Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Second Mid-term, 28th May 2019

Student name: _____

Matricola: _____

Open questions (60%)

Provide an answer within the space allocated for each question.

1. Describe how a forward proxy can realize a HTTP tunnel.

2. Briefly describe how a passive vulnerability scanner differs from an active one.

3. Briefly explain the *SSL bumping* mechanism.

4. Briefly describe what a CVE is.

5. Describe how an IPS is different from an IDS.

6. List the ways how a device can dynamically receive a GUA in IPv6.

7. Briefly explain the difference between stateless and stateful addressing in IPv6.

8. Describe the purpose of the event correlation engine in a SIEM.

Student name: _____

Matricola: _____

Multi-choice questions (40%)

Mark all the options you think are correct.

1. Which of the following is NOT a typical operational interface of a SIEM?

   A. Command line ★
   B. Dashboard
   C. Alert
   D. Map

2. In a typical penetration testing procedure

   A. intrusive target search happens before exploitation ★
   B. intrusive target search happens before planning
   C. planning happens after data analysis
   D. non-intrusive target search happens after reporting

3. What is true regarding the detection mechanisms of IDSs?

   A. The signature-based does not rely on detection rules
   B. The behavior-based cannot recognize unknown attacks
   C. The behavior-based relies on detection rules
   D. The signature-based hardly recognize unknown attacks ★

4. Which step happens earlier in a IDS/IPS system?

   A. Flow state table generation ★
   B. Flow Classification
   C. Alert raising
   D. Normalization

5. With respect to the SIEM, the IT Regulatory Compliance

   A. concerns the real-time analysis on the health and security of IT systems
   B. concerns the correlation of events in order to spot patterns of attacks
   C. concerns the validation of the compliance of the security checks against a standard ★
   D. concerns the monitor of endpoint security

6. Concerning the content of a SSL session flowing through a proxy:

   A. it can be examined without a client warning if the proxy is an anonymizer proxy
   B. it can be examined without a client warning if the proxy is the SSL termination ★
   C. it cannot be examined in any case
   D. it cannot be examined without a client warning

7. What is ICAP?

   A. A protocol for modifying managed device behavior on IP networks
   B. A protocol for standardizing remote procedure calls on HTTP contents ★
   C. A protocol for encrypting the HTTP contents
   D. A protocol for requesting contents, alternative to HTTP

8. The `FF02::1` IPv6 address refers to

   A. all DHCP servers within the link-local scope
   B. all the IPv6 devices within the link-local scope ★
   C. all the IPv6 devices within the site scope
   D. all DHCP servers within the site scope

9. What is FALSE regarding a reverse proxy?

   A. It can protect the origin server
   B. It appears to the client as the origin server
   C. It typically makes use of the HTTP CONNECT method ★
   D. It interacts with a server on behalf of the client

10. The Internet Header Length (IHL) field of the IPv4 header packet, in the IPv6 header packet

    A. has been substituted by the Next Header field
    B. has been substituted by the Total Length field
    C. has the same name and meaning
    D. has been removed ★

11. ICMPv6 Router Solicitation messages are sent

    A. by IPv6 devices for requesting a Router Advertisement message ★
    B. by IPv6 devices as part of the Neighbor Discover protocol
    C. by IPv6 routers to announce the prefix of a network
    D. by IPv6 devices for requesting the MAC address of another device in the network

12. In a typical penetration testing, exploitation is

    A. a step to find open ports in a target
    B. a step to find evidences about the feasibility of an attack ★
    C. a step to find live systems
    D. a step to enumerate the services in the system

13. Which of the following is NOT a valid IPv6 address?

    A. `2001:DB8::1234::5678` ★
    B. `2001:DB8:1000::1`
    C. `FE80::EE97:F7C5:F035:20C2`
    D. `FF02::1:FF00:0001`

14. Which of the following requires the users to proper setup its client software?

    A. Forward proxy ★
    B. All the types of proxies
    C. Reverse proxy
    D. Transparent proxy

15. In a IDS, a packet related to a known attack not raising an alarm is

    A. a false negative ★

Student name: _____

Matricola: _____

B. a true negative
C. a true positive
D. a false positive