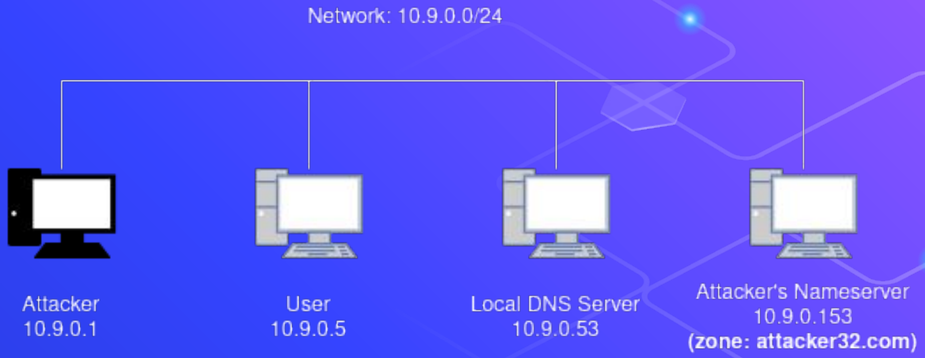
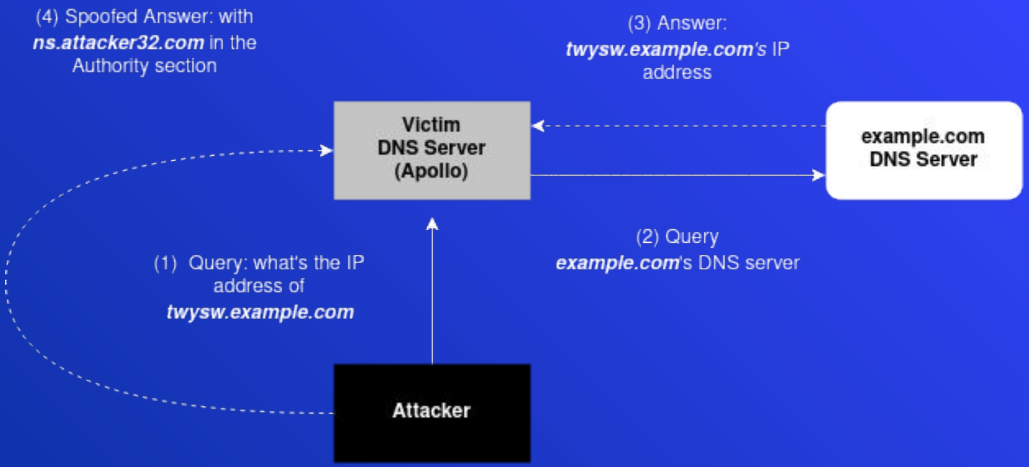
Kaminsky & DNS Rebinding Attacks

Network Security
2021/22

Kaminsky Attack

Setup


Network: 10.9.0.0/24
Attacker
10.9.0.1
User
10.9.0.5
Local DNS Server
10.9.0.53
Attacker's Nameserver
10.9.0.153
(zone: attacker32.com)


(4) Spoofed Answer: with *ns.attacker32.com* in the Authority section
(3) Answer: *twysw.example.com's* IP address
Victim DNS Server (Apollo)
example.com DNS Server
(1) Query: what's the IP address of *twysw.example.com*
(2) Query *example.com*'s DNS server
Attacker

Goal

Steps

Task 1

Query the DNS server for a random name in the target domain name.

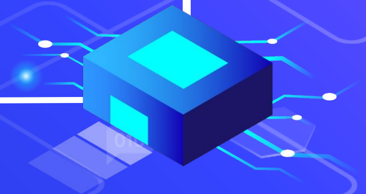
Task 2

Flood the victim server with spoofed DNS replies while it waits for a response from *example.com* DNS server.

Task 3

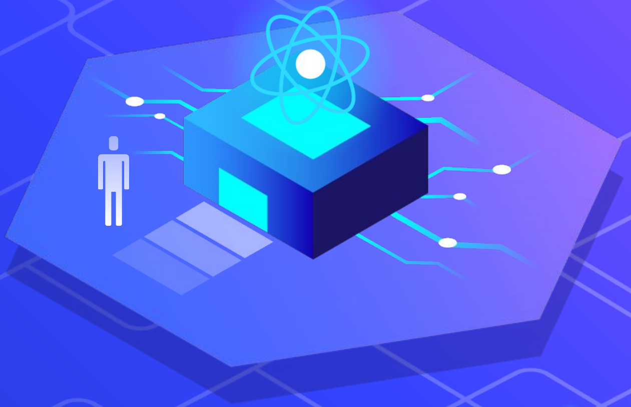
Respond to the victim before the legitimate name server.

Result - All future queries for this domain will be made to the attacker’s name server.

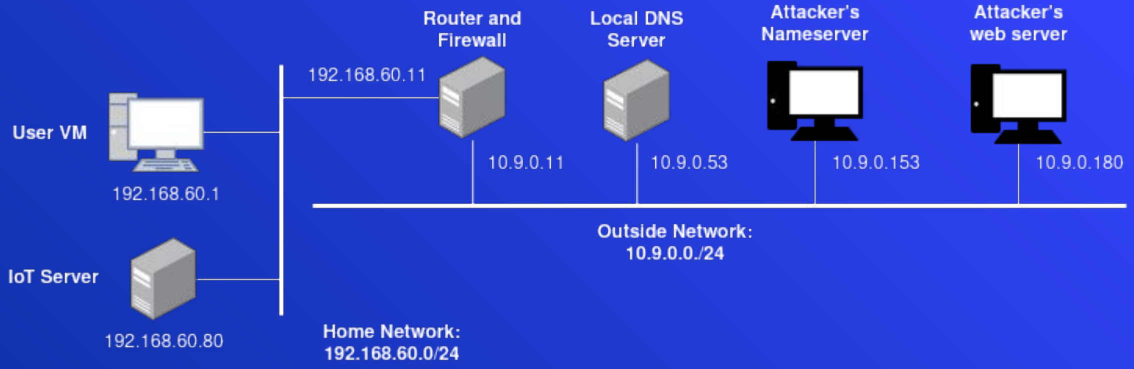


Live Demo

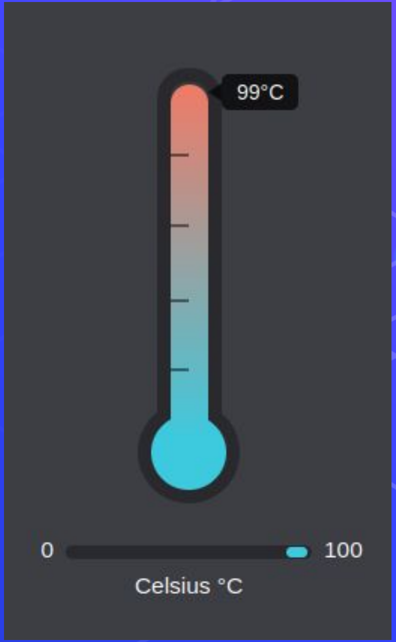
Rebinding Attack



Setup


Router and Firewall
Local DNS Server
Attacker's Nameserver
Attacker's web server
192.168.60.11
User VM
192.168.60.1
10.9.0.11
10.9.0.53
10.9.0.153
10.9.0.180
Outside Network: 10.9.0.0./24
IoT Server
192.168.60.80
Home Network: 192.168.60.0/24

Goal


99°C
0
100
Celsius °C

Steps

Task 1

Defeat the Same-Origin Policy Protection, so we can set the temperature from the attacker's page.

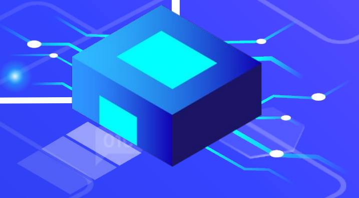
Task 2

Conduct the DNS rebinding by mapping *www.attacker32.com* to the IP address of the attacker’s web server. Then, remap it back to the IoT server.

Task 3

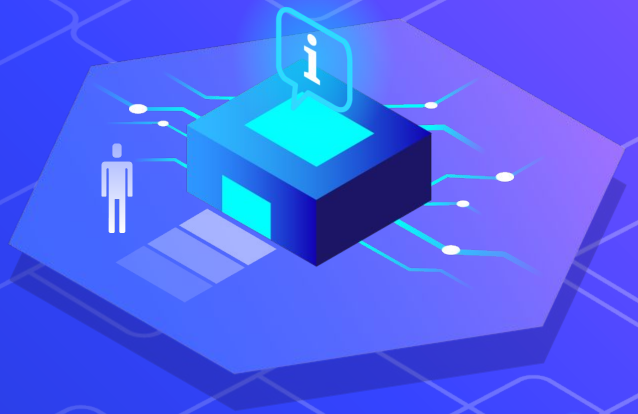
Launch an automatic attack.

Result - Upon sending the request to *www.attacker32.com*, we will actually send the request to the IoT server instead of the attacker's web server.

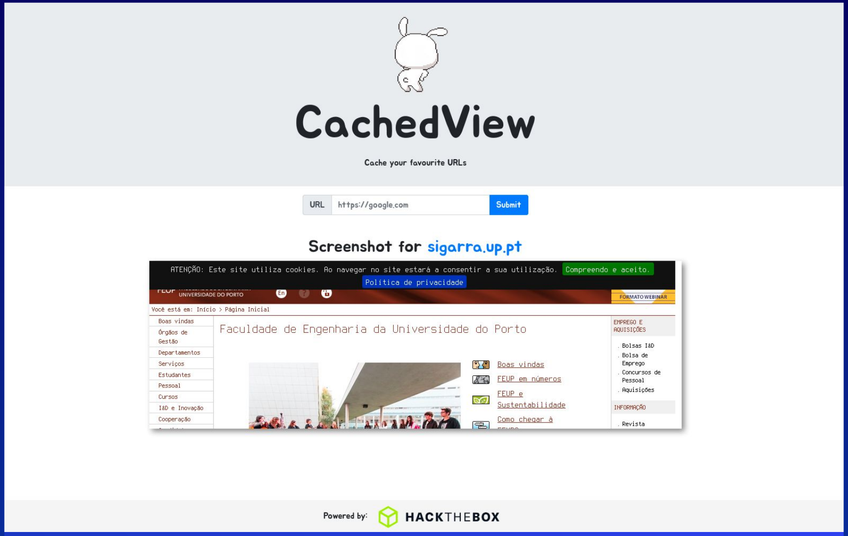


Live Demo

HTB Challenge
Cached View



Setup



CachedView

Cache your favourite URLs

URL: https://google.com

Screenshot for sigarra.up.pt

ATENÇÃO: Este site utiliza cookies. Ao navegar no site estará a consentir a sua utilização. Compreendo e aceito.

Política de privacidade

Você está em: Início > Página Inicial

Faculdade de Engenharia da Universidade do Porto

Powered by: HACKTHEBOX

Live Demo

Thank you

- Ana Barros - up201806593
- Davide Castro - up201806512
- Diogo Rosário - up201806582
- Rui Pinto - up201806441