**SEMESTER: VI**

**Discipline Centric Elective - 3**

**19UCC813 – Basics of Threat Detections**

**SYLLABUS**

**UNIT I:**

**Hacking Web Apps and Profiling.**

Web Application Hacking: GUI web Hacking, URI Hacking, Methods Headers and Body, Resources. The Web Client and HTML, Other Protocols, How & Why Web Apps attack. Infrastructure Profiling: Foot printing and Scanning, **Basic Banner Grabbing, Advanced HTTP Fingerprinting, Infrastructure Intermediaries.** Application Profiling: Manual Inspection, Search Tools for Profiling, Automated Web Crawling, **General Countermeasures**

**WHAT IS THREAT DETECTION?**

Threat detection is the process of identifying [cyber attacks](https://www.webopedia.com/definitions/cyber-attack/) trying to enter a [machine](https://www.webopedia.com/definitions/computer/) or [network](https://www.webopedia.com/definitions/network/). Threats are any actor or technology that has the potential to cause harm to a system. They are not the actual attack, just the possibility of one. Threat detection uses previously identified [intrusion signatures](https://www.webopedia.com/definitions/intrusion-signature/) and network traffic anomalies that deviate from normal baselines of behavior to identify threats so they can be stopped before being exploited.

**WHAT INFORMATION IS AT RISK?**

Most attacks are aimed at stealing information that can be used for monetary gain. This data can come in multiple forms.

**Intellectual property**

In order to compete with big players in their market, some organizations may take a malicious route. They may hire attackers to steal intellectual property and trade secrets to bolster their own products and services.

**User credentials**

An easy way for hackers to gain access to a network is by stealing [user credentials](https://www.webopedia.com/definitions/credentials/). In these cases, they’re not after an authorized user’s personally identifiable information (PII). Instead, bad actors seek network logins and passwords as a doorway to more sensitive resources. With the common lack of strong passwords and the frequency of scamming, stealing user credentials are often low-hanging fruit.

Read More: [Top Password Managers for 2021](https://www.webopedia.com/definitions/password-manager/)

**Personally identifiable information (PII)**

[Personally identifiable information (PII)](https://www.webopedia.com/definitions/pii-personally-identifiable-information/), on the other hand, specifically impacts individuals. PII includes information that can be used for identity theft, such as social security numbers and bank account information. The goal of identity theft is often to open accounts in usernames and make purchases on their behalf.

**TYPES OF THREATS**

Organizations of every size face a wide variety of threats. Threat detection identifies and analyzes these types of threats so that security teams can formulate strategies to mitigate risk. Here are some of the most common types.

**Malware**

[Malware](https://www.webopedia.com/definitions/malware/) is malicious software that infects a machine or network. It can come in multiple forms, including [viruses](https://www.webopedia.com/definitions/virus/), [trojan horses](https://www.webopedia.com/definitions/trojan-horse/%22%20%5Ct%20%22_blank), [ransomware](https://www.webopedia.com/definitions/ransomware/%22%20%5Ct%20%22_blank) and [spyware](https://www.webopedia.com/definitions/spyware/).  Malware can cause a variety of major issues, such as interrupting or disabling services, stealing sensitive information, taking control of applications and breaking down network infrastructure.

**Phishing**

[Phishing](https://www.webopedia.com/definitions/phishing-meaning/) is a form of social engineering attack that aims to trick users into revealing personal data, such as PII or credentials. The most common forms of phishing are through electronic communications, such as [emails](https://www.webopedia.com/definitions/email/) or websites requesting information.

**DDoS**

DDoS attacks flood [servers](https://www.webopedia.com/definitions/server/) and networks with [traffic](https://www.webopedia.com/definitions/traffic/) that make resources and websites unavailable. These attackers infect machines with malware so they can be controlled remotely. Each device is then turned into a [bot](https://www.webopedia.com/definitions/bot/%22%20%5Ct%20%22_blank), or [zombie](https://www.webopedia.com/definitions/zombie/), which is instructed to send requests to [IP addresses](https://www.webopedia.com/definitions/ip-address/) to cause an overwhelming spike in traffic that overloads a network.

**Ransoms**

Some attackers take a more aggressive approach and will hold information or resources hostage until they’re paid a ransom. One common method is to [encrypt](https://www.webopedia.com/definitions/encryption/) an organization’s information and hold the [encryption key](https://www.webopedia.com/definitions/encryption-key/) hostage. They may also use distributed [denial-of-service (DDoS) attacks](https://www.webopedia.com/definitions/ddos-attack/) to interrupt the availability of resources until they receive a ransom.

**THREAT DETECTION TOOLS**

Due to the importance of threat detection, many cybersecurity products offer threat detection as a feature. Some of the most popular solutions with threat detection include:

* [Security information and event management (SIEM) systems](https://www.webopedia.com/definitions/siem/)
* [Threat intelligence](https://www.webopedia.com/definitions/threat-intelligence/) platforms
* [Intrusion detection and prevention systems](https://www.webopedia.com/definitions/intrusion-detection-prevention/)
* [Endpoint detection and response](https://www.webopedia.com/definitions/endpoint-detection-and-response-edr/)
* [User and entity behavior analytics (UEBA)](https://www.webopedia.com/definitions/ueba-user-and-entity-behavior-analytics/)
* [Cloud access and security brokers (CASB)](https://www.webopedia.com/definitions/casb-cloud-access-security-broker/)

**THREAT DETECTION AND RESPONSE (TDR)**

Threat detection is essential to maintaining a strong security posture but it’s only the first step. Response must follow to remediate the identified threats. The majority of tools that offer threat detection also offer response.

These [threat intelligence platforms](https://www.esecurityplanet.com/products/threat-intelligence-platforms/) can automatically contain and block threats, as well as automatically implement patches. Others may offer the ability to prioritize risks and offer guidance to security teams to help them remediate the most high-risk threats first.

**Web Application Hacking**

**Web application hacker’s methodology**



A web application is a program or software that runs on a web browser to perform specific tasks.  Any web application has several layers – web server, the content of the application that is hosted on the web server and the backend interface layer that integrates with other applications. Web application architecture is scalable and has components which have high availability.

[Ethical Hacking](https://www.knowledgehut.com/it-security/certified-ethical-hacker-v10-training) is the process of the appropriating the web application from its actual user by tinkering in various ways.  The web application hacker needs to have deep knowledge of the web application architecture to successfully hack it. To be a master, the hacker needs to practice, learn and also tinker with the application.

[Web application](https://www.knowledgehut.com/blog/web-development/front-end-web-development-projects) hacking requires tenacity, focus, attention to detail, observation and interfacing. There are many types of web application hacking, and many defense mechanisms available to counter and to protect the application from being hacked.