**Known Vulnerabilities and Exploits**

This paper on known vulnerabilities and exploits provides a detailed overview of common security weaknesses in major systems such as Windows, VMware ESXi, Apache, and PHP. Its primary objective is to highlight critical vulnerabilities like EternalBlue, BlueKeep, PrintNightmare, and various buffer overflow and remote code execution threats, explaining how attackers exploit these weaknesses to gain unauthorized access or disrupt services. The paper also emphasizes mitigation strategies and the importance of proactive security measures to reduce risk.

This work is valuable for cybersecurity because it demonstrates an understanding of real-world threats, their technical mechanisms, and practical defenses. It shows the ability to recognize system weaknesses, assess risk, and implement strategies to protect sensitive data and network infrastructure.

The relevance to cybersecurity is reinforced through its discussion of mitigation strategies, including regular system updates, strict access controls, input validation, network segmentation, and firewalls. The paper also covers monitoring tools like IDS, SIEM, and log analysis to detect and respond to incidents quickly. By combining knowledge of vulnerabilities with defensive measures, this work reflects critical skills in threat assessment, risk management, and proactive system protection—core competencies required for effective cybersecurity practice.

**Windows**

1. **EternalBlue (CVE-2017-0144)**
   * Description: A vulnerability in the Server Message Block protocol that allowed remote code execution. This protocol is used to share any files as if they were locally stored. This vulnerability does not need user interaction to spread across the network (Microsoft, 2017).
2. **BlueKeep (CVE-2019-0708)**
   * Description: A vulnerability in Remote Desktop Services that allows remote code execution. This was discovered after a Remote Desktop Protocol implementation. The more developed hackers were able to target weak systems and break through with their own specially crafted code. This vulnerability did not need user interaction for the hackers to get into systems that were left unprotected (Microsoft, 2019).
3. **PrintNightmare (CVE-2021-34527)**
   * Description: A vulnerability in the Windows Print Spooler service that allows remote code execution. Attackers were able to gain SYSTEM-level access and put bugs in the Drivers. The attackers also had the ability to spread this vulnerability through the network without additional user input (Microsoft, 2021).

**Hypervisor (VMware ESXi)**

1. **ESXi OpenSLP Heap-Overflow (CVE-2021-21974)**
   * Description: A vulnerability in the OpenSLP service; a service that is used for location and configuration within a network. Unprotected systems were vulnerable when programs wrote more data to a buffer than it could hold. This access of data would cause an overflow that would allow attackers to get through and push the attacks without further user input through the network (VMware, 2021).
2. **ESXi Unauthorized Access (CVE-2020-3992)**
   * Description: The ESXi hosts are physical servers that can run multiple virtual machines with their own operating systems and applications. This vulnerability allowed hackers to gain Administrative privileges access to the ESXi host (VMware, 2020).
3. **ESXi Directory Traversal (CVE-2019-5544)**
   * Description: A vulnerability that allowed hackers to gain access to directory files without proper access data and files (VMware, 2019).

**Apache 2.X**

1. **Path Traversal (CVE-2021-41773)**
   * Description: This vulnerability allowed attackers to gain access to web files through an unencrypted URL path. The issue arose due to a change in the path normalization process, which inadvertently broke the techniques used to encode the URL path (Apache, 2021).
2. **HTTP Request Smuggling (CVE-2021-40438)**
   * Description: This vulnerability allowed attackers to smuggle HTTP requests without having the proper access credentials. They then used this vulnerability to pass code to the server that was not intended by the user (Apache, 2021).
3. **Buffer Overflow (CVE-2017-7679)**
   * Description: A buffer overflow vulnerability that allowed remote code execution. This affected the mod\_mine module which is responsible for directing the correct MIME type of files on a given server. Because the MIME type of files were vulnerable, an HTTP request could be sent out with a malicious Content-Type header. If this header was opened, a malicious remote code could potentially allow attackers to gain access to the entire affected system (Apache, 2017).

**PHP**

1. **Remote Code Execution (CVE-2019-11043)**
   * Description: This vulnerability was open to data breach via buffer overflow by attacking the NGINX server that had PHP-FPM or FastCGI Process Manager enabled (PHP, 2019).
2. **Deserialization Vulnerability (CVE-2019-11034)**
   * Description: The deserialization vulnerability allowed harmful code through by attacking the exif extension. The deserialization process is manipulated to take in affected script through a PHP application and crash or gain access to the system once the corrupted data attempts to be converted back to an object for a program to use (PHP, 2019).
3. **Remote File Inclusion (RFI)**
   * Description: A well-known vulnerability that allows unwanted code to be executed via a user input field if a user’s input is not properly validated (PHP, n.d.).

**Mitigation Strategies**

* **Regular Updates**: Keep all systems up to date with the latest updates. They may contain fixes that you may be unaware of or be experiencing currently. Alongside the regular updates, have standard work in place to keep an eye out for potential threats. This would take on the action of being proactive rather than reactive (Microsoft, n.d.).
* **Access Controls**: Implement strict access controls to limit access to sensitive services and interfaces (NIST, 2019).
* **Input Validation**: Validate and sanitize all user input to prevent injection attacks. Put an encryption on data prior to reaching the server that way it’s encrypted if it gets intercepted (OWASP, 2021).
* **Network Segmentation**: Implement network segmentation. Separate different business units into their own LAN network to separate data. If there is an attack on one LAN, the remaining data is not compromised. Isolating critical services also limits the impact of potential breaches (Cisco, 2020).
* **Firewalls**: Firewalls are usually implemented with different Operating systems automatically, but additional blockage can protect the company further. Firewall rules can restrict access to the web server and other critical services (Fortinet, 2021).

**Security Software and Hardware Components**

* **Web Application Firewall (WAF)**: This Firewall is used to monitor and filter through HTTP traffic, adding a layer of protection for Zeus’ company. This protects against common web attacks such as SQL injections and cross-site scripting (XSS). This could be hardware, virtual or a cloud-based service (Cloudflare, n.d.).
* **Intrusion Detection System (IDS)**: The IDS monitors network traffic for suspicious activity and potential threats. If anything is detected, an alert is sent out. IDS uses a database of known attack signatures to flag potential threats (Snort, 2021).
* **Antivirus Software**: Protects against malware and other malicious software. Antivirus software also provides an additional layer of firewall that blocks unauthorized access to the site (Symantec, 2021).
* **SSL/TLS Certificates**: Encrypts data transmitted between the web server and clients to protect against eavesdropping and man-in-the-middle attacks (Let's Encrypt, 2021).

**Monitoring and Alerting**

* **Log Monitoring**: Regularly monitor server logs for suspicious activity and potential threats. Log monitoring provides real-time alerts to allow for immediate response (Splunk, 2021).
* **Security Information and Event Management (SIEM)**: Use SIEM tools to collect, analyze, and correlate security events from various sources. This will ensure the company is not blindsided by a potential threat (ELK Stack, n.d.).
* **Automated Alerts**: Configure automated alerts to notify administrators of potential security incidents (PagerDuty, 2021).
* **Regular Audits**: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses (ISACA, 2019).

**References**

Apache. (2017). Buffer overflow (CVE-2017-7679). Retrieved from <https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2017-7679>

Apache. (2021). Path traversal (CVE-2021-41773). Retrieved from <https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-41773>

Apache. (2021). HTTP request smuggling (CVE-2021-40438). Retrieved from <https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-40438>

Cisco. (2020). Network segmentation. Retrieved from <https://www.cisco.com/c/en/us/solutions/enterprise-networks/segmentation.html>

Cloudflare. (n.d.). Web application firewall (WAF). Retrieved from <https://www.cloudflare.com/en-gb/waf/>

ELK Stack. (n.d.). Security information and event management (SIEM). Retrieved from <https://www.elastic.co/siem>

Fortinet. (2021). Firewalls. Retrieved from <https://www.fortinet.com/products/firewall.html>

ISACA. (2019). Regular audits. Retrieved from <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/regulatory-compliance-vs-security-what-are-the-differences>

Let's Encrypt. (2021). SSL/TLS certificates. Retrieved from <https://letsencrypt.org/>

Microsoft. (n.d.). Regular updates. Retrieved from <https://support.microsoft.com/en-us/help/12373/windows-update-faq>

Microsoft. (2017). EternalBlue (CVE-2017-0144). Retrieved from <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144>

Microsoft. (2019). BlueKeep (CVE-2019-0708). Retrieved from <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

Microsoft. (2021). PrintNightmare (CVE-2021-34527). Retrieved from <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527>

NIST. (2019). Access controls. Retrieved from <https://csrc.nist.gov/glossary/term/access_control>

OWASP. (2021). Input validation. Retrieved from <https://owasp.org/www-project-cheat-sheets/cheat-sheets/Input_Validation_Cheat_Sheet.html>

PHP. (2019). Deserialization vulnerability (CVE-2019-11034). Retrieved from <https://php.net/security/CVE-2019-11034>

PHP. (2019). Remote code execution (CVE-2019-11043). Retrieved from <https://php.net/security/CVE-2019-11043>

PHP. (n.d.). Remote file inclusion (RFI). Retrieved from <https://php.net/security/RFI>

Snort. (2021). Intrusion detection system (IDS). Retrieved from <https://www.snort.org/>

Splunk. (2021). Log monitoring. Retrieved from <https://www.splunk.com/>

Symantec. (2021). Antivirus software. Retrieved from <https://www.symantec.com/>