Midterm

October 16, 2019

Enterprise network security.

Networking:

For each question, **select all that apply**.

1. What does the TTL field keep track of?
   (a) Number of seconds a packet has before it dies.
   (b) Number of milliseconds a packet has before it dies.
   (c) Number of nodes a packet passes through before it dies.
   (d) Number of minutes a packet has before it dies.
2. Suppose I want to completely hide the identity of the websites I am visiting from an observer on my network. Which technology/technologies would I need to use to protect my traffic?
   (a) Tor
   (b) VPN
   (c) SSL/TLS-encryption of traffic
3. The IP layer instructs my packet on how to get to the:
   (a) Server machine.
   (b) Next router.
   (c) Correct process on a machine.
4. The TCP layer instructs my packet on how to get to the:
   (a) Server machine.
   (b) Next router
   (c) Correct process on a machine.
5. The Ethernet layer instructs my packet how to get to the:
   (a) Server machine.
   (b) Next router
   (c) Correct process on a machine.
6. nmap can be used to:
   (a) Detect the operating system of a machine
   (b) Open closed ports on a target machine
   (c) Probe a machine for open ports
7. A TCP packet that is split before arriving at its destination gets reassembled by:
   (a) The receiving machine

(b) The sending machine
(c) The next router that can
(d) The target application

OS containers

For each question, **select all that apply**.

1. Chroot is used to:
   (a) Isolate a PID space
   (b) Isolate a Directory
   (c) Limit System resources (cpu, memory, etc.)
2. When running chroot, you will have access to:
   (a) Only the programs in the folder.
   (b) All programs on the host system.
   (c) All folders in the system.
   (d) Only the folders below the directory chroot was called on.
3. Cgroups are used to
   (a) Isolate a PID space
   (b) Isolate a Directory
   (c) Limit System resources (cpu, memory, etc.)
4. Namespaces are a feature of the Linux operating system that form the basis for containers. Namespaces allow virtualization/isolation of which of these?
   (a) The address space (virtual memory)
   (b) Process IDs
   (c) User IDs
   (d) Network interfaces
   (e) The branch predictor
   (f) Compute resource utilization
   (g) The processor's L2 cache
5. The root directory in a container is, by default, the same as the host machine?
   (a) True
   (b) False

Monitoring

For each question, **select all that apply**.

1. tcpdump is used to.
   (a) Show all the running processes
   (b) Show/record systemcalls
   (c) Show/record network traffic
   (d) Show file input/output information

2. The program “ps” is used to:
   (a) Show all the running processes
   (b) Show/record systemcalls
   (c) Show/record network traffic
   (d) Show file input/output information
3. Sysdig is used to:
   (a) Show all the running processes
   (b) Show/record systemcalls
   (c) Show/record network traffic
   (d) Show file input/output information
4. Iotop is used to:
   (a) Show all the running processes
   (b) Show/record systemcalls
   (c) Show/record network traffic
   (d) Show file input/output information
5. Osquery makes what directory available through SQL like queries:
   (a) /root
   (b) /proc
   (c) /home
   (d) /dev
6. If a machine is running multiple kubernetes containers, sysdig will not see the processes running inside the container.
   (a) True
   (b) False
7. If a machine is running multiple kubernetes containers, osquery will not see the processes running inside the container.
   (a) True
   (b) False

SELinux

For each question, **select all that apply**.

1. SELinux can be used to:
   (a) Enforce Mandatory Access Control on a Linux system.
   (b) Keep an application from writing to sensitive files.
   (c) Alert a user when a process attempts to read a file of a specific type.
2. SELinux is implemented by:
   (a) Default in the Linux kernel.
   (b) A kernel moduel.