Reti di Calcolatori & Cybersecurity

PHISHING W/DNS SPOOFING

GIOVANNI D'AMBROSIO

Start

10:24 PM

PHISHING

OBIETTIVO: OTTENERE INFORMAZIONI PERSONALI DELL'UTENTE

Start

10:24 PM

ARP INTRODUCTION

A COSA SERVE ARP?

192.168.162.2
CC:CC:CC:CC:CC:CC

RISOLVERE INDIRIZZI IP IN INDIRIZZI MAC

Start

10:24 PM

DNS INTRODUCTION

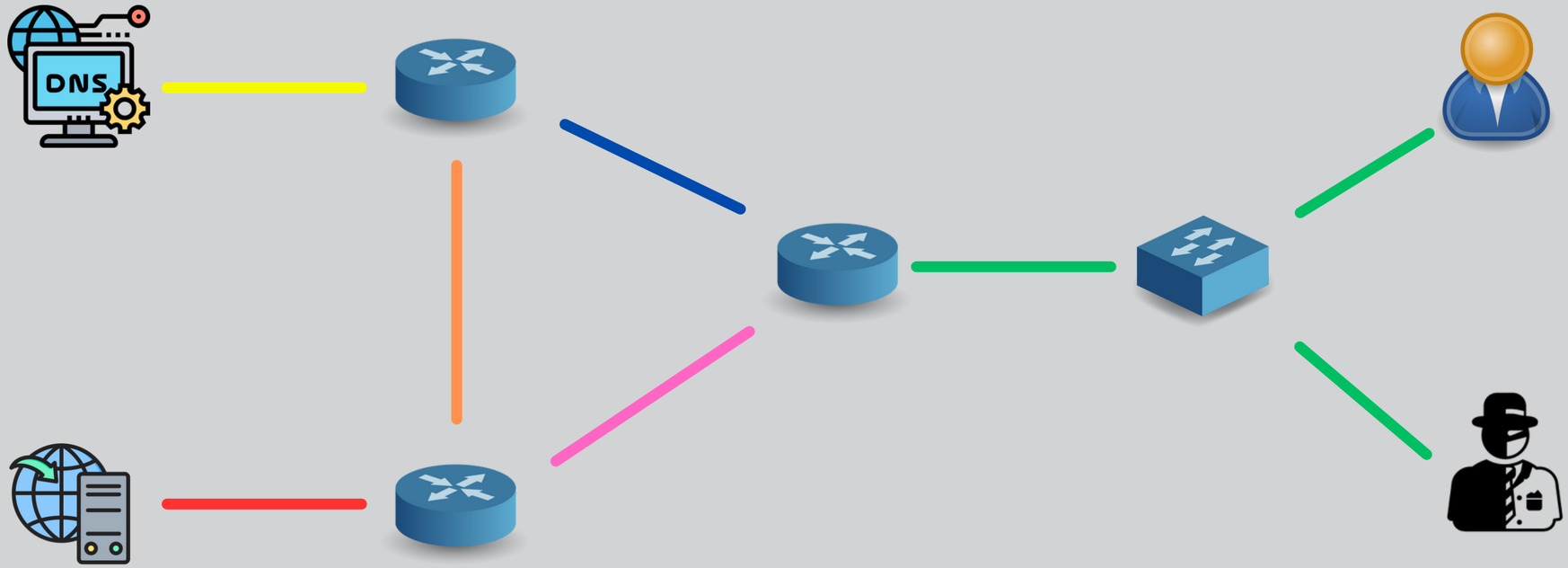
A COSA SERVE DNS?

RISOLVERE DOMINI IN INDIRIZZI IP (E ALTRO)

DNS SPOOFING

OBIETTIVO: INTERCETTARE E MODIFICARE LE RICHIESTE DNS

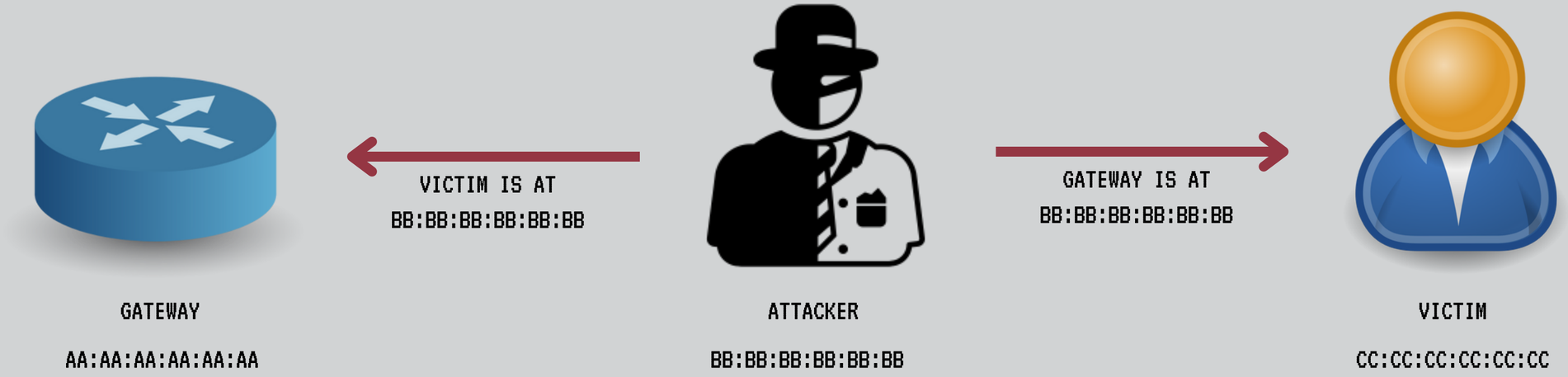
NETWORK



Start

10:24 PM

STEP 1: MITM WITH ARP POISONING



SFRUTTANDO ARP, CI SI METTE AL CENTRO

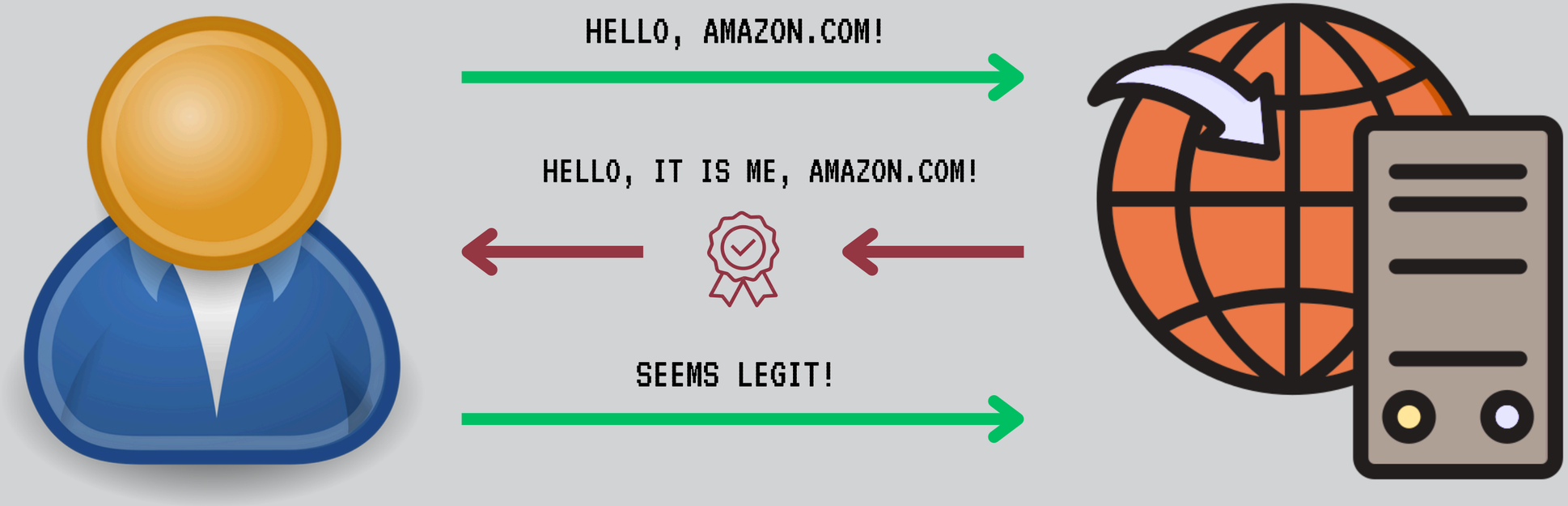
STEP 2: VICTIM QUERY

Start

10:24 PM

STEP 3: DNS RESPONSE

STEP 4: POISONED REQUEST



WEAKNESS: USER BEHAVIOUR

L'IGNORANZA DEL SIGNIFICATO DI INVALIDITÀ DEI CERTIFICATI PUÒ PORTARE A PROBLEMI...

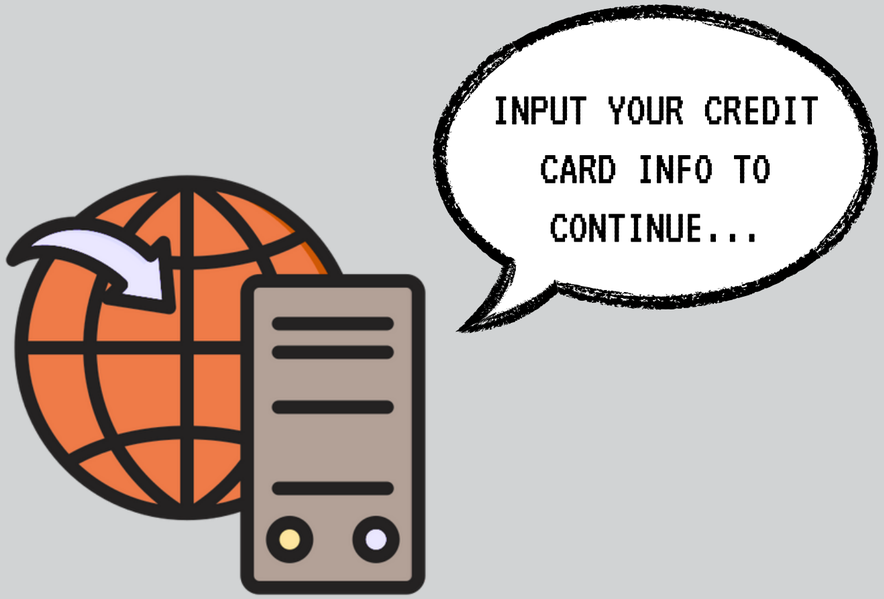
VULNERABILITIES: ARP AUTHENTICITY

LA MANCANZA DI MECCANISMI
DI VERIFICA DI AUTENTICITÀ
DEI MESSAGGI ARP LASCIA VIA
LIBERA ALL'ATTACANTE...

VULNERABILITIES: DNS INTEGRITY

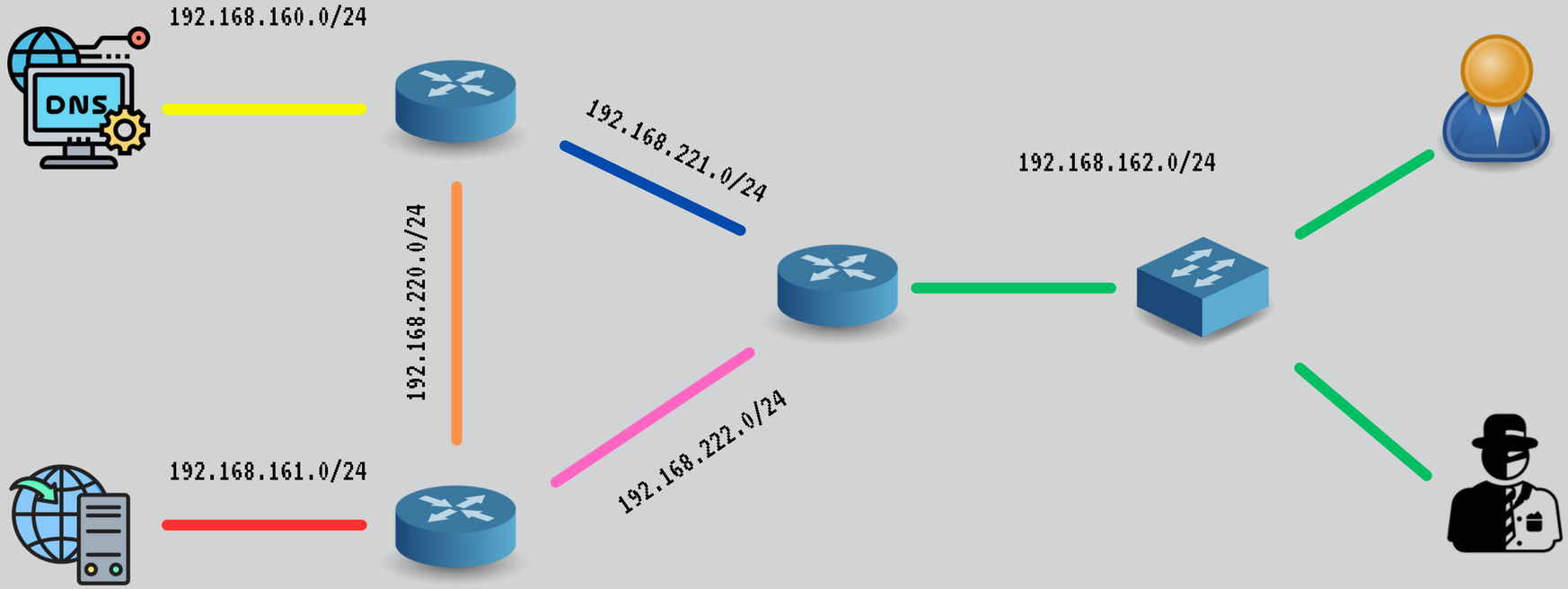
LE RISPOSTE INVIATE IN CHIARO E LA MANCANZA DI MECCANISMI DI VERIFICA DI AUTENTICITÀ E DI INTEGRITÀ DEI MESSAGGI NON AIUTANO...

THREAT: SENSITIVE DATA EXPOSURE



IL REINDIRIZZAMENTO CHE TENTA UN ATTACCO DI PHISHING METTE A RISCHIO LA PRIVATEZZA DEI DATI SENSIBILI DELLA VITTIMA

ATTACK SIMULATION - CONFIG



Start

10:24 PM

DNS SERVER CONFIG

MACCHINA VIRTUALE

DISCO: 2GB

RAM: 512MB

BIND 9.18.27

DNS SERVER CONFIG (/etc/bind/named.conf)

```
acl "trusted" {
    192.168.160.0/24;
    192.168.220.0/24;
    192.168.161.0/24;
    192.168.221.0/24;
    192.168.222.0/24;
    192.168.162.0/24;
};

options {
    directory "/var/bind";

    recursion yes;
    allow-recursion {
        trusted;
    };
    listen-on { 192.168.160.5; };
    allow-transfer { none; };
};

zone "amazon.com" {
    type primary;
    file "/etc/bind/zones/db.amazon.com";
    allow-transfer { none; };
};

zone "161.168.192.in-addr.arpa" {
    type primary;
    file "/etc/bind/zones/db.192.168.161";
    allow-transfer { none; };
};
```

DEFINIAMO LE RETI AFFIDABILI, I PARAMETRI DEL SERVER E LE ZONE DA UTILIZZARE

DNS ZONES CONFIG (/etc/bind/zones/db.amazon.com)

```
$TTL    604800
@   IN  SOA dns.amazon.com. admin.amazon.com. (
              3             ; Serial
              604800        ; Refresh
              86400         ; Retry
              2419200       ; Expire
              604800 )      ; Negative Cache TTL
;
; name servers - NS records
    IN  NS  dns.amazon.com.

; name servers - A records
dns.amazon.com. IN  A   192.168.160.5

; 192.168.161.0/24 - A records
amazon.com. IN  A   192.168.161.5
```

DEFINIAMO I PARAMETRI DI ZONA E I RECORD PER LE RISOLUZIONI

DNS ZONES CONFIG (/etc/bind/zones/db.192.168.161)

```
$TTL    604800
@   IN  SOA dns.amazon.com. admin.amazon.com. (
              4               ; Serial
              604800          ; Refresh
              86400           ; Retry
              2419200         ; Expire
              604800 )        ; Negative Cache TTL
;
; name servers - NS records
    IN  NS  dns.amazon.com.

; PTR Records

5   IN  PTR amazon.com.
```

DEFINIAMO I PARAMETRI DI ZONA E I RECORD PER LE RISOLUZIONI INVERSE

WEB SERVER CONFIG

MACCHINA VIRTUALE

DISCO: 2GB

RAM: 512MB

APACHE 2.4.59

WEB SERVER CONFIG

AI FINI DI RICREARE UNA SITUAZIONE REALE...

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key
-out /etc/ssl/certs/apache-selfsigned.crt
```

AMAZON.COM

WEB SERVER CONFIG

```
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:Campania
Locality Name (eg, city) []:Aversa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Amazon
Organizational Unit Name (eg, section) []:Amazing
Common Name (e.g. server FQDN or YOUR name) []:amazon.com
Email Address []:service@amazon.com
```

INSERIAMO LE INFORMAZIONI DEL CERTIFICATO

WEB SERVER CONFIG (/etc/apache2/httpd.conf)

```
LoadModule ssl_module modules/mod_ssl.so

<IfModule ssl_module>
    Listen 443
    <VirtualHost *:443>
        ServerName amazon.com
        DocumentRoot "/var/www/localhost/htdocs"

        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
        SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

        <Directory "/var/www/localhost/htdocs">
            AllowOverride None
            Require all granted
        </Directory>
    </VirtualHost>
</IfModule>

<VirtualHost *:80>
    ServerName amazon.com
    Redirect / https://amazon.com/
</VirtualHost>
```

CONFIGURIAMO APACHE PER UTILIZZARE IL CERTIFICATO E PER REINDIRIZZARE A CONNESSIONE SICURA

VICTIM CONFIG

KALI

MACCHINA VIRTUALE

DISCO: 20GB

RAM: 2GB

VICTIM

Start

10:24 PM

ATTACKER CONFIG & ASSUMPTIONS

KALI

MACCHINA VIRTUALE

DISCO: 20GB

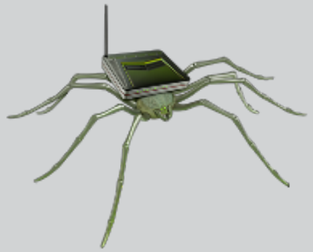
RAM: 2GB

ATTACKER (IN VICTIM'S NETWORK)

Start

10:24 PM

ATTACKING TOOLS CONFIG



ETTERCAP

(ARP POISONING - DNS SPOOFING)

SPOOF CONFIG

```
amazon.com A 192.168.162.3 3600
```

/etc/ettercap/etter.dns

Start

10:24 PM

WEB SERVER CONFIG

CREAZIONE DI UN CERTIFICATO FALSO

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key
-out /etc/ssl/certs/apache-selfsigned.crt
```

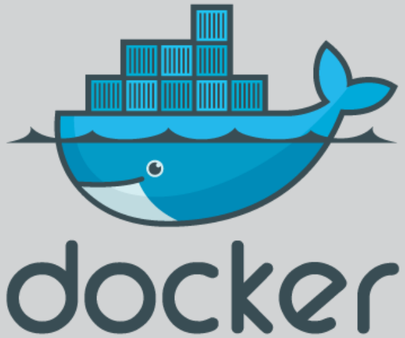
AMAZON.COM

WEB SERVER CONFIG

```
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:Campania
Locality Name (eg, city) []:Aversa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Amazon
Organizational Unit Name (eg, section) []:Amazon Inc
Common Name (e.g. server FQDN or YOUR name) []:amazon.com
Email Address []:amazon@amazon.com
```

INFORMAZIONI DEL CERTIFICATO

ROUTERS CONFIG



FRROUTING-FRR TEMPLATE

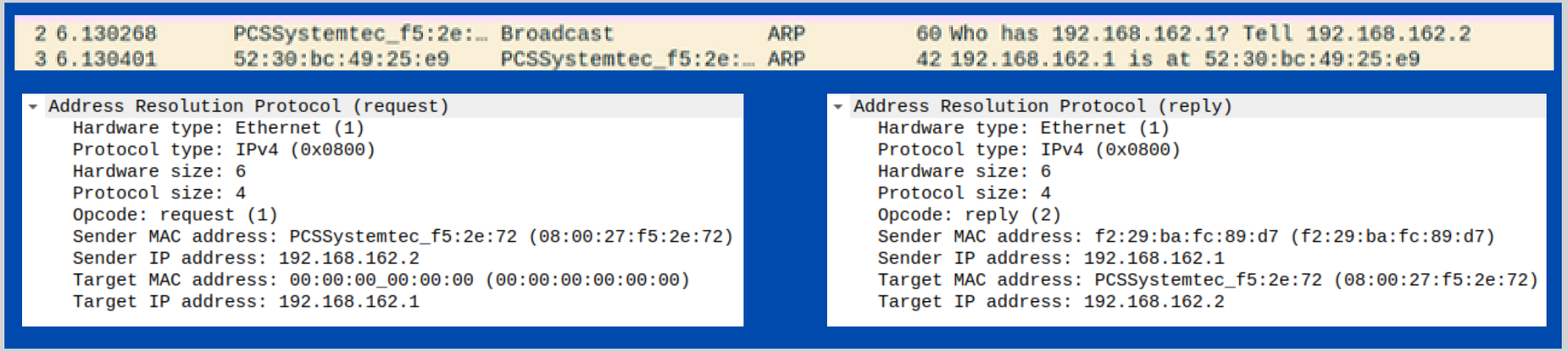
ROUTERS

ROUTERS CONFIG

```
# Static config for eth2
auto eth2
iface eth2 inet static
                address 192.168.222.20
                netmask 255.255.255.0
                gateway 192.168.222.10


# Static config for eth1
auto eth1
iface eth1 inet static
                address 192.168.221.20
                netmask 255.255.255.0
                gateway 192.168.221.10



# Static config for eth0
auto eth0
iface eth0 inet static
                address 192.168.162.1
                netmask 255.255.255.0


up ip route add 192.168.161.0/24 via 192.168.222.10 dev eth2
up ip route add 192.168.220.0/24 via 192.168.222.10 dev eth2
up ip route add 192.168.160.0/24 via 192.168.221.10 dev eth1
```

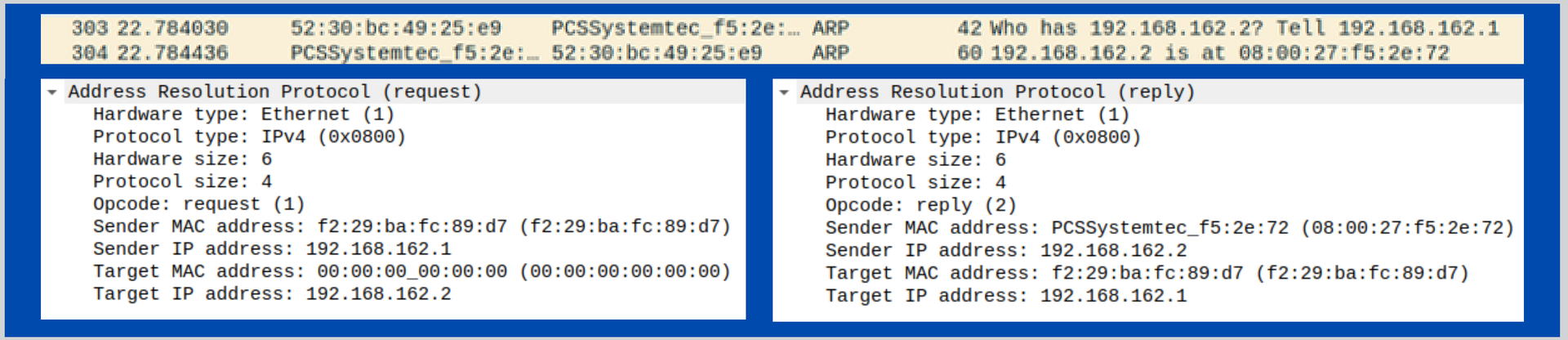
CONFIGURAZIONE STATICA DELLE INTERFACCE E DELLA TABELLA DI ROUTING

ARP POISONING EFFECTS



RICHIESTA VITTIMA PRIMA DELL'AVVELENAMENTO

ARP POISONING EFFECTS



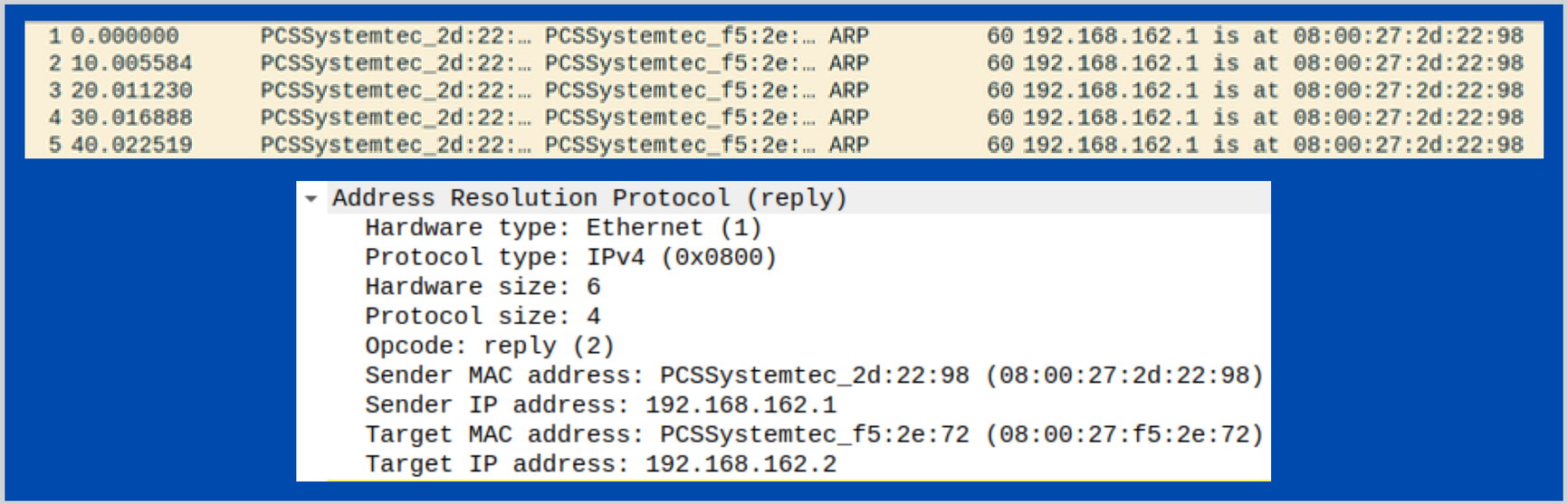
RICHIESTA GATEWAY PRIMA DELL'AVVELENAMENTO

ARP POISONING EFFECTS

1	0.000000	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
2	0.000067	PCSSystemtec_2d:22:…	PCSSystemtec_f5:2e:…	ARP	60 192.168.162.1 is at 08:00:27:2d:22:98 (duplicate use of 192.168.162.2 detected!)
3	10.009293	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
4	10.009365	PCSSystemtec_2d:22:…	PCSSystemtec_f5:2e:…	ARP	60 192.168.162.1 is at 08:00:27:2d:22:98 (duplicate use of 192.168.162.2 detected!)
5	20.015127	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
6	20.015169	PCSSystemtec_2d:22:…	PCSSystemtec_f5:2e:…	ARP	60 192.168.162.1 is at 08:00:27:2d:22:98 (duplicate use of 192.168.162.2 detected!)
7	30.021260	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
8	30.021390	PCSSystemtec_2d:22:…	PCSSystemtec_f5:2e:…	ARP	60 192.168.162.1 is at 08:00:27:2d:22:98 (duplicate use of 192.168.162.2 detected!)
9	40.027072	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
10	40.027120	PCSSystemtec_2d:22:…	PCSSystemtec_f5:2e:…	ARP	60 192.168.162.1 is at 08:00:27:2d:22:98 (duplicate use of 192.168.162.2 detected!)

PACCHETTI INVIATI DALL'ATTACCANTE PER AVVIARE L'AVVELENAMENTO ARP

ARP POISONING EFFECTS



PACCHETTI RICEVUTI DALLA VITTIMA

ARP POISONING EFFECTS

2	4.165445	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
3	14.170996	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
4	24.176517	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
5	34.181817	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98
6	44.187409	PCSSystemtec_2d:22:…	52:30:bc:49:25:e9	ARP	60 192.168.162.2 is at 08:00:27:2d:22:98

```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PCSSystemtec_2d:22:98 (08:00:27:2d:22:98)
    Sender IP address: 192.168.162.2
    Target MAC address: f2:29:ba:fc:89:d7 (f2:29:ba:fc:89:d7)
    Target IP address: 192.168.162.1
```

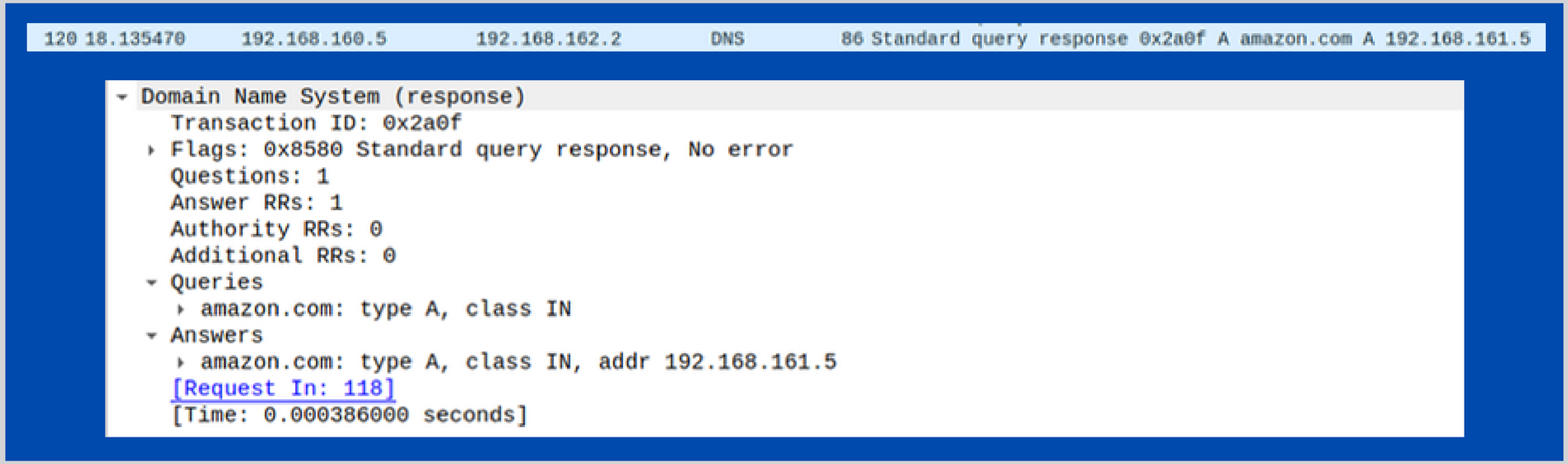
PACCHETTI RICEVUTI DAL GATEWAY

DNS SPOOFING EFFECTS

```
118 18.135084     192.168.162.2        192.168.160.5        DNS          70 Standard query 0x2a0f A amazon.com

▾ Domain Name System (query)
    Transaction ID: 0x2a0f
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ amazon.com: type A, class IN
    [Response In: 120]
```

QUERY DNS DELLA VITTIMA

DNS SPOOFING EFFECTS



RISPOSTA CORRETTA DEL SERVER DNS

DNS SPOOFING EFFECTS

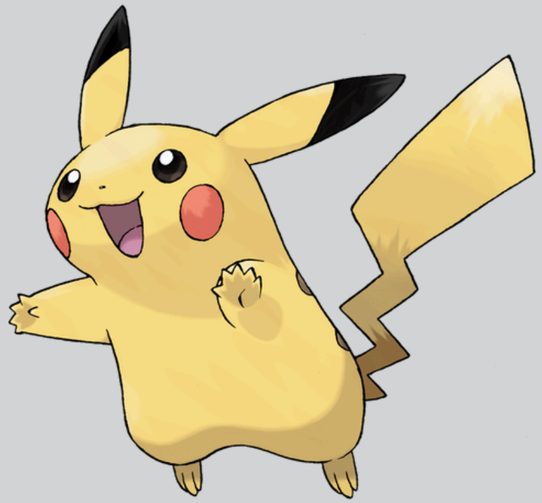
```
12 20.081286    192.168.162.2    192.168.160.5    DNS    70 Standard query 0xa661 A amazon.com
13 20.089514    192.168.160.5    192.168.162.2    DNS    86 Standard query response 0xa661 A amazon.com A 192.168.162.3
```

```
▾ Domain Name System (response)
    Transaction ID: 0xd0be
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▾ amazon.com: type A, class IN, addr 192.168.162.3
        Name: amazon.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 4
        Address: 192.168.162.3
```

RISPOSTA MODIFICATA DALL'ATTACCANTE (VISTA LATO VITTIMA)

COUNTERMEASURES (ARP POISONING)

1. TABELLE ARP STATICHE



CONVENIENZA: ★★☆☆☆

COSTO: ★☆☆☆☆

L'UTILIZZO DI TABELLE STATICHE RENDE VANO QUALSIASI MESSAGGIO INVIATO DALL'ATTACCANTE

COUNTERMEASURES (ARP POISONING)

3. VPN SU RETI PUBBLICHE

CONVENIENZA: ★★★☆☆

COSTO: ★★★☆☆

L'UTILIZZO DI UNA VPN GARANTISCE COMUNICAZIONI CIFRATE: L'ATTACCANTE NON HA IDEA DI COSA CI SIA NEI PACCHETTI

COUNTERMEASURES (ARP POISONING)

2. DYNAMIC ARP INSPECTION

CONVENIENZA: ★★★★☆

COSTO: ★★★☆☆

LA FUNZIONALITÀ DAI È IN GRADO DI RICONOSCERE INFORMAZIONI INCONGRUENTI INVIATE DA UTENTI NON FIDATI

COUNTERMEASURES (DNS SPOOFING)

1. DNS OVER TLS/HTTPS

CONVENIENZA: ★★★★☆

COSTO: ★★★★☆

DOT/DOH GARANTISCE
L'INCAPSULAMENTO DELLE RICHIESTE
DNS IN UN AMBIENTE CIFRATO,
RENDENDO SICURA LA COMUNICAZIONE

COUNTERMEASURES (DNS SPOOFING)

2. EDUCAZIONE INFORMATICA

CONVENIENZA: ★★★★☆

COSTO: ★★★☆☆

EDUCARE GLI UTENTI CHE NAVIGANO SULL'IMPORTANZA DEI CERTIFICATI RISOLVEREBBE PARTE DEL PROBLEMA

REFERENCES

GITHUB REPOSITORY: HTTPS://GITHUB.COM/GIOVANNI1717/PHISHING-ATTACK-W-DNS-SPOOFING
DNS CONFIG: HTTPS://WWW.DIGITALOCEAN.COM/COMMUNITY/TUTORIALS/HOW-TO-CONFIGURE-BIND-AS-A-PRIVATE-NETWORK-DNS-SERVER-ON-UBUNTU-22-04
CERTIFICATE CONFIG: HTTPS://WWW.DIGITALOCEAN.COM/COMMUNITY/TUTORIALS/HOW-TO-CREATE-A-SELF-SIGNED-SSL-CERTIFICATE-FOR-APACHE-IN-UBUNTU-22-04
ROUTER CONFIG: HTTP://WPAGE.UNINA.IT/RCANONIC/DIDATTICA/GNS3-LABS/LAB2/
OTHER CONFIG: HTTPS://CHATGPT.COM/