1
2
3   Penetration 'Testing' {
4
5   [Introduction]
6
7
8
9   < CSA — October 2024 >
10
11
12   }
13
14

```
1    Future Events {
2
3          < Upcoming BYU CSA Pentest Emphasis meetings >
4
5
6
7                                    *   October 29
8          < /1 >                    *   Hack-O-Ween – PenTest Activity
9
10
11         < /2 >         *   December 3
12                        *   Normal Meeting
13
14   }
```

```
1
2
3
4      Introduction to {
5      Penetration
6      Testing;
7
8
9
10
11
12      }
13
14
```

```
1    Penetration Testing 'Overview' {
2
3        ——— What?    A security test for computers,
4                     configurations, and services.
5
6        ——————— Who?  Internal team, or external 3rd
7                     party Penetration Testing company
8        ————————— How?  Based largely on a customer
9                       requested scope
10       ———————————— When?  According to a company's own
11                          desires, or as required by laws
12       —————————————— Why?  There are always new
13                            vulnerabilities to find
14   }
```
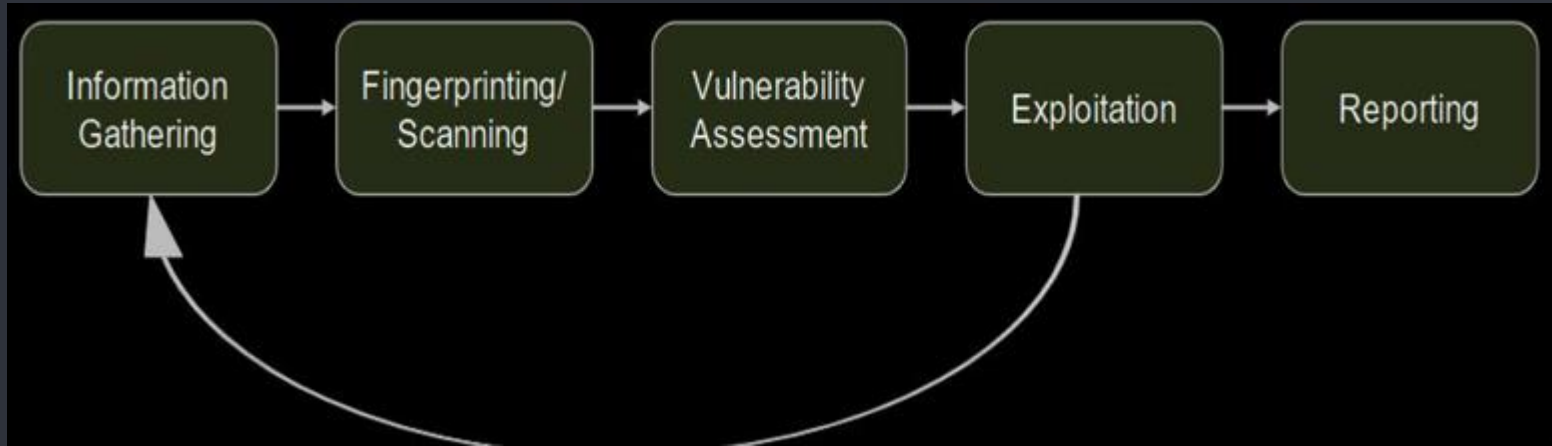
1   # Penetration Testing 'Steps' {

2

3

4

5

6

7

8

9

10

11

12

13

14 }

1 # Information Gathering {

2

3

4   [👁] < Gathering as much information as possible

5   about hosts, networks, etc. >

6

7

8

9

10   [✈]   < Two different methodologies: active vs,

11   passive >

12

13

14 }

```
1    Fingerprinting/Scanning {
2
3
4        [📊🔍]  < Gaining more specific information about
5                 technologies being used >
6
7
8
9
10       [👆]    < Scanning methods: Port, Directory, Web,
11                Service, etc. >
12
13
14   }
```

1 **Vulnerability Assesment {**
2
3
4   < Assessing Services, Computers, and
5   Configurations for vulnerabilities >
6
7
8
9
10   < VA Frameworks: Nikto, OpenVAS, etc. >
11
12
13
14 }

```
1   Exploitation {
2
3
4        [⚒]   < Using the knowledge gained during the VA
5              stage to obtain a desired role (i.e, a
6              foothood, privileges, etc) >
7
8
9
10       [⚗]   < Exploit Frameworks: Metasploit, ExploitDB,
11             etc. >
12
13
14   }
```

1   Reporting {

2

3

4   [📄]   < A company pays you for a report of your

5   findings, and steps to fix them, not for you

6   to hack them. >

7

8

9   [🛡️]   < Includes how to reproduce vulnerabilities,

10   why the vulnerability will affect business,

11   and how to mitigate it. >

12

13

14   }

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

Activity {

< Hands On Time >

}

```
1   Thanks; {
2
3       'Do you have any questions?'
4
5               Don't forget:
6               - October 29: Hack-O-Ween — PenTest Activity
7               - December 3: Normal Meeting
8
9
10              CREDITS: This presentation template was
                created by Slidesgo, including icons by
11              Flaticon, and infographics & images by
                Freepik
12
13
14      }
```