Spring 2021
CYB 404 – NETWORK SECURITY
FINAL EXAM
COVERSHEET

LAST NAME	Alamoudi
FIRST NAME	Abdulrahman
NAU EMAIL	aaa858@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.

Abdulrahman Alamoudi
Signature:

29/04/2021
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 implant zombie software on a number of sites distributed throughout the Internet. Often, the DDoS attack involves two levels of zombie machines: master zombies and slave zombies. The hosts of both machines have been infected with malicious code. The attacker coordinates and triggers the master zombies, which in turn coordinate and trigger the slave zombies. The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers. Reflector DDoS attack adds another layer of machines. The slave zombies construct packets requiring a response that contain the target's IP address as the source IP address in the packet's IP header. These packets are sent to uninfected machines known as reflectors. The uninfected machines respond with packets directed at the target machine. A reflector DDoS attack can easily involve more machines and more traffic than a direct DDoS attack and hence be more damaging. Further, tracing back the attack or filtering out the attack packets is more difficult because the attack comes from widely dispersed uninfected machines.

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 that can carry out the DDoS attack. The software must be able to run on a large number of machines, must be able to conceal its existence, must be able to communicate with the attacker or have some sort of time-triggered mechanism, and must be able to launch the intended attack toward the target.

2. A vulnerability in a large number of systems. The attacker must become aware of a vulnerability that many system administrators and individual users have failed to patch and that enables the attacker to install the zombie software.

3. A strategy for locating vulnerable machines, a process known as scanning. In the scanning process, the attacker first seeks out a number of vulnerable machines and infects them. Then, typically, the zombie software that is installed in the infected machines repeats the same scanning process, until a large distributed network of infected machines is created.

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

1. Attack prevention and preemption (before the attack): These mechanisms enable
the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources available on demand. In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS

2. Attack detection and filtering (during the attack): These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target. Detection involves looking for suspicious patterns of behavior. Response involves filtering out packets likely to be part of the attack.

3. Attack source traceback and identification (during and after the attack): This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack.

Q01. [10 points] Compare and contrast viruses, worms, and botnets.

Viruses

Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.

Worms

A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.

Botnets

Program activated on an infected machine that is activated to launch attacks on other machines.

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?

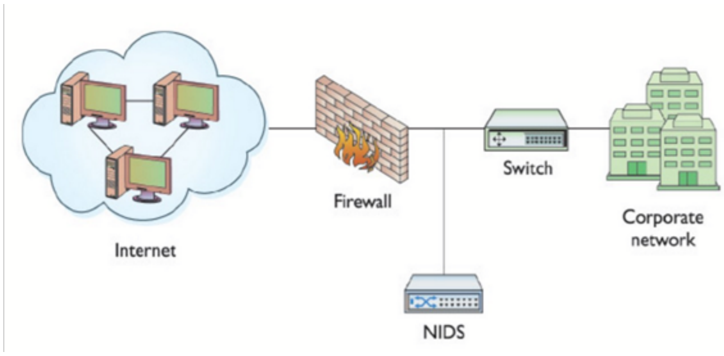
Web scrapers can be used to help automate spear phishing attacks. When surfing the web, users can come across pages that look legitimate, but are really phishing pages that are designed to look genuine but will actually be scraping the user data. There are now better ways to launch these personalized attacks e.g., automated personalization services sold through the dark web that connect attackers with people who use web scrapers to glean information from potential targets social media.

An example of this could be phishers can learn which employees might be more susceptible 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, etc. and essentially everything a hacker could need to craft their message to make it plausible and provoke the correct (rash and ill-informed) response in their victims.

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

A firewall is a device that filters traffic between a protected or inside network and a less trustworthy or outside network whereasan intrusion detection system gathers and analyzes information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse (attack from within the organization).

Intrusion detection system and firewall can work together to defend a network e.g., network-based intrusion detection system are placed next to the firewall on the network perimeter and analyze the traffic as it passes by for the protocols, source, destination, content, traffic already seen etc.



Extra Credit. [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: Involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder.

Pros: Able to recognize events and sequences that reveal penetration.
Cons: Deal only with known attacks

Statistical anomaly-based intrusion detection: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

Pros: Effective against masqueraders who are unlikely to mimic the behavior patterns of the accounts they appropriate
Cons: Unable to deal with misfeasors