Research
Chapter 08
CIT 288

Chaz Davis

BCTC
Spring 2020

March 7, 2020

Chapter 08

i) List and briefly define four classes of intruders.

- Cyber criminals: Are either individuals or members of an organized crime group with a goal of financial reward.
- Activists: Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes.
- State-sponsored organizations: Are groups of hackers sponsored by governments to conduct espionage or sabotage activities.
- Others: Are hackers with motivations other than those listed above, including classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation.Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class

ii) List and briefly describe the steps typically used by intruders when attacking a system.

- 1 Target acquisition and info gathering
- 2 Initial Access
- 3 Privilege escalation
- 4 Information gathering and/or system exploit
- 5 Maintaining access
- 6 Covering tracks

iii) Describe the three logical components of an IDS.

- Target Acquisition and info gathering using scam websites to gain access to valuable information.
- Initial Access when the hacker succeeds in guessing passwords and other valuable information
- Privilege Escalation When the attackers have the control to adjust privileges
- Information Gathering and/or System Exploit when the attackers have the ability to modify files inside a target's system
- Maintaining Access when the attackers plant a backdoor or other malware to assure that they have access over time

- Covering Tracks editing log files so the target won't notice any changes

iv) Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?

- Sensor it has responsibility in collecting data; input includes network packets, log files, system call traces.
- Analyzer receiving input from one or more sensors, responsible for determining if an intrusion has occurred. Te output of this component is an indication that an intrusion has occurred and may include evidence supporting the conclusion that an intrusion has occurred.
- User Interface it enables user to view the output of the system, or control the system behavior.

v) Explain the base-rate fallacy.

- Host based IDS monitors the characteristics of a single host and the events occurring within that host for suspicious activity.
- Network-Based IDS Monitors network traffic for a particular network segments and analyzes network, transport, and application protocols to identify suspicious activity.

vi) What is the difference between anomaly detection and signature or heuristic intrusion detection?

- Anomaly Detection Involves the collextion of data relating to the behavior of legitamate users over a period of time. Then, current observed behavior is analyzed to determine with a high level of confidence whether this behavior is that of legitamate user or alternatively that of an intruder.
- Signature or Heuristic detection Uses a set of know malicious data patterns (signatures) or attack rules (heuristics) that are compared with current data behavior to decide if it is that of an intruder. it is also known as misuse detection. This approach can only identify known attacks for which it has patterns or rules.

vii) What is the difference between signature detection and rule-based heuristic identification?

In essence, anomaly approaches aim to define normal, or expected, behavior, in order to identify malicious or unauthorized behavior. They can quickly and efficiently identify known attacks. However, only anomaly detection is able to detect unknown, zero-day attacks, as it starts with known good behavior and identifies anoalies to it. Given this advantage, clearly anomaly detection would be the proferred approach, were it not for the difficulty in collecting and analying the data required, and the high level of false alarms.

viii) What advantages do a Distributed HIDS provide over a single system HIDS?

Traditionally, work on host-based IDSs focused on single-system stand alone operaton. The typical organization, however, needs to defend a distributed collection of hosts supported by a LAN or internetwork. Although it is possible to mount a defense by using stand-alone IDSs on each host, a more effective defense can be acheived by coordination and cooperation among IDSs across the network.

ix) What are possible locations for NIDS sensors?

- Between the external Firewall and the internet
- Just inside the external firwall
- Inside internal Firewalls

  -between desktops/networks and internal firewall

  -between internal firewalls and servers and data resources

x) What is a honeypot?

Honeypots are resources that have no production value. There is no legitimate reason for anyone outside the network to interact with a honeypot. Thus, any attempt to communicate with the system is most likely a probe, scan, or attack. Conversely, if a honeypot initiates outbound communication, the system has probably been compromised.