UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 2 POSTI DI CATEGORIA D - 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" – BANDITO CON DETERMINA NR. 13934/2019 DEL 06/08/2019 E PUBBLICATO SULLA G.U. NR. 70 DEL 03/09/2019 - CODICE 20248

TRACCE PROVE SCRITTE

La Commissione Giudicatrice del concorso, nominata con determina n. 17240/2019 del 16/10/2019 e composta da:

PROF. MONGA MATTIA- PRESIDENTE

DOTT. CASELLA GIULIO FRANCESCO - COMPONENTE

SIG.RA ANGELILLO FILOMENA - COMPONENTE

DOTT.SSA DI TOMMASO HENNA MARIA STELLA - SEGRETARIO

comunica le tracce relative alla prima prova scritta:

TRACCIA n. 1

1. Si descriva una possibile strategia di backup di un ambiente di virtualizzazione per server, conosciuto dal candidato.

2. Facendo riferimento ad un sistema operativo conosciuto dal candidato (Windows, Linux, MacOS) si illustri un sistema di autenticazione e autorizzazione federata, evidenziando vantaggi e criticità.

3. Il candidato discuta il problema dei falsi allarmi nei sistemi di attenuazione della posta indesiderata (anti-spam).

4. Il candidato discuta l'efficacia dei sistemi di rilevazione automatica delle vulnerabilità in una rete complessa.

TRACCIA n. 2

1. Il candidato discuta l'efficacia dei sistemi di attenuazione della posta indesiderata (anti-spam).

2. Il candidato illustri una possibile integrazione dei servizi di autenticazione e autorizzazione in ambienti composti da client con sistemi operativi eterogenei (Windows, Linux, MacOS)

3. Il candidato descriva i più comuni attacchi informatici per le applicazioni *Web* non basate su database.

4. Il candidato discuta i rischi dei sistemi di rilevazione automatica delle vulnerabilità attivi, che cioè provano l'efficacia di un attacco conosciuto

TRACCIA 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 un sistema operativo conosciuto dal candidato (Windows, Linux, MacOS) si illustri un sistema di autenticazione e autorizzazione federata discutendone i possibili rischi cui espone.

3. Il candidato descriva i più comuni attacchi informatici alle applicazioni *Web* di tipo CRUD (Create, read, update and delete)

4. Il candidato discuta l'impatto dei sistemi di rilevazione automatica delle vulnerabilità in una rete complessa.

La Commissione comunica le tracce relative alla seconda prova scritta a contenuto teorico-pratico:

TRACCIA n. 1

- Considerando la registrazione di traffico fornita, si elenchino i nodi IP che fanno parte della LAN (broadcast domain) in cui il traffico è stato raccolto.

```
$ 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
09:18:16.940388 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
09:18:18.291957 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
09:18:20.940385 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
```

- Nei file di log di una macchina virtuale accessibile dall'esterno della rete di ateneo si leggono i seguenti dati. Il candidato fornisca un'interpretazione, spiegando quali possibili rischi per la sicurezza della rete sono in gioco.

```
Nov 12 07:01:30 aladdinsrv sshd[8837]: Invalid user admin from 121.137.77.82 port 58963
Nov 12 07:01:32 aladdinsrv sshd[8837]: error: maximum authentication attempts exceeded for
invalid user admin from 121.137.77.82 port 58963 ssh2 [preauth]
Nov 12 07:01:32 aladdinsrv sshd[8837]: Disconnecting invalid user admin 121.137.77.82 port
58963: Too many authentication failures [preauth]
```

- Si descriva lo schema logico di una rete in cui esiste una "zona demilitarizzata" (DMZ), spiegandone le finalità dal punto di vista della protezione.

- Dato il seguente estratto da un file di log di email:

```
Nov 20 08:24:23 mailserver postfix/smtpd[26501]: NOQUEUE: reject: RCPT from fibhost-67-179-
218.fibernet.hu[85.67.179.218]: 554 5.7.1 <pinco.pallino@gmail.com>: Relay access denied;
from=<ForgedAddress@fibernet.hu> to=<pinco.pallino@gmail.com> proto=ESMTP helo=<fibhost-67-179-
218.fibernet.hu>
```

si proponga una possibile causa del fallimento.

TRACCIA n. 2

- Considerando la registrazione di traffico fornita, si elenchino i nodi IP che NON fanno parte della LAN (broadcast domain) in cui il traffico è stato raccolto.

```
$ 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
09:18:16.940388 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
09:18:18.291957 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
09:18:20.940385 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
```

- Nei file di log di una macchina virtuale accessibile dall'esterno della rete di ateneo si leggono i seguenti dati. Il candidato fornisca un'interpretazione, spiegando quali possibili rischi per la sicurezza della rete sono in gioco.

```
concorso.unimi.it:443 123.136.144.118 - - [20/Nov/2019:09:42:44 +0100] "GET /favicon.ico
HTTP/1.1" 404 524 "https://www.google.com/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"
concorso.unimi.it:443 123.136.144.118 - - [20/Nov/2019:09:42:44 +0100] "GET
archive/index.php/%22%3E%3Cimg%20src=0%20onerror=alert('XSS')%3E HTTP/1.1" 200 199803
"https://www.google.com/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36"
```

- Si descriva lo schema logico di una rete in cui esiste un "bastion host", spiegandone le finalità dal punto di vista della protezione.

- Dato il seguente estratto da un file di log di email:

```
Nov 20 10:42:56 mailserver postfix/smtpd[7065]: NOQUEUE: reject: RCPT from out51-
ams.mf.surf.net[145.0.1.51]: 550 5.1.1 <mario.rossi@di.unimi.it>: Recipient address rejected:
User unknown; from=<om-announce-bounces@openmath.org> to=<mario.rossi@di.unimi.it> proto=ESMTP
helo=<out51-ams.mf.surf.net>
```

si proponga una possibile causa del fallimento.

TRACCIA n. 3

- Considerando la registrazione di traffico fornita, si dica fra quali coppie di nodi IP avviene una comunicazione bidirezionale, motivando la risposta.

```
$ 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
09:18:16.940388 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
09:18:18.291957 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
09:18:20.940385 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
```

- Nei file di log di una macchina virtuale accessibile dall'esterno della rete di ateneo si leggono i seguenti dati. Il candidato fornisca un'interpretazione, spiegando quali possibili rischi per la sicurezza della rete sono in gioco.

```
[Wed Nov 20 06:46:53.300765 2019] [php7:error] [pid 4624] [client 209.97.188.148:37362] script
'/home/www/concorso.unimi.it/pub/wp-login.php'  not  found  or  unable  to  stat,  referer:
http://concorso.di.unimi.it/wp-login.php
[Wed Nov 20 08:09:18.496130 2019] [php7:error] [pid 4448] [client 93.113.111.193:44736] script
'/home/www/concorso.di.unimi.it/pub/wp-login.php' not found or unable to stat
[Wed Nov 20 08:09:43.191547 2019] [php7:error] [pid 4447] [client 159.65.53.153:51404] script
'/home/www/concorso.unimi.it/pub/wp-login.php'  not  found  or  unable  to  stat,  referer:
http://concorso.unimi.it/wp-login.php
```

- Si descriva lo schema logico di una rete in cui esiste un "reverse proxy", spiegandone le finalità dal punto di vista della protezione.

- Dato il seguente estratto da un file di log di email:

```
Nov  20  11:00:16  mailserver  postfix/smtpd[7070]:  NOQUEUE:  reject:  RCPT  from  ip123.ip-5-39-
119.eu[5.39.119.123]:  450  4.1.8  <editor@remedypub.ga>:  Sender  address  rejected:  Domain  not
found; from=<editor@remedypub.ga> to=<giulio@di.unimi.it> proto=ESMTP helo=<pmta3.ip112.ip-5-39-
119.eu>
```

si proponga una possibile causa del fallimento.

LA COMMISSIONE

PROF. MONGA MATTIA - PRESIDENTE

DOTT. CASELLA GIULIO FRANCESCO - COMPONENTE

SIG.RA ANGELILLO FILOMENA - COMPONENTE

DOTT.SSA DI TOMMASO HENNA MARIA STELLA - SEGRETARIO