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. X
   (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 X
   (b) VPN
   (c) SSL/TLS-encryption of traffic
3. The IP layer instructs my packet on how to get to the:
   (a) Server machine. X
   (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. X
5. The Ethernet layer instructs my packet how to get to the:
   (a) Server machine.
   (b) Next router X
   (c) Correct process on a machine.
6. nmap can be used to:
   (a) Detect the operating system of a machine X
   (b) Open closed ports on a target machine
   (c) Probe a machine for open ports X
7. A TCP packet that is split before arriving at its destination gets reassembled by:
   (a) The receiving machine X

(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 X
   (c) Limit System resources (cpu, memory, etc.)
2. When running chroot, you will have access to:
   (a) Only the programs in the folder. X
   (b) All programs on the host system.
   (c) All folders in the system.
   (d) Only the folders below the directory chroot was called on. X
3. Cgroups are used to
   (a) Isolate a PID space
   (b) Isolate a Directory
   (c) Limit System resources (cpu, memory, etc.) X
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 X
   (c) User IDs X
   (d) Network interfaces X
   (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 X

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 X
   (d) Show file input/output information

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

SELinux

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

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