CSS300 Vulnerability Assessment and Management

Vulnerability Assessment Project

Hunter Morrison

April 23, 2019

Table of Contents

[Intrusion Tools and Techniques 4](#_Toc8210769)

[Intrusion Detection 4](#_Toc8210770)

[Intrusion Detection/Prevention Systems 4](#_Toc8210771)

[Auditing 5](#_Toc8210772)

[Audit Data Storage 5](#_Toc8210773)

[Audit Data Purpose 6](#_Toc8210774)

[Audit Data Review 6](#_Toc8210775)

[When to Conduct an Audit 6](#_Toc8210776)

[How to Review Audit Data 7](#_Toc8210777)

[Common Vulnerabilities and Exposures 8](#_Toc8210778)

[Definition of CVE 8](#_Toc8210779)

[Calculation of CVSS 8](#_Toc8210780)

[What is CVSS? 8](#_Toc8210781)

[How it is Calculated 8](#_Toc8210782)

[My Company 9](#_Toc8210783)

[The use of NVD 9](#_Toc8210784)

[Attack Methods 11](#_Toc8210785)

[Active and Passive Attacks 11](#_Toc8210786)

[Active 11](#_Toc8210787)

[Passive 11](#_Toc8210788)

[Authenticated and Unauthenticated Attacks 12](#_Toc8210789)

[Authenticated Attacks 12](#_Toc8210790)

[Unauthenticated Attacks 13](#_Toc8210791)

[Relation to Active and Passive Attacks 13](#_Toc8210792)

[Intrusion Detection System Policies 15](#_Toc8210793)

[Purpose of policies 15](#_Toc8210794)

[Incident Handling Policy in the Organization 15](#_Toc8210795)

[Protective Measures 18](#_Toc8210796)

[Tool Used 18](#_Toc8210797)

[Scan Results 18](#_Toc8210798)

[Works Cited 21](#_Toc8210799)

# Intrusion Tools and Techniques

## Intrusion Detection

Being that a company’s systems, servers, and networks contain their most important and valuable data, there has to be ways to prevent intrusion and know when it is happening. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can work hand in hand to tell when an attack is or was attempted and then stop it with minimal to no damage done. These systems are able to do this by monitoring traffic and either actively preventing it or alerting system admins (“Security: IDS vs. IPS Explained”, 2014).

### Intrusion Detection/Prevention Systems

An IDS constantly monitors traffic on the network and, based on anomalies, is able to determine when or if an attack is being attempted. An anomaly can either be a packet that is not normal traffic (if the IDS is behavior based) or something that doesn’t conform to the rules for allowed traffic (“Security: IDS vs. IPS Explained”, 2014). Once the IDS believes that an attack is occurring it is able to alert to the intrusion to allow for countermeasures to be taken against the issue. While an IDS does not directly act upon a threat, it is like a neighborhood watch program that looks for suspicious activity and then alerts the authorities or in this case systems admins and/or programs that do deal with threats.

An IPS on the other hand handles the attack and actually attempts to prevent it (“Security: IDS vs. IPS Explained”, 2014). The IPS is set in place to prevent certain packets from gaining access to the network or system. These systems detects and then attempts to actively prevent the attack (“Security: IDS vs. IPS Explained”, 2014). The best way to simply explain an IPS is as a customs agent. The IPS checks the incoming traffic for potentially harmful packets and turns them away if they are suspicious or raise any kind of red flag. An IPS is also sometimes able to "grab" the intruder and trap them for identification purposes. This would be considered intrusion deflection. This is a way to make an intruder think they have gained access by putting them into a controlled environment, or honeypot, to keep them busy so that they can be identified (Gupta, 2018).

## Auditing

According to Gadi Eichhorn, a data audit is a process by which data quality and/or utility are carefully assessed. This requires the use of key metrics rather than the quantity of data to determine the overall quality of the dataset being audited. This is essentially a process where every step of the data handling and manipulation process is carefully examined to ensure that all data is of the highest possible quality.

One of the largest issues in data quality, and most important things to take into account during a data audit, is human error. Humans cannot be perfect, therefore there is a certain degree of error to be expected when we are the point of entry for most data sets. It was found that the human error rate can be as high as 10% (Eichhorn, 2014). This can be extremely problematic for a company due to its effect on customer service and even legal proceedings. By accounting for humans, it can become much easier to catch errors in data during an audit and continuously improve the quality by correcting for mistakes that the non-machines may not be able to find otherwise (Eichhorn, 2014). Although other factors can cause inaccuracy, this is one of the largest causes. Just because it was collected and reviewed, does not mean it is 100% accurate. It is entirely possible for mistakes to be overlooked or hidden from the auditors and their tools. In other words, there is never a guarantee of 100% accuracy and security of data.

### Audit Data Storage

Due to the sensitive nature of audit data, the log files and related data should be stored on a separate and hardened server (Gupta, 2018). By using a separate server for storage, it becomes more difficult to gain access to the data without proper permissions. It is also a good idea to configure these servers to shut down if there are any difficulties within the system or if the server becomes full (Gupta, 2018). If the server shuts down when difficulties are encountered, then it should shut down if an intruder attempts to gain access to alter logs and cover their tracks.

### Audit Data Purpose

The data obtained from an audit can be used for many purposes. According to Gadi Eichhorn, the audit data is used to:

* “Ensure the end-to-end integrity of data activities by identifying when modifications are made.”
* “Detect and analyze intentional and accidental breaches in user behavior.”
* “Monitor and analyze the database activities of any user.”
* “Keep track of changes and updates made to data.”

These results can then be used as evidence in a legal case, to determine whether an employee is capable of performing their duties, or to help remedy any problematic protocols and improve security. In the end the audit data is used to help protect and improve the company’s data handling.

## Audit Data Review

### When to Conduct an Audit

While many times an audit may be conducted because of a breach, but this should not be the case if best practices are followed. It is much better to conduct an audit regularly to keep security practices up to date and effective against the everchanging world of technology (Fennelley, n.d.). This will greatly reduce the likelihood of a successful attack occurring and keep clients/investors at ease. Invested parties ease of mind is consequentially another reason an audit may be conducted. Many times, a party may request to see the results of a current audit before agreeing to do business with the company (Fennelley, n.d.). If the audit results are not satisfactory, deals may fall through giving more reason to conduct audits regularly.

### How to Review Audit Data

To get the most out of an audit the review of the data must be thorough and specific to the company. A generalized approach or checklist signifies an ineffective audit and auditor that does not take the weight of the situation seriously (Fennelley, n.d.). Starting the audit by reviewing the company’s security policies gives a foundation of what is and isn’t acceptable risk. This sets a standard to compare the current risks to and to begin suggesting remedies to the current policies. Carole Fennelly states that the auditor should also use experts on particular areas of the systems to find more specific issues as well as a lineup of reputable tools. If this is done, the reports should then be detailed and contain the auditor’s interpretation of the findings as they relate directly to current policies, including suggested remedies to currently perceived problems (tech target).

The audit report should allow the company to determine which fixes are essential and which ones are less pressing. To make these decisions they must look at effect the problems may have on the company. Whether it be possible legal trouble, monetary losses, impact on reputation, etc. (Fennelley, n.d.). All of which should be outlined and easily reviewable by the IT team and their superiors in any report conducted by a quality auditor.

# Common Vulnerabilities and Exposures

## Definition of CVE

In vulnerability assessment and management, vulnerabilities must be identified before they can be mitigated. To assist the team with threat identification, there is a catalog called the Common Vulnerabilities and Exposures (CVE). The CVE catalog is sponsored by the U.S. Department of Homeland Security (DHS) and is comprised of known security threats (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015). The threats found in the catalog are categorized as vulnerabilities and exposures (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015). According to Margaret Rousse, a vulnerability, for the sake of the CVE, is defined as “a mistake in software code that provides an attacker with direct access to a system or network,” while an exposure would be the same except it provides a hacker with indirect access to a system or network rather than direct access. The great thing about the CVE is that it allows administrators to quickly and easily access technical information about a threat (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015).

## Calculation of CVSS

### What is CVSS?

CVSS stands for Common Vulnerability Scoring System. It is a framework designed to allow organizations to measure and score vulnerabilities numerically so that they can be more easily prioritized (“VULNERABILITY METRICS”, N.D.). The system provides accurate and consistent impact scores to be used in the calculation of the severity of vulnerabilities discovered on a system (“VULNERABILITY METRICS”, N.D.).

### How it is Calculated

CVSS is calculated using three separate severity rating scores along with a specific algorithm (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). Those 3 scores, or metrics, are base (deals with inherent qualities of a vulnerability), temporal (represents the qualities of a vulnerability that change over time), and environmental (represents the vulnerabilities qualities that are specific to the user’s environment) (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). The difference between the base and temporal scores is that the temporal is affected by external events while the base deals solely with the qualities directly related to the vulnerability (“VULNERABILITY METRICS”, N.D.). These scores range from 0.0 to 10.0 with the higher score being the most severe (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). The NVD (National Vulnerability Database) breaks the scores down into ranges of low (0.0 – 3.9), medium (4.0 – 6.9), and high (7.0 – 10.0).

### My Company

In my company, like most, we have a website which indirectly uses WordPress. According to CVSS, there is a vulnerability (CVE-2019-10637) with WordPress that allows attackers to become an admin by changing the email address on the profile and then resetting the password with a simple forgotten password link (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). This is particularly worrisome because with very little effort someone can easily take over the company’s website. The company is also vulnerable to CVE-2019-0856 that allows remote code execution if Windows improperly handles objects in memory (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). This is particularly dangerous due to how easily a windows system can become overloaded in the typical work environment causing mishandling of memory objects. A similar vulnerability (CVE-2019-0828) exists in the Excel software when memory objects are handled properly (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). In a business that relies on spreadsheets this can be problematic, but easily fixed by using a different spreadsheet software.

## The use of NVD

The NVD is a database that works alongside the CVSS to provide calculated scores for many vulnerabilities, but currently only provides base scores (“VULNERABILITY METRICS”, N.D.). This is particularly important to understand because most organizations use the CVSS and the NVD helps break it down even more for easy classification of scoring. NVD is tool used for security management and compliance in order to help understand CVSS vulnerability scores and rankings (“VULNERABILITY METRICS”, N.D.).

# Attack Methods

## Active and Passive Attacks

Active and passive attacks differ in that one intercepts and alters, while the other intercepts and analyzes (“Difference Between Active and Passive Attacks”, 2018).

### Active

In an active attack, a hacker will intercept the connection to modify the information or send a fake message (“Difference Between Active and Passive Attacks”, 2018). This is typically quite difficult, as well as dangerous, to pull off (“Difference Between Active and Passive Attacks”, 2018). The danger comes from the fact that the person being attacked can become aware of the hacker’s presence very easily. An active attack could be in the form of an interruption, modification, or fabrication (“Difference Between Active and Passive Attacks”, 2018). These types of active attacks are not system specific and therefore can be carried out on any operating system including Windows as well as Linux/Unix. An interruption, also known as a masquerade, is when the hacker intercepts the connection and attempts to pose as the other person (“Difference Between Active and Passive Attacks”, 2018). Modification is a combination of a replay attack and alteration. First the attacker sends the original user a series of captured events to keep things moving and looking okay, then the message is altered in the second step (“Difference Between Active and Passive Attacks”, 2018). Then there is the fabrication which causes a denial of service (DoS). The hacker poses as an authorized user to gain access and then denies the actual authorized user access (“Difference Between Active and Passive Attacks”, 2018).

### Passive

Unlike an active attack where modifications are made to connections and messages, a passive attack is more like a reconnaissance mission. During these attacks the hacker is typically only eavesdropping on the victim to gather useful information (“Difference Between Active and Passive Attacks”, 2018). This also makes it a much safer attack to perform and much more difficult for the affected system to detect the intrusion (“Difference Between Active and Passive Attacks”, 2018). To perform these attacks, malware is often used. Much like active attacks, the ways of conducting a passive attack are the same from operating system to operating system. The only real difference between an attack on a Windows system and a Linux/Unix system is the code used to carry it out. The attack itself will exploit a similar vulnerability and achieve the same purpose regardless of the base operating system. Some examples of these attacks are keystroke loggers, email scrubbers, and the interception of packets (DiGiacomo, 2017). Through keystroke loggers the hacker can record what keys are pressed when and determine passwords, birthdates, social security numbers, and other sensitive information (DiGiacomo, 2017). The same information can be found from the email scrubbers or from intercepting packets sent to or from the target and then decrypting the information. Often times this information is then auctioned off on the dark web to whoever is willing to pay the highest price (DiGiacomo, 2017).

## Authenticated and Unauthenticated Attacks

### Authenticated Attacks

Authenticated and unauthenticated attacks are, as the prefix 'un' suggests, essentially opposites. An authenticated attack is an attack that gains access by targeting the authentication process (“Authenticated and Unauthenticated Attack”, 2018). This would entail the hacker gaining access to the system/network by using a trusted individual's credentials and then performing the attack. A couple examples of authenticated attacks could be a brute force attack or a weak password recovery process (“Authenticated and Unauthenticated Attack”, 2018). In the brute force attack the hacker uses automated processes to carry out the action of guessing credentials and gaining access. The automated processes can be used to guess login ID's, passwords, cryptographic keys, and credit card numbers of the user. On the other hand, weak password recovery process can allow a hacker to easily gain access to the targeted individuals website and change their email for password recovery. This then allows them to change the password to whatever they want and gain full access and then carry out their attack.

### Unauthenticated Attacks

An unauthenticated attack is used by an attacker who does not want to attempt to obtain login credentials to perform the attack (“Authenticated and Unauthenticated Attack”, 2018). Instead the hacker will exploit a vulnerability in the system to bypass security controls and carry out an attack. The attack is typically motivated by a malicious intent to gain sensitive information about the targeted user(“Authenticated and Unauthenticated Attack”, 2018). Examples of these attacks include phishing scams, and reconnaissance attacks. In the phishing scam a well-versed individual may conduct a phone call posing as a representative from the target’s financial institution or another place that holds protected information for the target. In either case they would have a script and quick improv skills to obtain typically hard to obtain information that would allow them to gain access to the target’s information. In the reconnaissance attack the user can determine the vulnerability of the SIP machine by sending an invite to the target. SIP (Session Initiation Protocol) is used by most companies as a resource for free and high quality internal and external communication (Unuth, 2019). The attacker can then analyze the feedback from the sent message to determine the vulnerability of the targets SIP machine. This attack is used not to directly gain access, but to gain information to determine the best way to attack (“Authenticated and Unauthenticated Attack”, 2018).

### Relation to Active and Passive Attacks

Authenticated attacks can be used to perform active or passive attacks by allowing the hacker to gain the access required to intercept and modify connections and messages. While not all attacks require an authenticated attack to be pulled off, attacks become easier to perform when access is more available. This means that an authenticated attack is often the start of active and passive attacks. Unauthenticated attacks can also be used to assist active and passive attacks. The reconnaissance of an unauthenticated attack is a logical way to start any hack. After all, to carry out any plan successfully, information of what and how it must be done is essential. By learning some sensitive information through unauthenticated attacks, the hacker can learn the information needed to begin and carry out an interruption, fabrication, or interception attack.

# Intrusion Detection System Policies

## Purpose of policies

Policies are a fundamental part of a company’s security infrastructure. Without proper policies, it would be difficult to prevent many breaches as well as to properly handle the aftermath of an incident. Well written policy can protect the organization from avoidable mistakes as well as keep it running smoothly in the event of an incident (Poundstone, 2015). According to Jessica Poundstone, organizations put policies into place to maintain a safe and respectful workplace for employees and consumers while protecting the company from litigation and criminal misconduct (2015). In the end the purpose of a company’s policies is to protect them from legal issues as well as incidents and provide a guideline for the mitigation of these issues should they arise.

## Incident Handling Policy in the Organization

To properly handle an incident, priority levels must be set based on the level of threat the issue presents to the organization. Each level, typically a minimum of three, has a set of guidelines for how quickly the issue must be handled. The first level would likely have an incident response within an hour of discovery, the second level within a couple of hours of discovery, and the third level within at least a day of discovery (“Incident Management Policy”, 2018). This would be determined after detection which can be done in multiple ways. According to the National Institute of Standards and Technology,

“Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect,” (Cichonski et all., 2012).

The incident should then be entirely resolved or have a solution planned within two hours at level one, twenty-four hours at level 2, and a minimum of 5 working days at level 3 (“Incident Management Policy”, 2018). To start resolving the incident systems and networks should be compared to an initial profiling which determines the normal characteristics and metrics to compare against (Cichonski et all., 2012). This would allow for a more accurate and thorough analysis can be made and changes can be identified. To help in this process and ensure that incidents are “handled and resolved in a timely manner,” and incident tracking system will be utilized (Cichonski et all., 2012). In this organization the incident tracking system will need to include:

* “The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
* A summary of the incident
* Indicators related to the incident
* Other incidents related to this incident
* Actions taken by all incident handlers on this incident
* Chain of custody, if applicable
* Impact assessments related to the incident
* Contact information for other involved parties (e.g., system owners, system administrators)
* A list of evidence gathered during the incident investigation
* Comments from incident handlers
* Next steps to be taken (e.g., rebuild the host, upgrade an application),” (Cichonski et all., 2012).

Each incident will be required to be communicated to the CIO, security staff, and potentially law enforcement depending on the scope of the incident. It will be determined at this point what other parties are affected by the incident, or must know to mitigate the issue, including the consumers if their services are affected (Cichonski et all., 2012).

With the incident identified and the necessary parties identified, the organization moves to analysis and recovery. In this step the IP addresses of the attackers will be verified and research done into them. This research will be done in an attempt to determine identity and other information about the attack (Cichonski et all., 2012).

Once properly resolved through these processes, meetings must take place to discuss the incident and create policies to prevent a duplicate from ever happening again. These policies must be well established in writing and communicated throughout the organization to make all staff aware of the potential issue. If well communicated, the policies should prevent the same incident from occurring again within the organization.

# Protective Measures

## Tool Used

My company, Ullr Athletics, uses a security software called GamaScan to protect the organization’s website. This software finds weaknesses in web applications such as our website, ullrathletics.com. According to the GamaSec website home page, GamaScan is able to identify cross site scripting, SQL injection, code inclusion and more (Gamasec, n.d.). This software is also able to produce high level reports that rank threat priority and provide detailed reports (GamaSec, n.d.).

## Scan Results

Figure 1: Number of Vulnerabilities on UllrAthletics.com

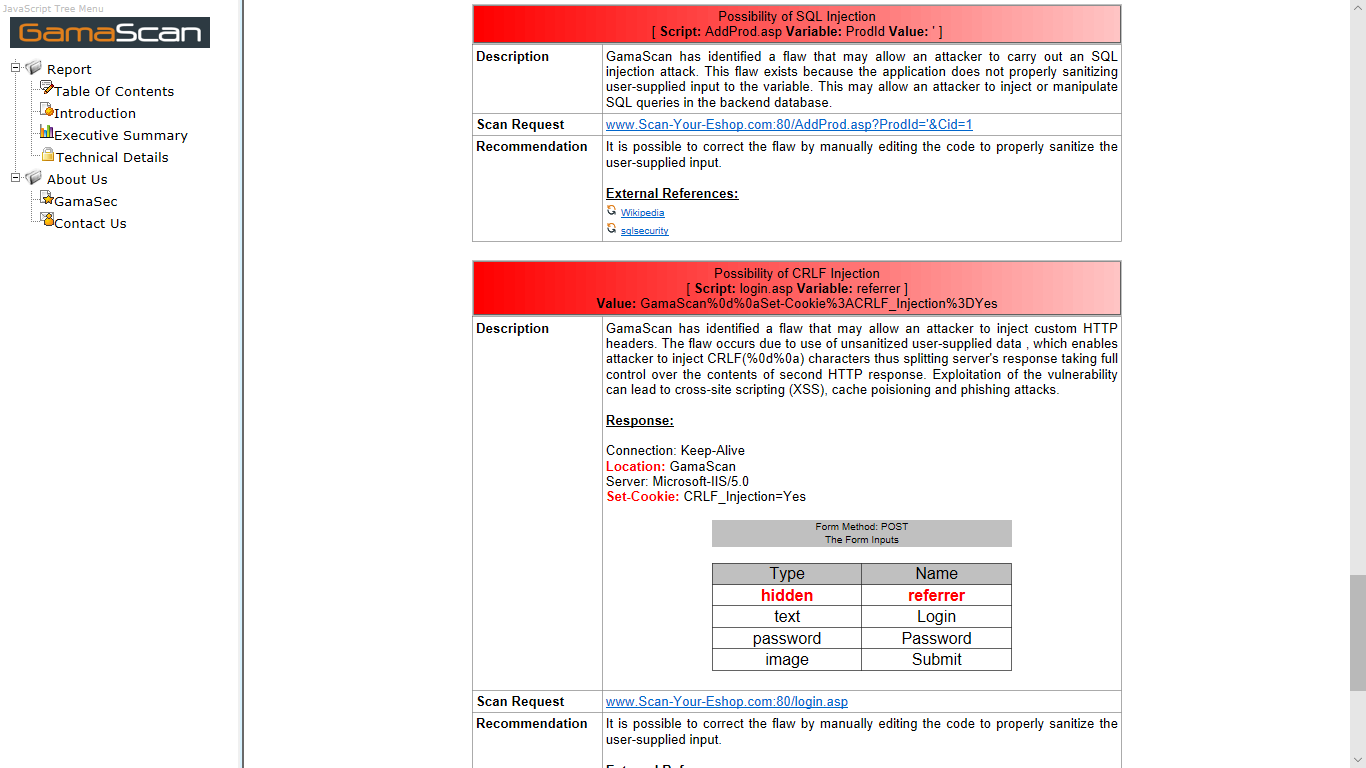
As illustrated by figure 1 above, there are only 10 high level vulnerabilities currently on the website. Being that this is a new platform, it is surprising that there are not more potential issues. After the scan there were no identified incidents and no reports of false positives. The 10 high level risks that are currently present are split between two types of threats. These potential attacks are SQL injection and CRLF injection. Figure 2 illustrates these risks. The possibility of SQL injection can allow an attacker the ability to inject SQL queries on the back end and manipulate information. A potentially more dangerous threat illustrated by GamaScan was the possibility of a CRLF injection. CRLF injections allow the attacker to manipulate HTTP headers and perform cross site scripting attacks and phishing scams by taking over the HTTP response. This can lead to the attacker gaining access to the website and attached databases to steal and/or manipulate data. Correction of both vulnerabilities can be achieved by manually manipulating the code to properly sanitize user input preventing the ability of attackers to intercept and attempt to conduct a SQL or CRLF injection.

Figure 2: High Risk Vulnerabilities

# Works Cited

Authenticated and Unauthenticated Attack. (2018, March 27). Retrieved April 23, 2019, from <https://bohatala.com/authenticated-and-unauthenticated-attack/>

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer Security Incident Handling Guide [PDF]. Gaithersburg: National Institute of Standards and Technology.

DiGiacomo, J. (2017, February 14). Active vs Passive Cyber Attacks Explained. Retrieved April 23, 2019, from https://revisionlegal.com/cyber-security/active-passive-cyber-attacks-explained/

Difference Between Active and Passive Attacks (with Comparison Chart). (2018, February 2). Retrieved April 23, 2019, from https://techdifferences.com/difference-between-active-and-passive-attacks.html

Eichhorn, G. (2014, October 14). Why exactly is data auditing important? Retrieved April 10, 2019, from https://www.realisedatasystems.com/why-exactly-is-data-auditing-important/

Fennelley, C. (n.d.). IT security auditing: Best practices for conducting audits. Retrieved April 10, 2019, from <https://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits>

Gamasec. (n.d.). Retrieved May 8, 2019, from http://www.gamasec.com/Gamascan.aspx

Gupta, A. (2018, August 16). What are Honeypots and how can they secure computer systems. Retrieved April 10, 2019, from <https://www.thewindowsclub.com/what-are-honeypots>

Incident Management Policy – Template And Procedure. (2018, February 13). Retrieved May 2, 2019, from http://itil-docs.com/incident-management-policy/

Poundstone, J. (2015, June 16). None. Retrieved May 1, 2019, from https://www.navexglobal.com/blog/article/ten-things-every-employee-should-understand-about-purpose-workplace-policies/

Rouse, M. (2015, April). What is Common Vulnerabilities and Exposures (CVE)? Retrieved April 17, 2019, from https://searchfinancialsecurity.techtarget.com/definition/Common-Vulnerabilities-and-Exposures

Rouse, M. (2016, August). What is CVSS (Common Vulnerability Scoring System)? Retrieved April 17, 2019, from https://searchsecurity.techtarget.com/definition/CVSS-Common-Vulnerability-Scoring-System

Security: IDS vs. IPS Explained. (2014, March 18). Retrieved April 10, 2019, from https://www.comparebusinessproducts.com/fyi/ids-vs-ips

Security Vulnerabilities (CVSS score between 9 and 10). (n.d.). Retrieved April 17, 2019, from <https://www.cvedetails.com/vulnerability-list/cvssscoremin-9/cvssscoremax-10/vulnerabilities.html>

Unuth, N. (2019, April 11). What is SIP and What is it Good For? Retrieved April 23, 2019, from https://www.lifewire.com/what-is-sip-3426669

Vulnerability Metrics. (n.d.). Retrieved April 17, 2019, from <https://nvd.nist.gov/vuln-metrics/cvss>