**EMCS2020: Advanced Topics in Computer Security**

Assignment: Explaining Operating Systems and Network Security Concepts

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

***Please provide a brief, simple, and informal explanation of the following operating systems and network security concepts. Imagine you are explaining these concepts to a CEO or Board member who does not have a cybersecurity background.***

**Hibernation attack**

A hibernation **file** attack is an attack on the Windows Hibernation File, usually in Windows Vista or below, in an effort to illicitly recover information about Operating System application states and credentials that may exist in memory. The hibernation file potentially holds a trove of memory information from the target machine and is used by Windows as instructions on what to run/initialize when the system is waking from hibernation. This file is not protected by any type of user authentication.

**Why it is impossible to detect all malicious code with 100% certainty?**

Since malicious code often uses existing programs and protocols to execute its malicious intent, it is often hard to distinguish malicious code activity ( it’s signature ) from other processes running on the machine. Often malware will hide by “hooking” existing libraries or processes and streaming information inline with normal traffic previously present on the machine. “Living Off The Land”, has been a popular term in InfoSec that refers to attackers that have gotten extremely skilled at using attack vectors that require minimal foreign code, but instead use programs and processes on the target’s machine.

**Distributed denial of service attack**

A Distributed Denial of Service Attack or DDoS is an attacker’s attempt to affect the availability of and sometimes trigger a fault in an application or service. By bombarding and overloading the server with more fake requests than it can handle, the attacker is hoping that the server with “break” under the load. Furthermore, the attack is conducted in a way that makes the source of attack indistinguishable from real requests, often forcing the target to stop accepting requests from everyone, including real customers. Attackers use bots and previously compromised machines sometimes referred to as “zombies” to orchestrate the attack.

**Rule-based intrusion detection**

A rule-based intrusion detection system is a defender’s attempt to use the analysis of system or network activity ( often log files ) to detect malicious activity. Often the defense includes small agent applications that sit in strategic places in the system to collect data about the activities and another centralized application that analyzes the activity in comparison to the “rules” set up by the system administrator. Deviations, like a user logging in from an unknown location, attempting to escalate privileges or access files that do not belong to the user’s normal domain, may cause the detection system to trigger countermeasures like requiring additional authentication, alerting the user and the admin of the suspicious behavior or even locking the users account or a service.

**Statistical intrusion detection**

Statistical Intrusion Detection, much like Rule-Based Intrusion Detection, is defenders attempt to find intrusion by analyzing network traffic. By profiling multiple characteristics of a user’s network traffic, a statistical intrusion detection system may be able to detect malicious activity simply by comparing the attacker’s network activity with the traffic of a normal user. This system doesn’t require as much of the admin generated rules as the rule-based system and usually relies on some form of machine learning or automated network analysis to run the complex statistical algorithms to find anomalies in network activity that may allude human review.