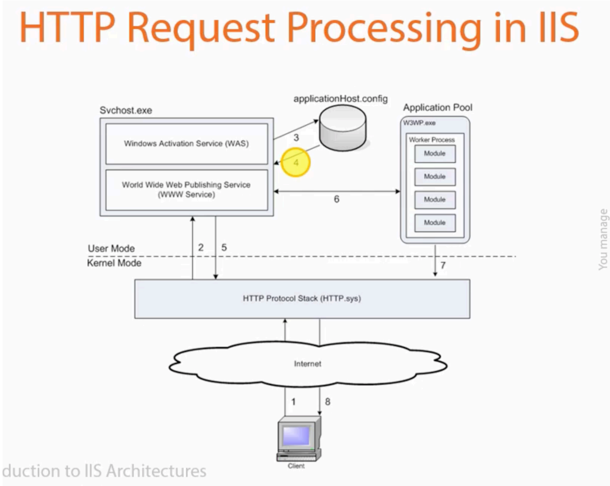
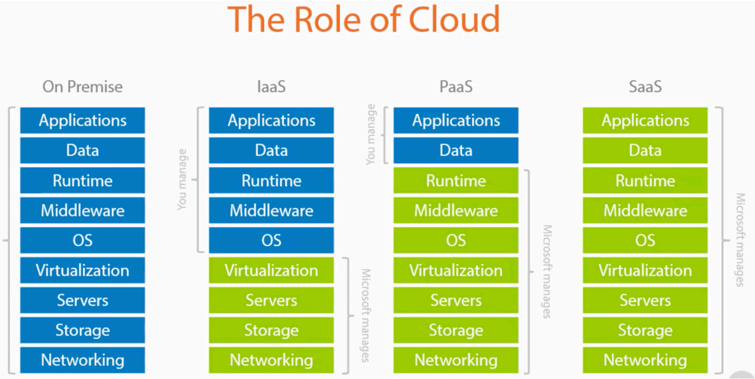
Module - 12
Hacking Web Servers

The **User mode** is normal **mode** where the process has limited access. While the **Kernel mode** is the privileged **mode** where the process has unrestricted access to system resources like hardware, memory, etc.


HTTP Request Processing in IIS
Svchost.exe
Windows Activation Service (WAS)
World Wide Web Publishing Service (WWW Service)
applicationHost.config
Application Pool
W3WP.exe
Worker Process
Module
Module
Module
Module
3
4
6
2
5
7
User Mode
Kernel Mode
HTTP Protocol Stack (HTTP.sys)
Internet
1
8
Client
duction to IIS Architectures



The Role of Cloud

On Premise	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

The server is not self managed (PaaS)

# Web Server Misconfiguration

1. Internal Data
2. Debug Settings : gives verbose output
3. Excessive Access rights

Principle of least Privileges

Every module must be able to access only the information and resources that are necessary for its legitimate purpose.

4. Misconfigured SSL
5. Weaknesses in default configuration

www.defaultpassword.com

# Managing and Hardening Web Servers :

Patch Management

- Have a change control Process
- Apply updates on a need basis
- Have a Testing process
- Have a rollback plan
- Schedule an update cadence
- Automate Monitoring

Support and End of Life

Locking Down Services

- Disable Unnecessary Services
- Disable unused ports

Network Segmentation : Splitting the computer network into subnetworks, each being a network segment. Advantages of such splitting Are primarily for boosting performance and improving the security.

- Isolating RDP (Remote Desktop Protocol)

Sandboxing : Isolating the processes do that they can't interact with each another.

# Other Attacks Against Web Servers :

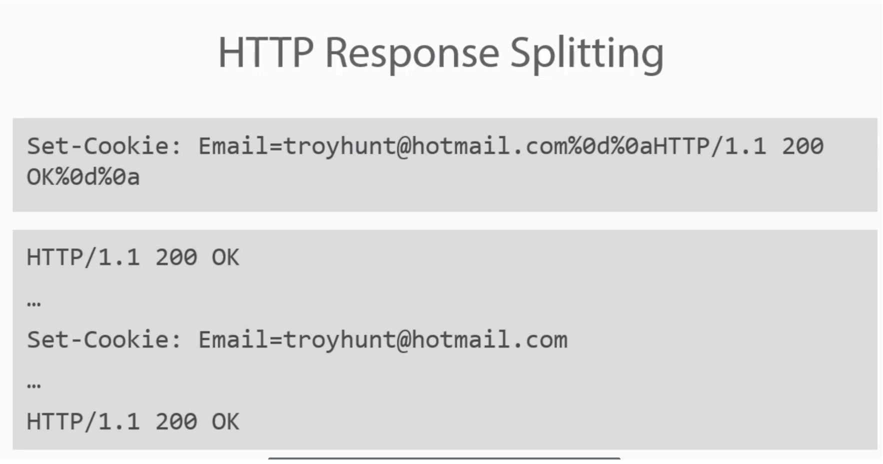
1. Web Site Defacement :

Website defacement is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.

# **Defacement Attacks vector :**

1. Compromised Credentials
2. Cross Site Scripting
3. Insufficient Sandboxing
4. DNS Hijacking

2. HTTP Response Splitting :



HTTP Response Splitting

```
Set-Cookie: Email=troyhunt@hotmail.com%0d%0aHTTP/1.1 200
OK%0d%0a
```

```
HTTP/1.1 200 OK
…
Set-Cookie: Email=troyhunt@hotmail.com
…
HTTP/1.1 200 OK
```

3. Web Cache Poisioning :

Attacker loaded the cache server with malicious data and when the legitimate user access the cache server he will be served with malicious server.

a. Remove the Existing page from the cache (using http response spiliting)
b. The the user is served with the malicious content

4. Brute Force Attacking :

use Burpsuite

5. Streamline Testing with Automation :

1. BurpSuite
2. OWASP ZAP
3. Fiddler
4. Netsparker
5. Nmap