



UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 2 POSTI DI CATEGORIA D - POSIZIONE ECONOMICA D1 AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI - TECNICO INFORMATICO SPECIALIZZATO PER SUPPORTO AI LABORATORI DI RICERCA DI INFORMATICA, CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO, PRESSO IL DIPARTIMENTO DI INFORMATICA GIOVANNI DEGLI ANTONI, DA RISERVARE, PRIORITARIAMENTE, ALLE CATEGORIE DI CUI AL DECRETO LEGISLATIVO N. 66/2010 - BANDITO CON DETERMINA N. 910/2019 DEL 21.01.2019 E PUBBLICATO SULLA G.U. N. 10 DEL 5.02.2019 - CODICE 19652

TRACCE DELLE PROVE SCRITTE

La Commissione giudicatrice del concorso, nominata con determina n. 8943/2019 del 22.05.2019 e così composta:

PROF. MONGA MATTIA - PRESIDENTE

DOTT. CASELLA GIULIO FRANCESCO - COMPONENTE

SIG.RA ANGELILLO FILOMENA - COMPONENTE

SIG.RA CIERI ELENA - SEGRETARIO

comunica le tracce relative alla prima prova scritta:

TEMA n. 1

1. Considerando una piattaforma *cloud* conosciuta dal candidato per la collaborazione e la condivisione dei dati si discutano le caratteristiche di riservatezza, sicurezza e integrità dei dati.
2. Facendo riferimento ad uno dei seguenti sistemi operativi *server* Windows, Linux, MacOS, il candidato illustri il sistema di gestione degli utenti in presenza di sistemi di autenticazione federata e il controllo degli accessi alle risorse.
3. Il candidato discuta il problema dei falsi allarmi nei sistemi di rilevamento delle intrusioni informatiche (IDS).

TEMA n. 2

1. Il candidato discuta il problema dei falsi allarmi nei sistemi di rilevamento delle intrusioni informatiche (IDS).
2. Il candidato illustri il ruolo di un servizio di *directory* in un ambiente complesso, in cui convivono numerosi dispositivi equipaggiati con sistemi operativi differenti.
3. Il candidato descriva le più comuni vulnerabilità tipiche delle applicazioni *Web-based*.

TEMA n. 3

1. Il candidato descriva il ruolo del protocollo DHCP nella gestione di una rete complessa, suddivisa in numerosi *broadcast domain*.
2. Facendo riferimento ad uno dei seguenti sistemi operativi *server* Windows, Linux, MacOS, il candidato illustri il sistema di gestione degli utenti in presenza di sistemi di autenticazione federata e il controllo degli accessi alle risorse.
3. Il candidato descriva le più comuni vulnerabilità tipiche delle applicazioni *Web-based*.



La Commissione comunica le tracce relative alla seconda prova scritta:

Tema n. 1

\$ tcpdump -qns 0 -A -r traffico.pcap

09:18:14.940358 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:15.176123 IP 159.149.152.9.17500 > 255.255.255.255.17500: UDP, length 189
09:18:15.176387 IP 159.149.152.9.17500 > 159.149.152.255.17500: UDP, length 189
09:18:15.940453 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:16.095830 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:16.940388 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:17.940443 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:18.095845 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:18.291957 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 644
09:18:18.292007 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 14
09:18:18.308032 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 0
09:18:18.311727 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 1246
09:18:18.311742 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 0
09:18:18.940399 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:19.940612 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:20.095799 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:20.940385 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:21.940543 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:22.095826 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102

- Considerando la registrazione di traffico fornita, si dica quali nodi IP è possibile identificare come parte della LAN (broadcast domain) in cui il traffico è stato raccolto. (punteggio massimo 10/30)
- Si progetti l'architettura di una rete complessa in un'organizzazione in cui siano previsti:
 - + servizi a disposizione del pubblico
 - + servizi a disposizione degli utenti (ma non del pubblico)
 - + dispositivi che conservano dati per i quali si vuole ridurre al minimo il rischio di accesso non autorizzato dall'esterno(punteggio massimo 20/30)

Tema n. 2

\$ tcpdump -qns 0 -A -r traffico.pcap

09:18:14.940358 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:15.176123 IP 159.149.152.9.17500 > 255.255.255.255.17500: UDP, length 189
09:18:15.176387 IP 159.149.152.9.17500 > 159.149.152.255.17500: UDP, length 189
09:18:15.940453 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:16.095830 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:16.940388 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:17.940443 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:18.095845 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:18.291957 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 644
09:18:18.292007 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 14
09:18:18.308032 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 0
09:18:18.311727 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 1246
09:18:18.311742 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 0
09:18:18.940399 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:19.940612 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:20.095799 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:20.940385 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:21.940543 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:22.095826 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102



- Considerando la registrazione di traffico fornita, si dica quali nodi IP sono probabilmente coinvolti in una comunicazione HTTP, precisano i nodi client e quelli server. (punteggio massimo 10/30)
- Data una rete locale IP, organizzata in varie sottoreti, il candidato progetti una possibile architettura di rete in cui possano coesistere perimetri separati in modo sicuro, cercando di mantenere il più possibile il piano di indirizzamento IP esistente. (punteggio massimo 20/30)

Tema n. 3

\$ tcpdump -qns 0 -A -r traffico.pcap

```
09:18:14.940358 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:15.176123 IP 159.149.152.9.17500 > 255.255.255.255.17500: UDP, length 189
09:18:15.176387 IP 159.149.152.9.17500 > 159.149.152.255.17500: UDP, length 189
09:18:15.940453 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:16.095830 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:16.940388 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:17.940443 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:18.095845 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:18.291957 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 644
09:18:18.292007 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 14
09:18:18.308032 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 0
09:18:18.311727 IP 178.63.37.166.80 > 159.149.152.12.55771: tcp 1246
09:18:18.311742 IP 159.149.152.12.55771 > 178.63.37.166.80: tcp 0
09:18:18.940399 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:19.940612 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:20.095799 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
09:18:20.940385 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:21.940543 ARP, Request who-has 159.149.152.113 tell 159.149.152.254, length 46
09:18:22.095826 STP 802.1s, Rapid STP, CIST Flags [Proposal, Learn, Forward, Agreement], length 102
```

- Considerando la registrazione di traffico fornita, si dica se è possibile identificare un nodo IP destinatario per ciascuna delle 8 richieste ARP presenti. (punteggio massimo 10/30)
- Dato un sistema di virtualizzazione conosciuto dal candidato (ovirt, vmware, RHV, ...), si descrivano le criticità e le problematiche dell'utilizzo di tale sistema per la virtualizzazione dei computer di un numero cospicuo di aule didattiche universitarie e si progetti un'adeguata architettura della rete con cui questo servizio dovrebbe essere erogato. (punteggio massimo 20/30)

LA COMMISSIONE

PROF. MONGA MATTIA - PRESIDENTE

DOTT. CASELLA GIULIO FRANCESCO - COMPONENTE

SIG.RA ANGELILLO FILOMENA - COMPONENTE

SIG.RA CIERI ELENA - SEGRETARIO