Spring 2020 CYB 404 – NETWORK SECURITY FINAL EXAM COVERSHEET

LAST NAME	Musku
FIRST NAME	Krushith Reddy
NAU EMAIL	Km3248@nau.edu

Please only write your name and any other identifying information on this coversheet. This will allow me to grade your exam via a single-blind process.

I confirm that I have completed this exam using my own knowledge and have not committed any acts considered "academic dishonesty" according to the University's Academic Dishonesty Policy.

Krushith reddy — Signature:

04/30/2022 — Date:

Instructions: Provide your answer to each question in the box below the question. The provided space should be more than enough for a complete answer. **If you are printing this PDF and writing your answers with pen or pencil, be sure to write very darkly and legibly so the scanned version with your answers appears clearly in Gradescope.**

You must upload your completed exam to BbLearn in a PDF. Failure to do so will result in a zero grade on your exam. You must also ensure that the uploaded PDF has the same page numbers and formatting as the blank exam form you download. Failure to do so will result in half the points from your exam being removed.

Q0. [20 points] Describe how an attacker might launch a distributed denial of service attack via botnet. How might a network engineer mitigate the threat of this type of attack?

The attacker can launch a distributed denial of service attack via botnet in two ways.

1. Direct DDoS attack
2. Reflector DDoS attack

In a direct DDoS attack, the attacker is able to infect a number of sites across the internet with zombie software. DDoS attacks frequently include two types of zombie machines: master zombies and slave zombies. Both machines' hosts have been attacked with malicious programs. The attacker directs and activates the master zombies, who then direct and activate the salve zombies. The employment of two levels of zombies makes tracing the assault back to its source more difficult and creates a more resilient network of attackers. Another layer of machines is added by the Reflector DDoS attack. In the packet's IP header, the slave zombies include the target's IP address as the source IP address, demanding a response. These packets are transmitted to reflectors, which are machines that are not infected. Uninfected machines respond by sending packets to the infected machine. A reflector DDoS attack can potentially involve more devices and traffic than a direct DDOS attack, resulting in greater damage. Furthermore, because the assault originates from widely spread uninfected devices, tracking back the attack or filtering out the attack packets is more challenging.

The first step in a DDoS attack is for the attacker to infect a number of machines with zombie software that will ultimately be used to carry out the attack. The essential ingredients In this phase of the attack are the following:

1. Software capable of launching a DDoS attack. The software must be able to execute on a large number of machines, conceal its presence, interact with the attacker or have some form of time-triggered mechanism, and launch the planned assault against the target.
2. A flaw that affects a vast number of systems. To install the zombie software, the attacker needs get aware of a vulnerability that many system administrators and individual users have failed to repair.
3. The scanning procedure is an approach for detecting vulnerable devices. The attacker starts by looking for and infecting a number of vulnerable machines. The zombie software installed on infected workstations then typically repeats the scanning process until a large distributed network of infected machines has been built.

The network engineer can mitigate the threat of this type of attack in the following ways:

1. **Attack avoidance:** These strategies allow the victim to withstand an attack while still providing service to genuine clients. Techniques include imposing resource consumption policies and making backup resources available on demand. Furthermore, DDoS prevention measures alter internet systems and protocols to lessen the risk of DDoS.
2. **Attack detection:** These techniques aim to detect and respond to an attack as soon as it begins. The target's influence is reduced as a result. The process of detection entails searching for suspicious patterns of behavior. Filtering away packets that are likely to be part of the attack is part of the response.

3. **Identifying the Source of the Attack:** This is the first step in preventing future assaults by identifying the source of the attack. However, if you use this strategy, you will usually not get results quickly enough.

Q01. [5 points] Compare and contrast viruses, worms, and botnets.

Viruses:

A virus is the most basic and well-known type of malicious software. Viruses operate in a particular way that sets them apart from other types of malware.

First, viruses infect other programs. They insert their code into another program with the hope that it will be executed when someone runs the legitimate program. Secondly, viruses self-replicate by infecting other programs they find on a computer.

Apart from trying to spread to other programs, viruses also have a payload. The payload can be anything the virus author wants it to be. Some viruses have benign payloads that don't actually damage anything.

Worm:

Computer worms and viruses are very similar in the sense that they self-replicate and execute a (usually) malicious payload on computer systems. Where they differ is in how they spread. A virus needs a host program to infect and relies on users to spread that infected program using removable storage, email, or another similar transmission method.

A worm exists as its own independent program, not as code attached to a third-party application. They also spread by themselves, without human intervention. So if one computer at a company or school became infected, the program could quickly spread itself to other connected machines. Worms usually use vulnerabilities discovered in operating systems, hardware, or software to run their code without the user having to do anything at all.

Botnet:

A botnet is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks, usually for nefarious purposes. A compromised computer, known as a zombie, is one whose owner is unaware the computer is being controlled remotely by an outsider. Cybercriminals use botnets to send spam via e-mail, spread viruses and other malware, or commit a denial of service attack.

Q02. [10 points] Web scrapers are scripts that open a web page and "read" information on the web page, writing information encountered to files or databases. One way that web scrapers can be used is by opening a Google web search about a person and then traveling to each page returned in response to the query and scraping the content. Based on your understanding of socially engineered attacks, such as spear phishing, how might web scrapers be used to help automate spear phishing attacks?

Spear phishing assaults can be automated with the use of web scrapers. When surfing the web, users may come across pages that appear to be authentic but are actually phishing pages that are meant to appear genuine but are harvesting user data. There are now improved ways to conduct these targeted attacks, including automated personalization services provided on the dark web that connect attackers with persons who utilize web scrapers to gather data from potential targets social media accounts.

Phishers, for example, can learn which employees are more vulnerable to phishing attacks or who has the job titles they need to target, or hackers can learn the names of superiors, ongoing projects, trusted third parties, and essentially everything a hacker could need to craft their message to make it plausible and elicit the appropriate response from their victims.

Q03. [10 points] Describe how intrusion detection systems and firewalls might work synergistically to defend a network.

An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse. A firewall is a device that traffic between a protected or inside network and a less trustworthy or outside network, whereas an intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse.

Network-based IDS, for example, are located next to the firewall in the network perimeter and evaluate traffic as it goes by for protocols, source, destination, content, and traffic already encountered.

Q04. [5 points] Compare and contrast rule-based and statistical anomaly-based intrusion detection. What are the pros and cons to each approach?

Rule-based intrusion detection:

Rule based intrusion detection system detects anomalous behavior by comparing the features of the packets to some predefined rules which are defined by the administrator or which are created by some algorithm through learning. Rule based systems use highly distributable predefined signatures to detect known attacks.

Pros

1. It has a very high detection rate for known attacks.

Cons

1. The selection of features to identify each attack is difficult.
2. For the intrusion detection system to have high detection rate.

Anomaly based intrusion detection:

Anomaly based intrusion detection system is based on the network behavior. The network behavior is defined by the administrator or is learned by the dataset during the training phase of the development of IDS. Rules are defined for normal behavior and abnormal behavior. Example, Snort and Bro-IDS are anomaly based intrusion detection system.

Pros:

1. It has the ability to detect unknown attacks.

Cons:

1. Defining the rule set for intrusion detection is difficult
2. Efficiency of system depends on the fitness of the rule and its testing on the datasets.