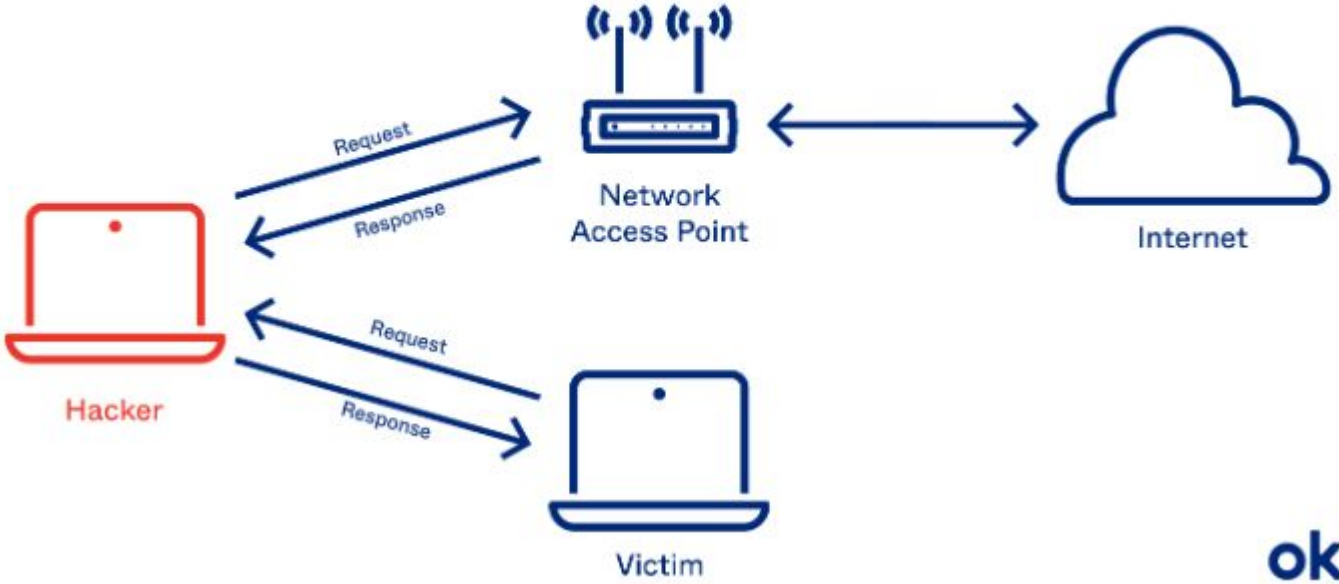
Cloud Security

By: Jamison Stalter, Corban Sy, Erik Ziegler, Alac Springer, Epifanio Solano

What is ARP Spoofing?

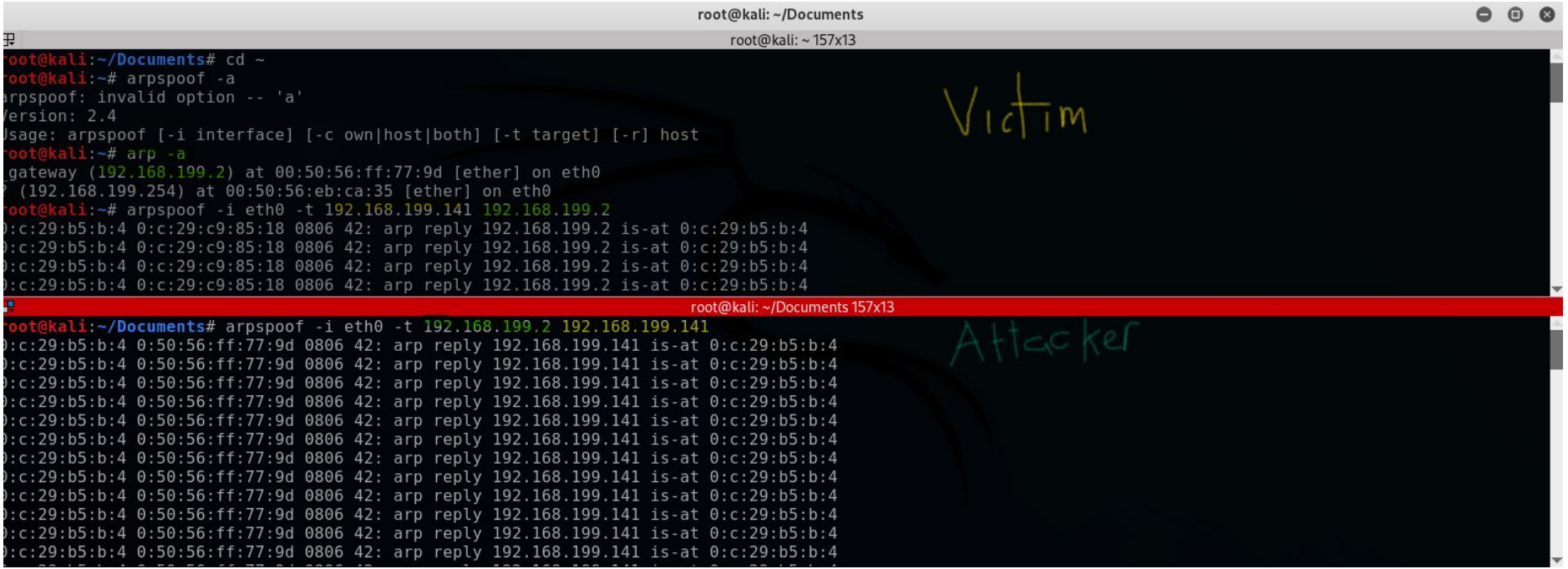
- ARP spoofing is a type of Man-in-the-Middle (MitM) attack.
- ARP (Address Resolution Protocol) spoofing involves sending falsified ARP messages over a local area network (LAN).
- This malicious activity aims to associate the attacker's MAC (Media Access Control) address with the IP address of another host, such as the default gateway.

ARP Poisoning/Spoofing



okta

ARP Spoofing In Action



What is happening?

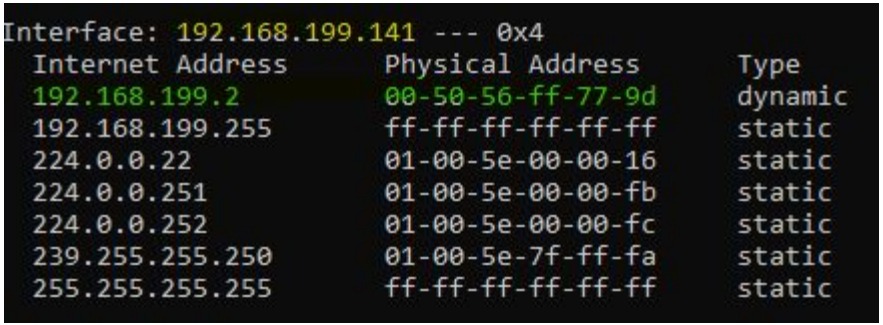
First the victim machine at IP Address 192.168.199.141 is being told that the router is at the attackers machine IP Address 192.168.199.2.

Second, the router is now being told that the attacking machine is now the victim.

Notice before, the attack is started the

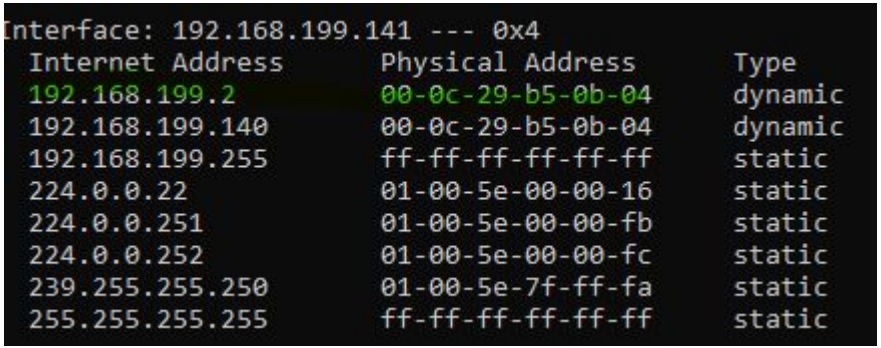
MAC Address of the “router” with

IP Address 192.168.199.2



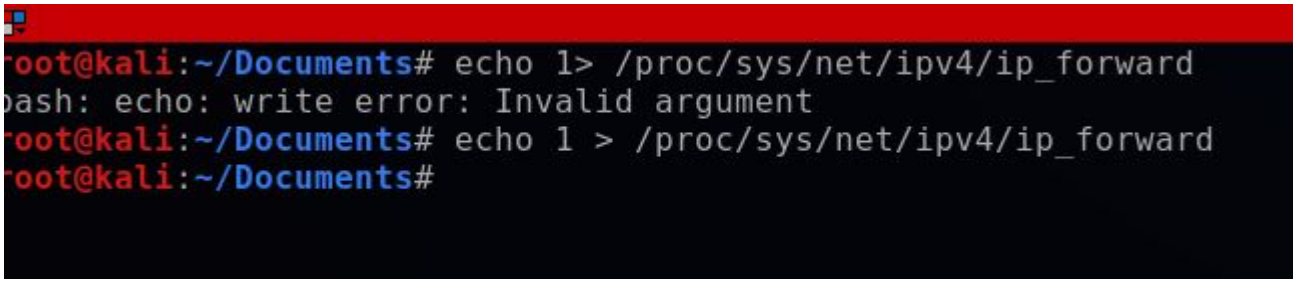
What is happening?

Now the MAC Address that was previously there for the router has now changed. It is now the MAC Address of the attacking machine. Therefore, the attacking machine will now be the one that receives request from the victim.



Security Feature?

Because the attacking machine is not a router, the packets will eventually stop there and nothing will happen, this is a security feature implemented by the OS. In order to bypass it we need do the following to enable port forwarding:



Aggressive Server Scan

-A (IP Address)

OS Detection
Version Detection
Script Scanning
Provides Traceroute

```
ubuntu@ip-172-31-1-226:~$ sudo nmap -A 172.31.1.226
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 20:35 UTC
Nmap scan report for ip-172-31-1-226.us-east-2.compute.internal (172.31.1.226)
Host is up (0.000017s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
```

Scripting Engine

--script vuln (IP Address)

Scans for vulnerabilities


```
ubuntu@ip-172-31-1-226:~$ sudo nmap --script vuln 172.31.1.226
```

```
ubuntu@ip-172-31-1-226:~$ sudo nmap --script vuln 172.31.1.226
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 20:44 UTC
Nmap scan report for ip-172-31-1-226.us-east-2.compute.internal (172.31.1.226)
Host is up (0.0000040s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 10.49 seconds
```

Scan failed due to AWS security features.

What a Vulnerable Scan would look like

```
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
      of insufficient strength, especially those using one of a few commonly
      shared groups, may be susceptible to passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
    References:
      https://weakdh.org
|_ssl-poodle:
  VULNERABLE:   '
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  CVE:CVE-2014-3566  BID:70574
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
    Check results:
```

Comparing AWS and GCP Security

Amazon AWS

- Encryption at rest and in transit
- Key Management Service
- Identity and Access Management
- CloudTrail (logging), CloudWatch (monitoring), and GuardDuty (threat detection) for continuous monitoring and logging of activity
- Virtual Private Cloud (VPC), security groups, Network Access Control Lists (NACLs), and Web Application Firewall (WAF)
- Macie (for sensitive data discovery) and Detective (security investigation and analysis)

Google Cloud

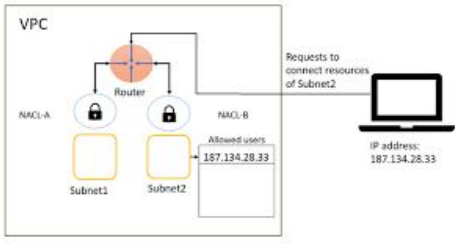
- Encryption at rest and in transit
- Cloud KMS
  - GCP allows client-side encryption and key import/export.
- Google Cloud Identity and Access Management can leverage Google's global single sign-on (SSO)
- Cloud Audit Logs, Cloud Monitoring, and Security Command Center
- Virtual Private Cloud (VPC), firewall rules, Cloud Armor (WAF), and Cloud DNS
- Data Loss Prevention (DLP) for data classification, Security Health Analytics for scanning, and Forseti (open-source) for configuration monitoring

Cloud-Specific Security Enhancements for ARP Spoofing

AWS

Virtual Private Cloud (VPC) - logically isolated section of the cloud. Isolation helps against ARP spoofing by limiting broadcast domains

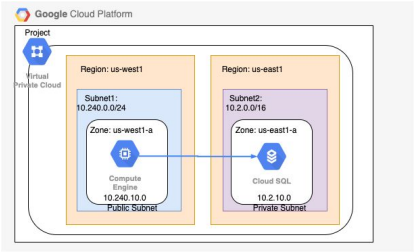
NACL (Network access control list) - viral firewalls for EC2 instances and subnets. Provides control over inbound and outbound traffic which reduces ARP risks from external sources

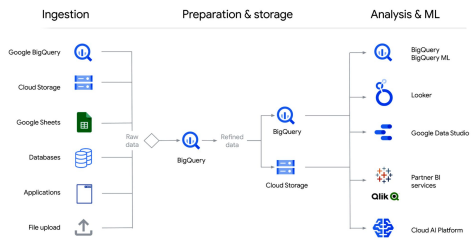


GCP

Virtual Private Cloud (VPC) - Segments network traffic to prevent the spread of ARP broadcasts across multiple instances

Google BigQuery/Cloud Storage - Allows instance communication without exposing traffic to public internet reducing attack surface for ARP spoofing by limiting network exposure



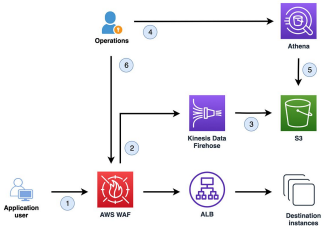


Cloud-Specific Security Enhancements for Vulnerability Scanning

AWS

AWS WAF - Detects common exploitation attempts that could arise from vulnerability scanning

AWS Shield - Mainly focused on DDoS protection but does include measures to identify and mitigate unexpected network scans



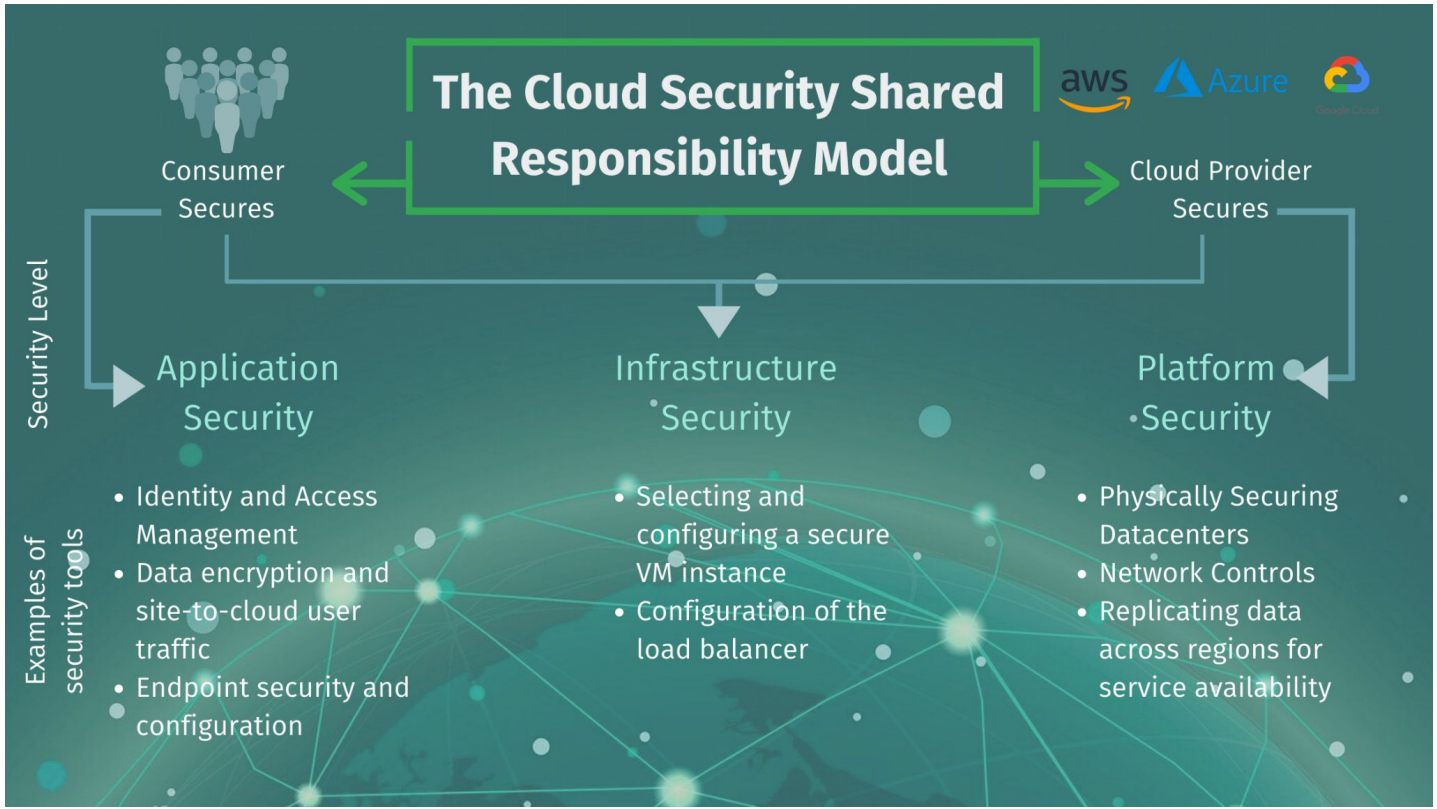
GCP

Identity and Access Management (IAM) - Ensures only authenticated and authorized users can access resources preventing unauthorized scans

Context-Aware Access - Provides granular access control through identity, location, device security status, and IP address

Google Cloud IAM

Shared Responsibility Model



https://www.amoebanetworks.com/managed-IT-services-nyc/cloud-security-a-shared-responsibility-model-1600187704178.html

Findings compared to industry

- Security is a partnership between the provider and its customers.
- Both AWS and GCP define their security models that they are responsible for the security *of* the cloud and the customers are responsible for the security *within* the could.
- Our findings show this to be true. Even though the devices were vulnerable to attacks, these attacks were within the cloud. Any vulnerabilities of our applications are solely our responsibility.
- It is critical for application developers and customers to make extensive use of their cloud providers extensive toolset but to also program with security in mind first and not later.

THANK YOU!