offsec.html

offsec.css

```
Offensive ‘Security’ {
    [Introduction]

    < CSA – September 2025 >

}
```

offsec.html

offsec.css

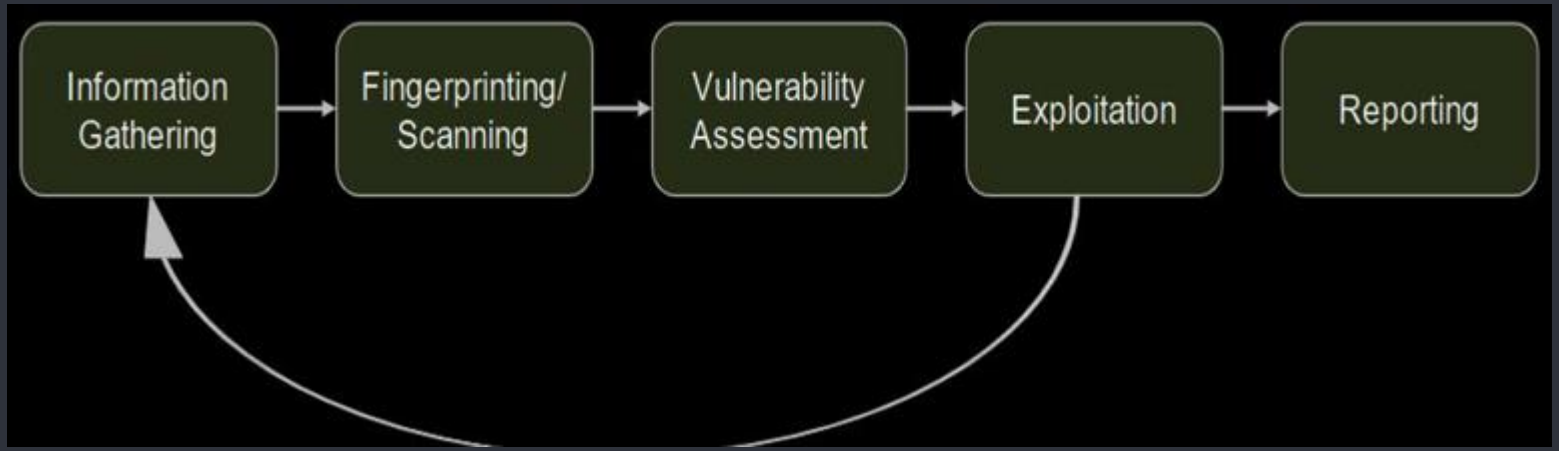
```
1
2
3
4
5
6
7
8
9
10
11
12
13
14
```

Introduction to { Offensive Security;

}

offsec.html offsec.css

Offensive Security ‘Steps’ {



}

offsec.html

offsec.css

Information Gathering {

< Gathering as much information as possible about hosts, networks, etc. >

< Two different methodologies: active vs, passive >

}

Fingerprinting/Scanning {

< Gaining more specific information about technologies being used >

< Scanning methods: Port, Directory, Web, Service, etc. >

}

Vulnerability Assesment {

< Assessing Services, Computers, and Configurations for vulnerabilities >

< VA Frameworks: Nikto, OpenVAS, etc. >

}

Exploitation {

< Using the knowledge gained during the VA stage to obtain a desired role (i.e, a foothood, privileges, etc) >

< Exploit Frameworks: Metasploit, ExploitDB, etc. >

}

offsec.html

offsec.css

Reporting {

< A company pays you for a report of your findings, and steps to fix them, not for you to hack them. >

< Includes how to reproduce vulnerabilities, why the vulnerability will affect business, and how to mitigate it. >

}

offsec.html

offsec.css

```
Career in {
Offensive Security;

}
```

offsec.html

offsec.css

Penetration Tester ‘Overview’ {

- **What?** A security test for computers, configurations, and services.
- **Who?** Internal team or external Penetration Testing company
- **How?** Based largely on a customer requested scope
- **When?** According to a company's own desires, or as required by laws
- **Why?** There are always new vulnerabilities to find

}

offsec.html

offsec.css

Red Teamer ‘Overview’ {

- **What?** A security test for incident response, computers, people, and just about everything else
- **Who?** Internal team or external Red Teaming company
- **How?** Based largely on a customer requested scope, usually more open than a Penetration Test
- **When?** According to a company's own requirements
- **Why?** Companies want to test their security solutions in depth

}

offsec.html

offsec.css

Security Engineer ‘Overview’ {

- **What?** A security professional who develops or tests company security
- **Who?** Usually an internal team
- **How?** Based largely on internal requirements
- **When?** 24/7/365
- **Why?** Companies want to have continuous internal security developers

}

offsec.html

offsec.css

Why OffSec? {

< Wondering if OffSec is right for you? >

< /1 >
* Average base salary of $125k
* Source: Indeed

< /2 >
* 5 billion dollar market by 2031
* Source: Cybercrime Mag

< /3 >
* ~50,000 open job postings
* Source: Cyberseek

< /4 >
* 3 – 5 years of OffSec work required
* Source: Numerous job postings

}

offsec.html

offsec.css

Future Events {

< Upcoming BYU CSA Pentest Emphasis meetings >

< /1 >
* October 14
* Access Control Security

< /2 >
* October 28
* Hack-O-Ween

< /3 >
* November 11
* Password Cracking + WiFi Hacking

< /4 >
* December 9th
* AI Attacks

}

offsec.html

offsec.css

```
Thanks; {

    ‘Do you have any questions?’

}
```