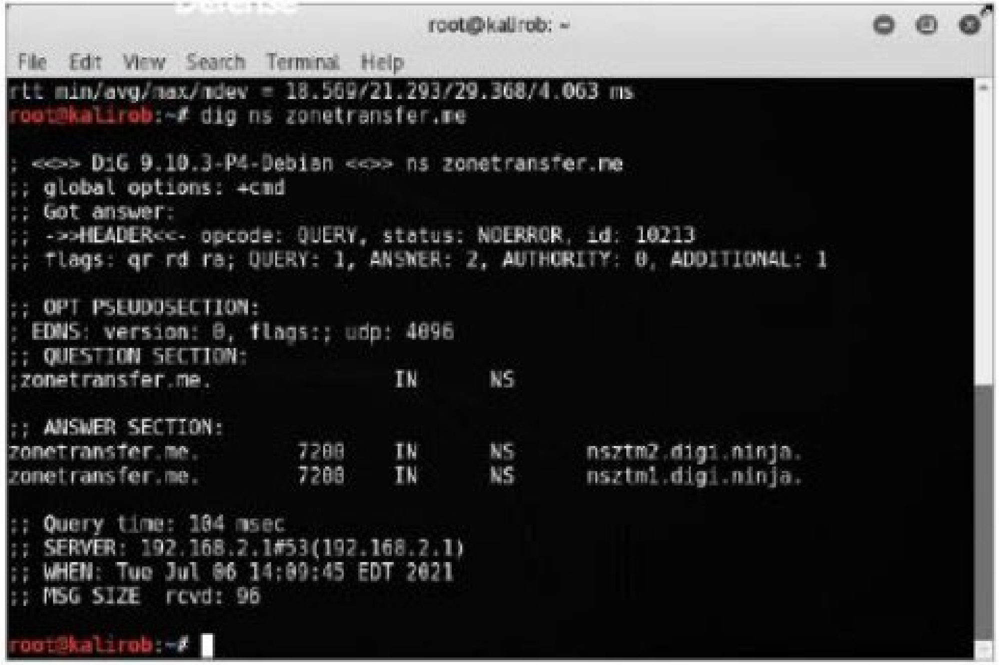
1. Using Kali Linux, open a terminal shell and enter the command “dig ns zonetransfer.me” and hit Enter. In the picture you see two server names nsztm.1.dig.ninja and nsztm2.digi.ninja. This means that the DNS was configured incorrectly leaving the network vulnerable to attacks.

2. Perform a zone transfer on nsztm1.digi.ninja DNS server by typing command “dig axfr @nsztm1.digi.ninja zonetransfer.me” and hit Enter. After a while, a few records should appear.

3. Do the zone transfer again, but this time use the | less parameter by typing “dig axfr @nsztm1.digi.ninja zonetransfer.me | less” and hit Enter.

4. Press Enter to view additional records and when done press q.

- If an attack works, copy all files and data obtained in the hack to a disk or thumb drive as soon as possible.



```
rtt min/avg/max/mdev = 18.569/21.293/29.368/4.063 ms
root@kalirob:~# dig ns zonetransfer.me

; <<>> DiG 9.10.3-P4-Debian <<>> ns zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10213
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zonetransfer.me.               IN      NS

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.

;; Query time: 104 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Tue Jul 06 14:09:45 EDT 2021
;; MSG SIZE  rcvd: 96

root@kalirob:~# 
```

Source: Kali Linux

Using the dig command

Photo by Pixabay: https://www.pexels.com/photo/door-handle-key-keyhole-279810/

Social Engineering

- Social engineering uses the art of deception to extract valuable information from well-meaning people who are trying to be helpful.
- The best defense against this tactic is training people in an organization on what to look out for.
- One of the biggest security threats to networks as they are most difficult to protect against.
- Why crack a password when you can just ask for one?
- It is the study of human behavior.
- Humans are the weakest link in security, and those in an organization must be trained and tested regularly.

Social Engineering Techniques

Social Engineers use many techniques to try to gain information out of people which includes:

- Urgency- Saying that something drastic will happen unless the information is gathered quickly.
- Quid pro quo- Promising desired results for the victim if the information is provided immediately.
- Status quo- Will tell the victim that everyone else is doing it, so they should too.
- Kindness- The most dangerous weapon because majority of people are kind- a victim will help a person of who has a problem or a need to be fixed.
- Position- Convincing the victim that you are in a position of authority or of higher rank to get what is desired quickly.

** You should never use social-engineering tactics unless you have specific permission. All tests should be documented as well as any people of whom tests were performed on. Confidentiality is also key. **

Photo by Andrea Piacquadio: https://www.pexels.com/photo/smiling-formal-male-with-laptop-chatting-via-phone-3760263/

The Art of Shoulder Surfing

- Another skill mastered by Social Engineers is to read what a user inputs on their keyboards, primarily for passwords and login names. Could also be utilized at ATM's or in at a checkout for a PIN, which is identity theft.
- Smartphone cameras are utilized to capture credit card numbers.
- Shoulder surfers train themselves to memorize the key positions and they pay attention to the location of what was pressed.
- They know popular letter substitutions like @ for a or $ for s. Typing a password slow (special characters) makes it easier for the shoulder surfer.
- To prevent these attacks, users must be taught not to type their credentials when someone is behind them or even nearby, or when someone is even on their cell phone (because of the cameras).
- Place displays away from doors or cubicle entries helps.
- If observed, users should change passwords immediately.

Photo by Eduardo Soares: https://www.pexels.com/photo/person-pressing-keys-of-an-atm-5497951/

The Art of Dumpster Diving

- Another method used by social engineers is dumpster diving.
- They can gain valuable information such as old computer documentation that would show OS and potential vulnerabilities, notes which could include passwords and many other treasure troves.
- Users must be educated on how to dispose of trash.
- Disks should be formatted with "disk-cleaning" software that writes binary Os on all portions of the disks.
- Old computers should be discarded offsite.
- Before being thrown away, these items should be in a locked room.
- All documents should be shredded.

Photo by Christian Naccarato: https://www.pexels.com/photo/city-road-sunny-street-4124936/

The Art of Dumpster Diving

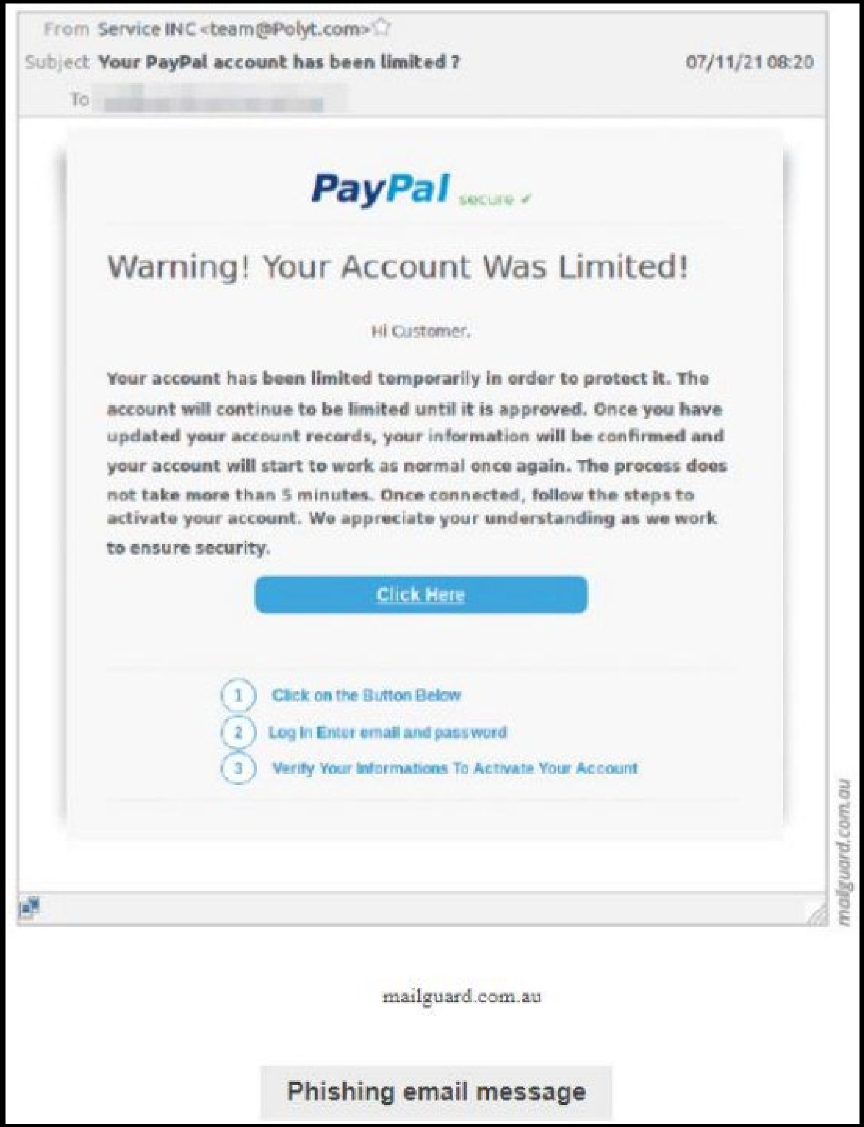
- Items that could be used to gain information could include:
  - Company calendars
  - Meeting schedules
  - Employee vacations
  - Financial reports
  - Interoffice memos
  - Discarded digital media
  - Company organizational charts showing managers' names
  - Resumes of employees
  - Company policies or systems and procedures manuals
  - Professional journals or magazines
  - Utility bills
  - Solicitation notices from outside vendors
  - Regional manager reports
  - Quality assurance reports
  - Minutes of meetings
  - Federal, state, or city reports
  - Employee charge card receipts

Photo by Steve Johnson: https://www.pexels.com/photo/focus-photo-of-yellow-paper-near-trash-can-850216/

The Art of Piggybacking

- Piggybacking is trailing closely behind an employee who has access to an area without the employee realizing you didn't use a PIN or a security badge to the area.
- Skilled piggybackers watch how authorized personnel enter areas and wait to join them.
- They can also rely on a kind stranger to hold open a door with the stranger thinking that they actually are authorized to enter.
- Some will wear a fake badge and try to pass off as a person authorized to enter and if it does not work, will use their personal skills to back out.
- Employees or authorized users should never let someone in through the door, even if they know them and everyone should use their proper access cards.
- Turnstiles can help, but the best way to prevent piggybacking is to train personnel.

Photo by Charlotte May: https://www.pexels.com/photo/crop-person-turning-door-handle-while-entering-house-5825403/



From Service INC <team@Polyt.com>

Subject **Your PayPal account has been limited ?** 07/11/21 08:20

To [redacted]

Warning! Your Account Was Limited!

Hi Customer,

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved. Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again. The process does not take more than 5 minutes. Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

1. Click on the Button Below
2. Log In Enter email and password
3. Verify Your Informations To Activate Your Account

mailguard.com.au

Phishing email message

Phishing

- Everyone has had a phishing email at some point in their lives and it usually comes with a message that you need to update your account, but then eventually someone will click, give their personal data, and real money is lost.
- Look out for greetings that do not mention your name, spelling, and grammar errors.
- Spear phishing is more dangerous to companies as it is an attack carried out by email that combines social engineering with exploiting any vulnerabilities where millions of dollars have been lost.
- The goal is to entice recipients in an organization to open a malicious link on the organization's network.
- Security consulting companies will include it in their testing, using tools such as Metasploit, email authentication technologies, and creating training for users on what to look for.

In Closing:

- How much time did I spend reading and preparing the slides? I spent 11 1/2 hours on reading, studying, and preparing the slides.
- The most interesting part of the chapter was Social Engineering. I always find it fascinating how people are so willing to give away information voluntarily.
- The most difficult part of the chapter was learning about using HTTP methods. I am just not that familiar, so I was intently studying this part.
- A topic I would still want to learn more about from this chapter would have to be what I considered to be the most difficult, using HTTP methods. I find that I have not encountered this in any of my labs and if I have, I do not remember, but it is important so it is something I will dive deeper into.