Relatório de Estágio

Rafael Figueiredo Camilo

Curso Técnico Superior Profissional em Cibersegurança

dez | 2022

GUARDA
POLI
TÉCNICO

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Relatório de Estágio

Rafael Figueiredo Camilo

IPG

CTesp em Cibersegurança

UTC de Informática
Escola Superior de Tecnologia e Gestão

Dezembro, 2022

CTeSP em Cibersegurança

Candidato: Rafael Camilo, Nº 1705293, rafaelcamilo0014@gmail.com

Orientação Científica: Paulo Alexandre de Andrade Vieira, pavieira@ipg.pt

Empresa: Qiba/Barix.

Supervisor na Empresa: Mário Almeida, [redacted]

UTC de Informática
Escola Superior de Tecnologia e Gestão
Endereço: Av. Dr. Francisco Sá Carneiro 50, 6300-559 Guarda

Dezembro, 2022

Elementos Identificativos

Aluno

Nome: Rafael Camilo
Número de aluno: 1705293
Curso: CTeSP Cibersegurança
Ano Letivo: 2021/2022
E-mail: rafaelcamilo0014@gmail.com

Estabelecimento de Ensino

Escola Superior de Tecnologia e Gestão - Instituto Politécnico da Guarda
Morada: Av. Dr. Francisco Sá Carneiro, 50 – 6300-559 Guarda
Telefone: +351 271 220 100
E-mail: ipg@ipg.pt

Orientador: Professor Doutor Paulo Alexandre de Andrade Vieira
E-mail: paulovieira@ipg.pt

Local de Estágio

Empresa de acolhimento: Qiba
Morada: Edifício 3, PCI – Parque da Ciência e Inovação, Via do Conhecimento, 1º piso, 3830 – 352, Ílhavo
Telefone: 300 509 114
E-mail: info@qiba.pt
Website: qiba.pt
Supervisor na empresa de acolhimento: Mário Almeida

Período do Estágio: 01 de abril a 19 de agosto
Duração do Estágio: 750 horas

Agradecimentos

Quero agradecer a todos aqueles que direta ou indiretamente tiveram influência positiva no meu percurso para me tornar um profissional durante o Curso CTesp Cibersegurança dos anos letivos 2020/2021 e 2021/2022.

Quero agradecer também à Qiba por me ter disponibilizado este estágio, por me ter instalado com as melhores condições, e por me incluírem como membro da empresa.

Agradeço também à equipa Barix, que estiveram sempre disponíveis para me esclarecer dúvidas.

Resumo

O estágio foi realizado na empresa Qiba. Na Qiba estagiei com o red team e fiz pentests (testes de intrusão) no website de gestão dos dispositivos da Barix e nos seus dispositivos entre 01 de abril de 2022 e 19 de agosto de 2022. Para executar as tarefas do estágio usei conhecimentos das aulas e conhecimento que obtive em aprendizagem autodidata através de bastante pesquisa sobre várias ferramentas e conceitos de hacking.

Índice

Índice de Figuras

Índice de acrónimos

Acrónimos	Descrição
API	Application Programming Interface
CLI	Command-Line Interface
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IOT	Internet Of Things
IP	Internet Protocol
IPG	Instituto Politécnico da Guarda
MDB	Multi Drop Bus
MTU	Maximum Transmission Unit
OS	Operating System
OSVDB	Open Source Vulnerability Database
SSH	Secure Shell
SSL	Secure Sockets Layer
Tcl	Transaction Control Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XSS	Cross Site Scripting

Capítulo 1

Introdução

Pentest é uma forma de encontrar e explorar vulnerabilidades nos sistemas, é uma simulação de ataques de hackers. Estas avaliações são úteis para validar a eficácia dos mecanismos de defesa das aplicações e servidores.

Este tipo de teste pode ser feito manualmente, mas normalmente é apoiado por ferramentas.

1.1 Objetivos

O objetivo geral deste estágio foi colaborar com a empresa Barix em encontrar vulnerabilidades no website de gestão e nos seus dispositivos de áudio sobre ip (retail player device). Para isso foram realizados testes de intrusão. Durante o estágio adquiri conhecimento em contexto de empresa e apliquei conhecimento das aulas.

1.2 Calendarização

O estágio deu início no dia 01 de abril de 2022. Finalizado dia 19 de Agosto de 2022. O Horário foi das 09:00 às 12:00 e 13:00 às 18:00.

1.3 Descrição do Instituto Politécnico da Guarda e do Curso de Cibersegurança

Se o ensino superior universitário, em Portugal, conta já com mais de 700 anos, o mesmo não acontece com o ensino politécnico, que é relativamente recente. A sua criação jurídica remonta aos inícios da década de 70, mais precisamente a meados de 1973, com a Lei nº 5/73, de 25 de julho.

Na Guarda, a primeira instituição de ensino superior foi a *Escola Superior de Educação*, criada em 1979 pelo Decreto-Lei nº 513 – T/79, de 26 de dezembro. A criação do *Instituto Politécnico da Guarda* verifica-se apenas em 1980, através do Decreto-Lei nº 303/80, de 16 de agosto, que cria também os Politécnicos de Leiria, Portalegre e Viana do Castelo.

Com a criação do Instituto Politécnico da Guarda, a Escola Superior de Educação passou, por força do artigo 2º do mesmo Decreto-Lei, a ser uma escola integrada.

O Curso de Cibersegurança ensina a implementar, analisar, gerir redes de comunicação e planear, projetar, desenvolver software e salvaguardar requisitos de segurança de acordo com as necessidades das organizações.

1.4 Organização do Relatório

O capítulo 1 é a introdução a este relatório, onde são relatados os objetivos, a calendarização do estágio, empresa que me acolheu neste estágio, Qiba, um resumo do que é a Qiba e que é descrita. É também feita a caracterização do espaço e ambiente de trabalho.

O capítulo 2 é um resumo de todas as ferramentas e aplicações que foram usadas durante este estágio.

O capítulo 3 define as tarefas que foram realizadas durante todo o estágio.

O capítulo 4 contém a conclusão do estágio e referências

1.5 A Empresa

A Qiba[1] foi fundada por Mário Almeida e Johannes Rietschel em Aveiro no ano 2019 e desde então a empresa tem vindo a crescer não só no mercado, mas também como equipa.

A Qiba é uma empresa portuguesa que nasceu da necessidade de marcas Suíças, como a Qibixx[2], MOH, entre outras, para criarem um canal de distribuição na Europa para os seus produtos e soluções. O foco da empresa é em dispositivos IoT, soluções eletrônicas, sistemas centralizados de pagamento, monitorização de automação e muitos outros campos, como tecnologia MDB (Multi Drop Bus), controladores para máquinas de vending, contadores de eventos, alojamento de dados na web, etc.

A Qiba é um cluster de empresas, eu trabalhei essencialmente com a Barix.

A Barix[3] é uma empresa orientada para a inovação localizada em Zurique e fundada em 2001, que desenvolve, com sucesso, hardware e soluções de áudio sobre IP. É um player a nível mundial em aplicativos de áudio e de rede inteligente.

Para permanecer na vanguarda de uma indústria em constante mudança, a empresa continuamente expande o conhecimento de áudio e desenvolve skills para novas tecnologias emergentes. Os produtos são usados em quase todos os mercados e o seu uso continua a crescer.

[1] https://www.qiba.pt/pt/home-pt/
[2] https://qibixx.com
[3] https://www.barix.com

1.6 Caracterização do espaço e ambiente

A Qiba é uma empresa com excelentes condições e situa-se no Edifício 3, PCI - Parque Ciência e Inovação, Via do Conhecimento 1º Piso. A Qiba é constituída por 4 escritórios, neles estão as empresas Qiba, Brightsuff[4], Barix e um Lounge room. Tudo faz parte da Qiba, tem também um escritório/laboratório em Oiã[5] com um armazém onde testam hardware.

[4] https://www.brightstuff.pt/pt
[5] https://www.jf-oia.pt

Capítulo 2

Ferramentas utilizadas

Durante o meu estágio usei as ferramentas seguintes como auxiliares para o sucesso no meu trabalho como pentester.

2.1 Nitko

Figura 1 Logotipo Nikto

Nikto é um scanner de vulnerabilidades open-source com conexão por CLI, usado para fazer scan de servidores web para procurar documentos perigosos, programas desatualizados e outros problemas. É capaz de fazer tanto análises genéricas como análises específicas de servidor. Também faz a captura e exibição de cookies HTTP.

2.2 Nmap

Figura 2 Logotipo nmap

Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker “Fyodor”. É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores. Nmap é conhecido pela sua rapidez e pelas opções que dispõe.

Nmap é uma ferramenta que nos permite fazer scan de redes, portas, sistemas operativos e vulnerabilidades

2.3 Burp suite

Figura 3 Logotipo Burp Suite.

Burp Suite é um software desenvolvido em Java pela PortSwigger, para a realização de testes de segurança em aplicações web. O Burp Suite é dividido em diversos componentes como Burp Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder e Comparer.

2.4 Dirbuster / Gobuster

Figura 4 Logotipo Dirbuster

Dirbuster ou o Gobuster são duas ferramentas open-source e ambas servem para usar brute force com wordlists de diretorias dentro do website

2.5 Sqlmap

Figura 5 Logotipo SQLmap

sqlmap é uma ferramenta de teste de intrusão open-source que automatiza o processo de detecção e exploração de falhas de injeção de SQL e controle de servidores de base de dados. sqlmap vem com um poderoso mecanismo de detecção, muitos recursos de nicho para o melhor testador de intrusões e uma ampla gama de opções que vão desde impressão digital do base de dados, busca de dados na base de dados, acesso ao sistema de documentos subjacente e execução de comandos no sistema operativo via out- conexões de rede.

2.6 Metasploit

Figura 6 Logotipo Metasploit

O Projeto Metasploit é um projeto de segurança de computadores que fornece informações sobre vulnerabilidades de segurança e ajuda em testes de intrusão e desenvolvimento de assinaturas Intrusion Detection System (IDS) .

2.7 Hping3

Figura 7 Logotipo hping

Hping é uma ferramenta para redes que permite modificar pacotes ICMP/UDP/TCP e permite exibir as respostas de destino como o ping faz com as respostas ICMP. Ele lida com fragmentação e corpo e tamanho de pacotes arbitrários, e pode ser usado para transferir

documentos sob protocolos suportados. Usando o hping3, pode-se testar regras de firewall, executar varredura de porta (spoofed), testar o desempenho da rede usando diferentes protocolos, fazer descoberta de Maximum Transmission Unit (MTU) de caminho, executar ações do tipo traceroute em diferentes protocolos, sistemas operativos remotos de impressão digital, auditar pilhas TCP/IP, etc. hping3 é programável usando a linguagem Tcl[6].

Hping é usado para fazer um ataque Denial of Service (DoS).

[6] https://www.tcl.tk/about/language.html

Capítulo 3

Tarefas realizadas

Na tabela que se segue está descrito de forma sucinta as tarefas realizadas. Na tabela estão indicados: o tipo de teste de intrusão realizado, é explicado em que consiste cada um desses testes, que ferramentas usadas (é indicado o link para a ferramenta), e as vulnerabilidades encontradas.

Tabela : Resumo de tarefas realizadas

tipo de teste de intrusão	explicação em que consiste	ferramenta usada	Vulnerabilidades encontradas
SQL Injection	Injeção de código sql na página log in do website	SQLmap	não foram encontradas vulnerabilidades.
Injeção de scripts	XSS(cross site script) é injeção de código java	não foi usado ferramentas	Não foram encontradas vulnerabilidades.
Brute Force de diretorias e documentos	Este teste consiste em encontrar documentos que possam revelar informação sensível.	Dirbuster GoBuster	Vários documentos expostos que possam ser úteis para o atacante.
Mapa do website	Ao fazermos várias conexões com o website o burp cria um mapa com documentos e respostas do website	BurpSuite	podemos ver como é chamada a admin role.
Login Brute force	Com a ferramenta intruder do Burp Suite podemos usar e modificar wordlist para descobrir usernames e passwords	BurpSuite	Não tem limite de tentativas de login.
ID da Organização	No mapa feito pelo burpsuite temos acesso a um documentos com ID da organização	BurpSuite	Permite aceder à edição da Organização.
Escalação de privilégios	Ao manipular a edição da conta podemos adicionar a admin role a nós próprios	Burpsuite	API facilmente manipulada.
Port Scanning	Scan de portas e softwares	nmap	Portas abertas.
Análise geral	Procura de vulnerabilidades	Nikto	Falta de security headers e

			alguns possíveis documentos com informação sensível.
Bruteforce conexão ssh	Uso de um auxiliar para Brute force log in por ssh	Metasploit	O atacante não leva timeout por várias tentativas de login.
Dos attack	Dos no hub do dispositivo	hping3	o hub do dispositivo vai abaixo.
Alterações do Cartão SD	Alteração da root password do sistema do dispositivo.	uso de um adaptador de cartão SD para USB	Cartão visível e fácil de remover do dispositivo.
Port scan do Retail player	scan das portas abertas do dispositivo e sistemas	nmap	portas abertas.
Scan geral do Retail player	scan geral de vulnerabilidades do hub do dispositivo	Nikto	não foi encontrado vulnerabilidade

3.1 Portal Retail Player (https://manage.barix.com/login)

3.1.1 injeção de código SQL

Sqlmap[7] é uma ferramenta open-source para pentest que consegue detectar se o website é vulnerável a injeção SQL automaticamente ao testar vários comandos de vários tipos de bases de dados.

Neste tipo de ataque o objetivo é injetar código através do website para a base de dados onde podemos manipular a base de dados de várias maneiras como por exemplo aceder a contas sem conhecimento da password ou nome do utilizador.

[7] https://sqlmap.org

Figura 8 teste de injeção de código SQL com SQLmap

Nesta imagem representa uma tentativa de injeção de código SQL com a ferramenta do SQLmap na página log in do site https://manage.barix.com/login, não é possivel injetar código sql porque a API[8] transforma qualquer valor introduzido numa string e mesmo que feche essa string e injete código a seguir o website vai retribuir com um bad request.

[8] https://en.wikipedia.org/wiki/API

3.1.2 XSS (Cross Site Scripting)

XSS[9] é um ataque de desfiguração onde se injeta código malicioso através de barras de pesquisa ou onde se possa escrever no website.

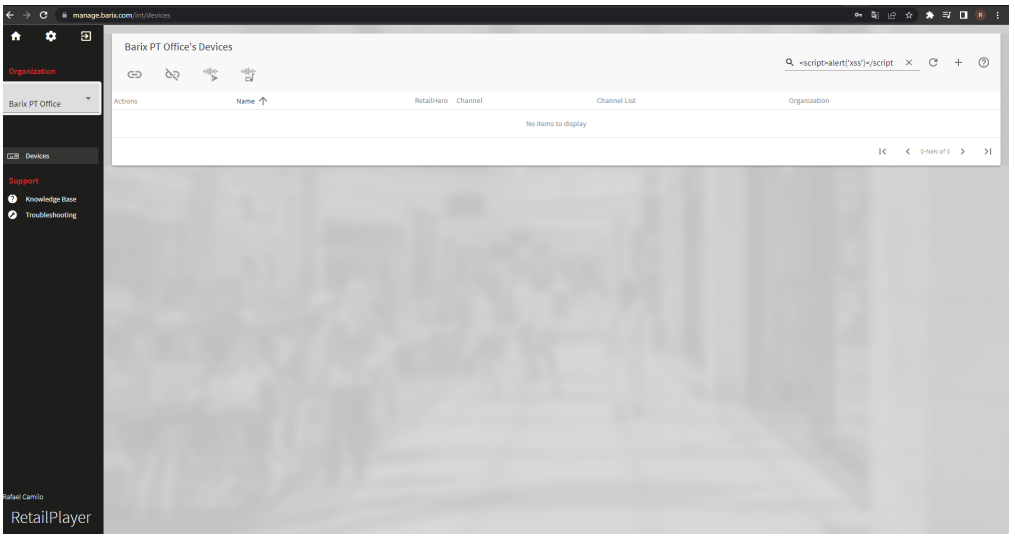

Figura 9 Teste de injeção de código XSS (Cross Site Script)

O site https://manage.barix.com/int/devices não aparenta ser vulnerável a XSS visto que também não tem um retorno do valor introduzido na barra de pesquisa no mesmo body da página.

[9] https://en.wikipedia.org/wiki/Cross-site_scripting

3.1.3 Dirbuster e gobuster

Dirbuster[10] e Gobuster[11] são ferramentas que usam Wordlists para fazer brute force de diretorias e documentos do website onde podemos obter informação sensível do website.

O objetivo deste ataque é apanhar documentos que mostrem informação sensível do site como informação dentro do website.

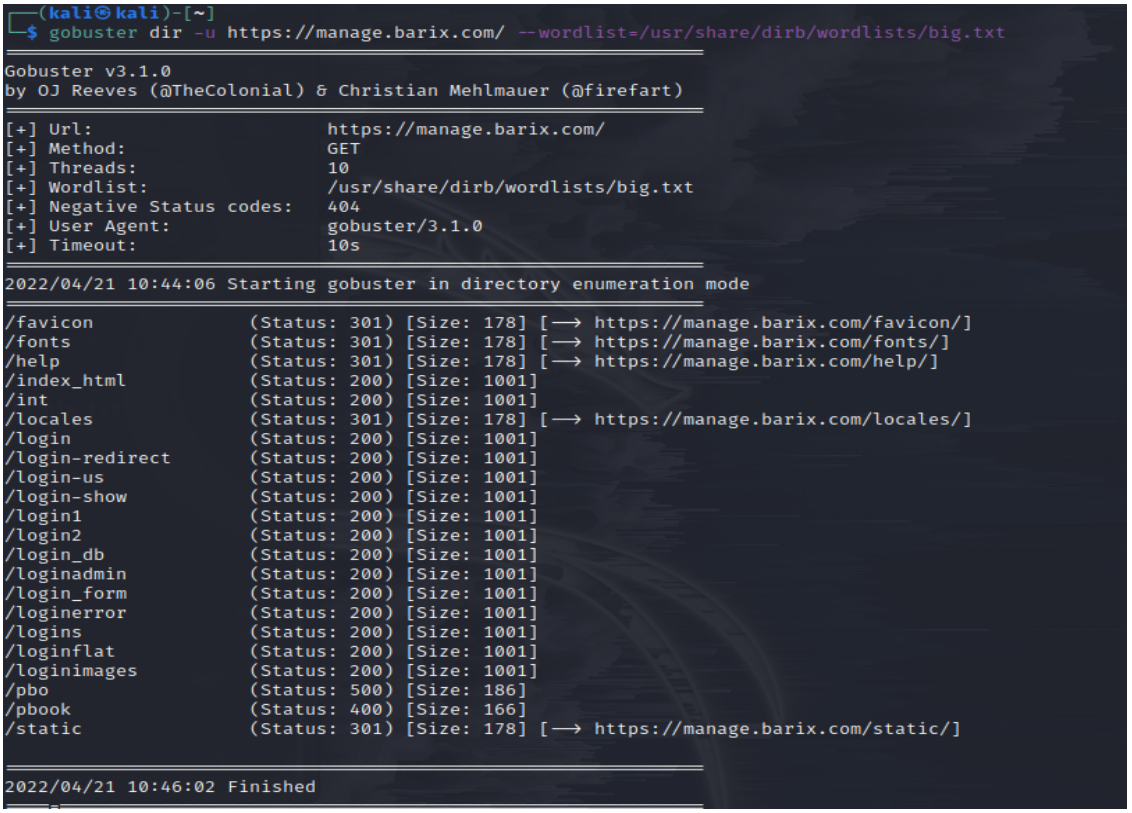

Figura 10 Brute force com uma worldlist de nomes de ficheiros e pastas comuns dentro de um site com gobuster

[10] https://www.kali.org/tools/dirbuster/
[11] https://www.kali.org/tools/gobuster/

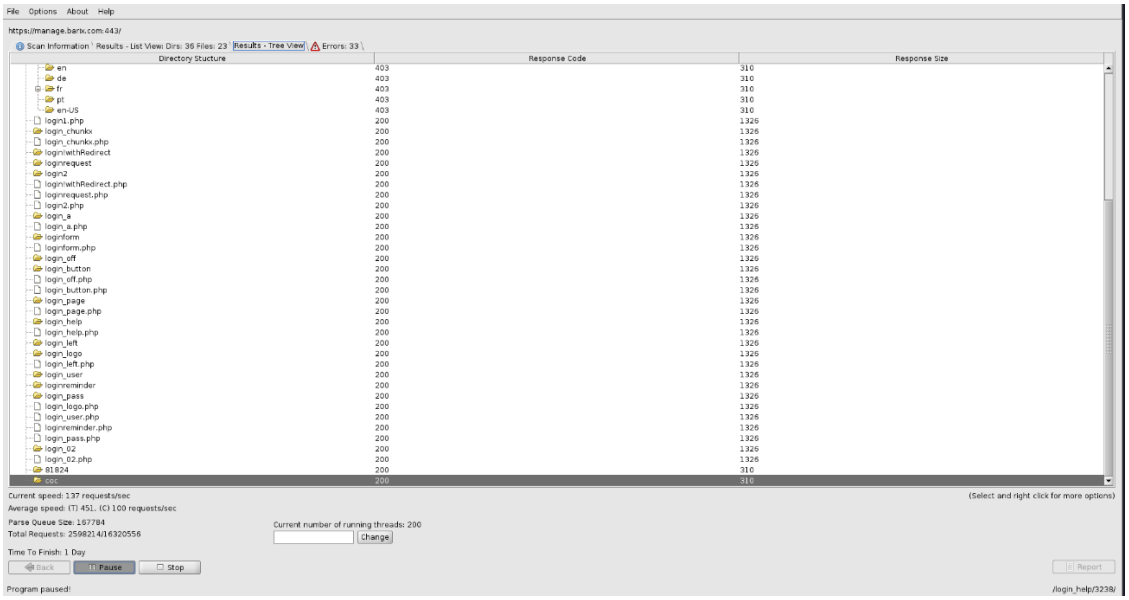

Figura 11 Brute force com uma worldlist de documentos comuns dentro do site com Dirbuster

Ao fazer um ataque brute force de diretorias o website mostra bastantes documentos que podem revelar informação adicional: passwords etc. No meu caso este teste foi bastante demorado (aproximadamente 3 horas) e houve alguns problemas com a máquina e acabei por não encontrar nada relevante.

3.1.4 Burpsuite

Burp Proxy

Permite inspecionar e modificar o tráfego entre o navegador e o aplicativo de destino. Proxy

Burp Spider

Ferramenta do tipo Web crawler para realizar a procura de conteúdo dentro de aplicações web.

Site map

Explorar o mapa de documentos do website pode mostrar informações sobre o site como roles e funcionalidades.

Mapeamos o site ao fazermos várias conexões e recebemos respostas que não são visíveis no browser.

Aqui temos o mapa do website onde mostra Diretorias do site e documentos.

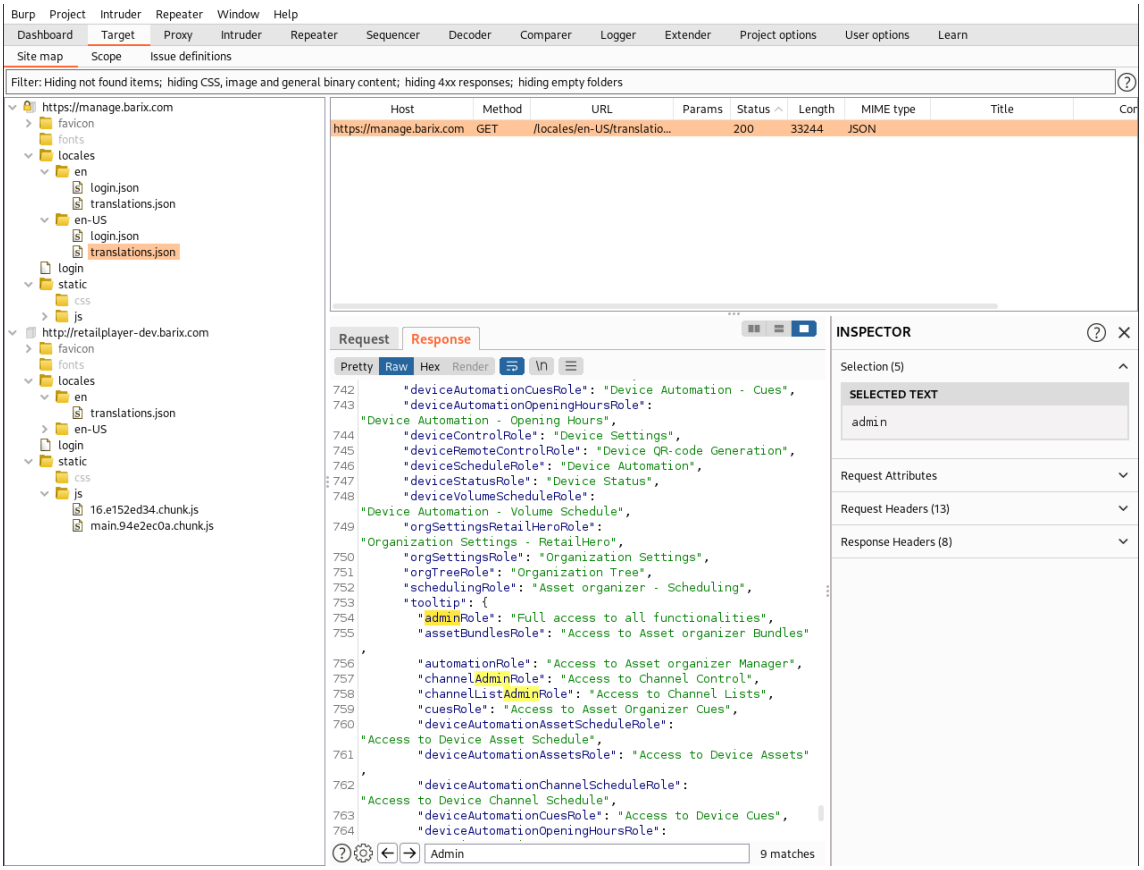

Figura 12 burpsuite mapa do site alvo

Sem um login no portal podemos obter informação das funções do portal desde Admin roles as opções de configuração dos devices.

3.1.5 Login Bruteforce

Burp Intruder

Uma ferramenta, para a realização de diversos ataques para encontrar e explorar vulnerabilidades incomuns.

Mesmo que as passwords tenham mais de 8 caracteres com letras maiúsculas, minúsculas, números e caracteres especiais, não se pode facilitar brute force pois há a possibilidade que o hacker tenha informação das vítimas e crie wordlist personalizadas para tentar adivinhar a password e username.

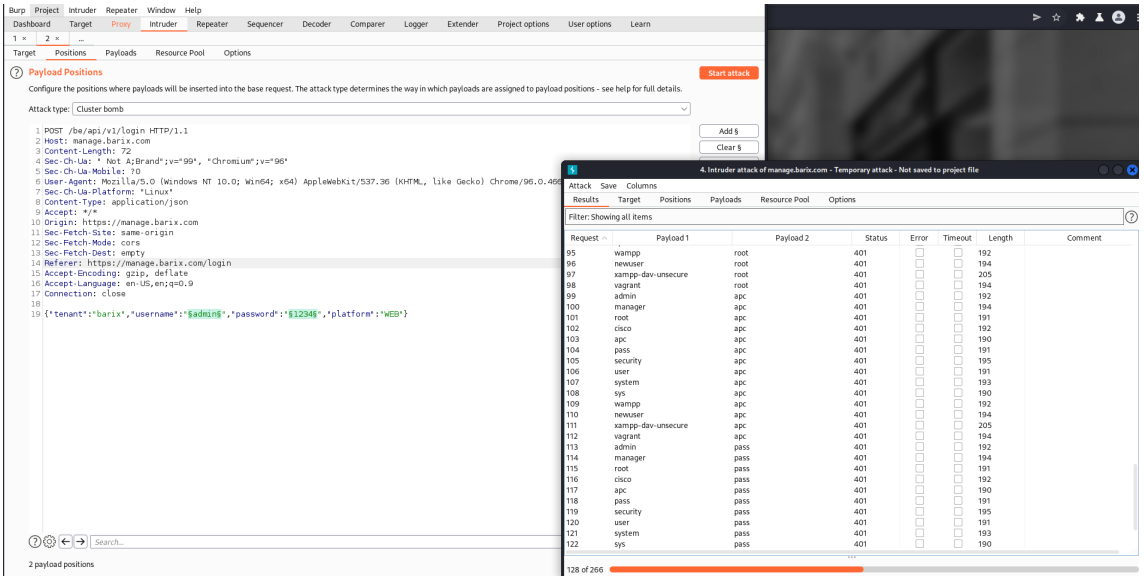

Figura 13 Login brute force com burp intruder

Com o Burp intruder podemos ver na figura 13, que temos 128 login requests sem um bloqueio de várias tentativas falhadas, o que facilita o ataque brute force do atacante.

Cenário onde o atacante tem acesso a uma conta.

3.1.6 ID das Organizações visível

Quando entramos no website a api envia para a nossa máquina a informação da conta por exemplo onde pertence as roles etc.

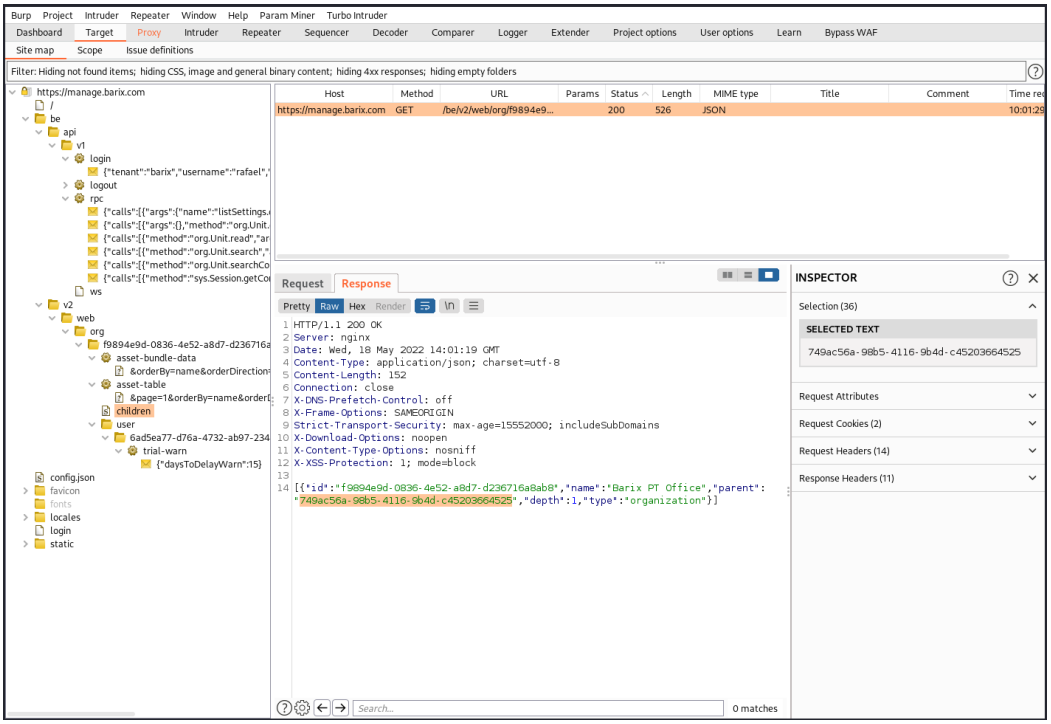

Figura 14 id da organização da conta no mapa do site

Neste caso nós temos acesso a documentos que mostram o id da organização onde com várias tentativas podemos adivinhar o endereço que leva a página edição das organizações.

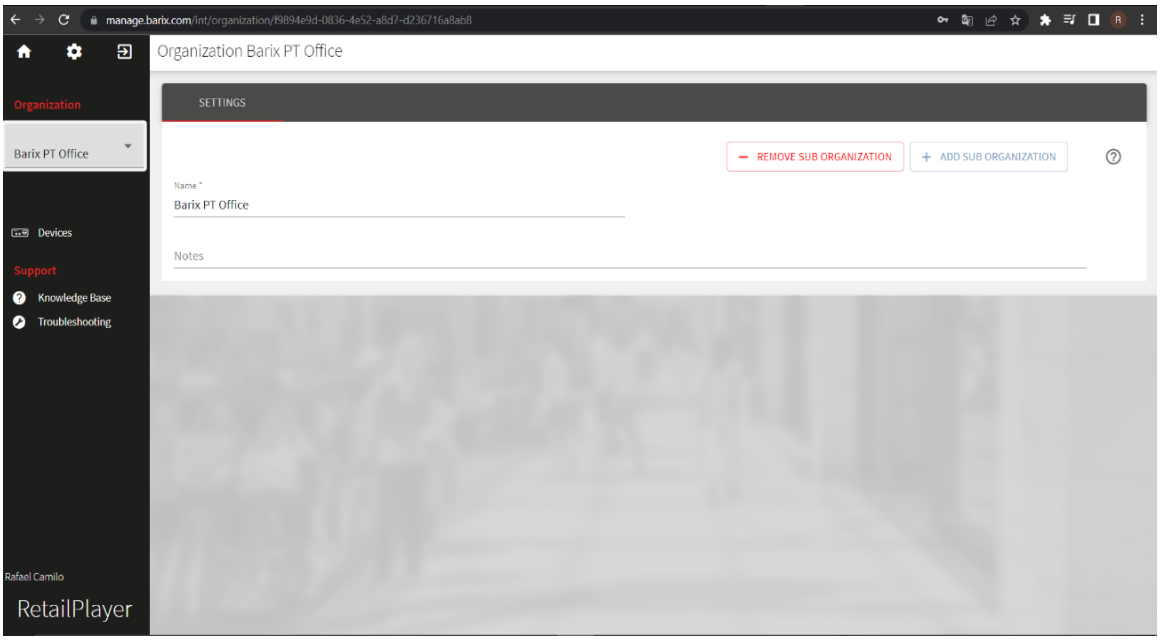

Figura 15 acesso a edição da organização dentro do site através do id

Ao usarmos o endereço https://manage.barix.com/int/organization/ com o id da organização temos acesso a edição da organização com uma conta que não tem permissões.

3.1.7 Escalação de privilégios

Burp Repeater é uma ferramenta para manipular e reenviar pedidos entre o navegador e o aplicativo de destino.

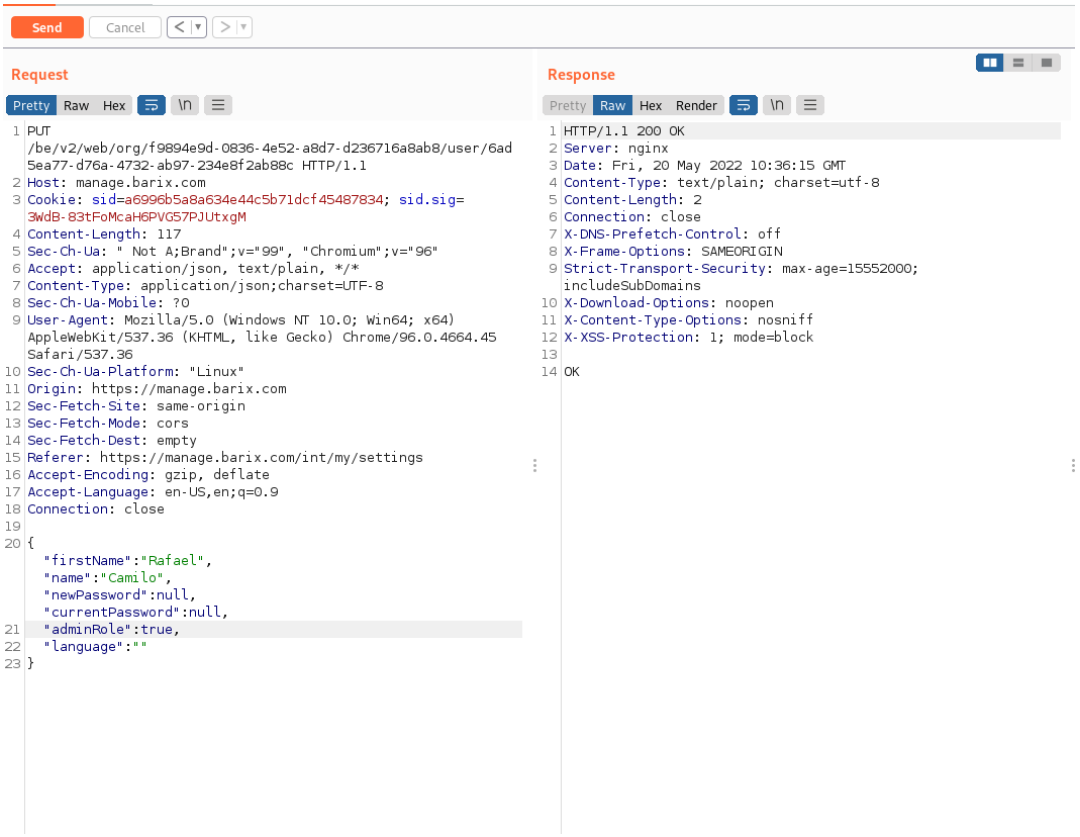

Figura 16 Uso do burp repeater para manipular o request enviado para o site

Ao alterar o nome da conta no website podemos ver no burpsuite proxy como o pedido de edição é enviado para o website, com a informação das respostas do website sabemos o nome da role admin ao manipular o pedido e adicionar “adminRole”:true a api aceita o pedido sem restrições de uma conta sem permissão.

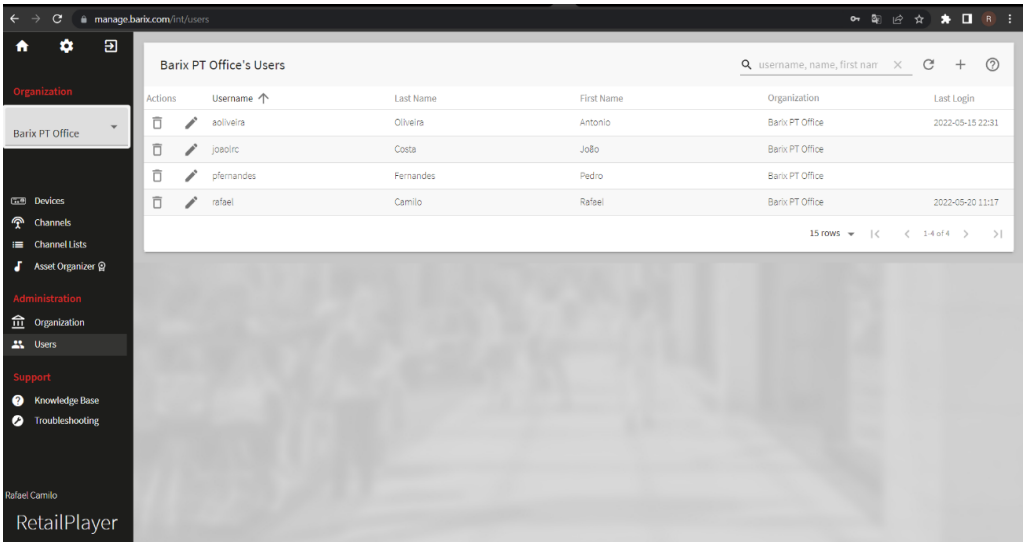

Figura 17 mostra que a conta ficou como administrador no site

Tendo acesso às contas de outros utilizadores da organização e poder editá-las mostra que a minha conta ficou com o encargo de administrador.

3.2 Scans

3.2.1 Nmap scan - https://manage.barix.com/

Uso do nmap para fazer um scan de portas vulneráveis

```
# Nmap 7.92 scan initiated Fri Apr 8 12:39:18 2022 as:
nmap -sS -A -T4 -p- -oN manage_nmap.txt 195.201.171.48

Nmap scan report for manage.barix.com (195.201.171.48)

Host is up (0.013s latency).

Not shown: 65531 filtered tcp ports (no-response)

PORT     STATE  SERVICE      VERSION

80/tcp   open   http         nginx

|_http-title: Did not follow redirect to
https://manage.barix.com/

88/tcp   closed kerberos-sec

443/tcp  open   ssl/http     nginx

|_http-title: RetailPlayer Portal

| tls-alpn:

|_  http/1.1
```

```
| tls-nextprotoneg:

|_  http/1.1

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject:
commonName=player.manage.barix.com/organizationName=Barix
AG/stateOrProvinceName=Switzerland/countryName=CH

| Not valid before: 2019-01-16T08:34:47

|_Not valid after:  2118-12-23T08:34:47

8822/tcp open   ssh          OpenSSH 7.6p1 Ubuntu
4ubuntu0.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   2048 d6:58:f8:52:f1:53:16:b8:cd:9f:30:21:97:87:97:db
(RSA)

|   256 32:e3:2e:b7:6a:c3:e0:c7:bc:4f:6e:95:af:52:77:84
(ECDSA)

|_  256 45:96:6d:2f:62:d6:3b:c1:99:76:37:7c:fc:8b:a1:4f
(ED25519)

Device type: bridge|general purpose|switch

Running (JUST GUESSING): Oracle Virtualbox (99%), QEMU
(97%), Bay Networks embedded (90%), Linux (89%), Allied
Telesyn embedded (89%)

OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
cpe:/h:baynetworks:baystack_450
cpe:/o:linux:linux_kernel:2.6.18
cpe:/h:alliedtelesyn:at-9006

Aggressive OS guesses: Oracle Virtualbox (99%), QEMU user
mode network gateway (97%), Bay Networks BayStack 450
switch (software version 3.1.0.22) (90%), Linux 2.6.18
(CentOS 5, x86_64, SMP) (89%), Allied Telesyn
AT-9006SX/SC switch (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

TRACEROUTE (using port 80/tcp)

```
HOP RTT     ADDRESS

1   5.74 ms 10.0.2.2

2   5.90 ms manage.barix.com (195.201.171.48)
```

```
OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .

# Nmap done at Fri Apr  8 13:04:42 2022 -- 1 IP address
(1 host up) scanned in 1523.85 seconds
```

3.2.2 Nikto scan - https://manage.barix.com/

Aqui usamos o nikto para fazer um scan de vulnerabilidades gerais conhecidas nas portas 80 e 443

```
- Nikto v2.1.6/2.1.5

+ Target Host: manage.barix.com

+ Target Port: 443

+ GET The anti-clickjacking X-Frame-Options header is not
present.

+ GET The X-XSS-Protection header is not defined. This
header can hint to the user agent to protect against some
forms of XSS

+ GET The site uses SSL and the Strict-Transport-Security
HTTP header is not defined.

+ GET The site uses SSL and Expect-CT header is not
present.

+ GET The X-Content-Type-Options header is not set. This
could allow the user agent to render the content of the
site in a different fashion to the MIME type

+ GET The Content-Encoding header is set to "deflate"
this may mean that the server is vulnerable to the BREACH
attack.

+ GET Hostname 'manage.barix.com' does not match
certificate's names: player.manage.barix.com

+ GET Uncommon header 'x-dns-prefetch-control' found,
with contents: off

+ OSVDB-3092: GET /login/: This might be interesting...

+ OSVDB-3093: GET /login.php3?reason=chpass2%20: This
might be interesting... has been seen in web logs from an
unknown scanner.

+ OSVDB-3233: GET /index.html.ca: Apache default foreign
language file found. All default files should be removed
from the web server as they may give an attacker
additional system information.
```

+ OSVDB-3233: GET /index.html.cz.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.de: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.dk: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ee: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.el: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.es: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.et: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.fr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.he.iso8859-8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.hr.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.it: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ja.iso2022-jp: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.kr.iso2022-kr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ltz.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.lu.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.nl: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.nn: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.no: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.po.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.pt: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.pt-br: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ru.cp-1251: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ru.cp866: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ru.iso-ru: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ru.koi8-r: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.ru.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.se: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.tw: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.tw.Big5: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: GET /index.html.var: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ GET /login_db/: Admin login page/section found.

+ GET /login-redirect/: Admin login page/section found.

+ GET /login-us/: Admin login page/section found.

+ GET /login.asp: Admin login page/section found.

+ GET /login.html: Admin login page/section found.

+ GET /login.php: Admin login page/section found.

+ GET /login1/: Admin login page/section found.

```
+ GET /loginflat/: Admin login page/section found.
```

No scan na página 27 da linha 13 a 31 mostra que faltam alguns headers de segurança como anti-clickjacking, X-XSS-Protection header, Strict-Transport-Security, X-Content-Type-Options, Content-Encoding e de resto mostra que alguns documentos que possam mostra informação sensível do website.

Scan na porta 80 por tentativa de encontrar alguma vulnerabilidade

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 195.201.171.48 -C all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          195.201.171.48
+ Target Hostname:    195.201.171.48
+ Target Port:        80
+ Start Time:         2022-05-11 10:17:24 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ 26521 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2022-05-11 10:44:36 (GMT-4) (1632 seconds)
```

O Scan na porta 80 apenas mostra a falta dos headers no código HTTP uma vez que a porta 80 não é usada e não é muito relevante.

+ 1 host(s) tested

Scan depois de um update do website.

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 195.201.171.48 -port 443
[sudo] password for kali:
      - Nikto v2.1.6
---------------------------------------------------------------------------
      + Target IP:          195.201.171.48
      + Target Hostname:    195.201.171.48
      + Target Port:        443
---------------------------------------------------------------------------
      + SSL Info:        Subject:
      /C=CH/ST=Switzerland/L=Zurich/O=Barix
      AG/CN=player.manage.barix.com
                         Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                         Issuer:   /C=CH/ST=Switzerland/O=Barix
      AG/OU=Barix AG Certificate Authority/CN=Barix AG service
      CA/emailAddress=support@barix.com
      + Start Time:         2022-05-11 10:49:23 (GMT-4)
---------------------------------------------------------------------------
      + Server: nginx
      + The anti-clickjacking X-Frame-Options header is not
      present.
      + The X-XSS-Protection header is not defined. This header
      can hint to the user agent to protect against some forms
      of XSS
      + The site uses SSL and the Strict-Transport-Security
      HTTP header is not defined.
      + The site uses SSL and Expect-CT header is not present.
      + The X-Content-Type-Options header is not set. This
      could allow the user agent to render the content of the
      site in a different fashion to the MIME type
       - STATUS: Completed 60 requests (~1% complete, 28.5
      minutes left): currently in plugin 'Guess authentication'
      - STATUS: Running average: 10 requests: 0.2363 sec.
```

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.

+ Hostname '195.201.171.48' does not match certificate's names: player.manage.barix.com

+ Uncommon header 'x-dns-prefetch-control' found, with contents: off

+ OSVDB-3092: /login/: This might be interesting...

+ OSVDB-3093: /login.php3?reason=chpass2%20: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3233: /index.html.ca: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.cz.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.de: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.dk: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ee: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.el: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.es: Apache default foreign language file found. All default files should be removed

from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.et: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.fr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.he.iso8859-8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.hr.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.it: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ja.iso2022-jp: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.kr.iso2022-kr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ltz.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.lu.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.nl: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.nn: Apache default foreign language file found. All default files should be removed

from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.no: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.po.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.pt: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.pt-br: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ru.cp-1251: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ru.cp866: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ru.iso-ru: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ru.koi8-r: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.ru.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.se: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.

+ OSVDB-3233: /index.html.tw: Apache default foreign language file found. All default files should be removed

```
from the web server as they may give an attacker
additional system information.

+ OSVDB-3233: /index.html.tw.Big5: Apache default foreign
language file found. All default files should be removed
from the web server as they may give an attacker
additional system information.

+ OSVDB-3233: /index.html.var: Apache default foreign
language file found. All default files should be removed
from the web server as they may give an attacker
additional system information.

+ /login_db/: Admin login page/section found.

+ /login-redirect/: Admin login page/section found.

+ /login-us/: Admin login page/section found.

+ /login.asp: Admin login page/section found.

+ /login.html: Admin login page/section found.

+ /login.php: Admin login page/section found.

+ /login1/: Admin login page/section found.

+ /loginflat/: Admin login page/section found.

+ /login.json: This might be interesting...

+ 7920 requests: 0 error(s) and 51 item(s) reported on
remote host

+ End Time:           2022-05-11 11:20:50 (GMT-4) (1887
seconds)
```

No scan depois da atualização do website apresenta os mesmo problemas que no scan anterior.

3.3 Retail Player Device[12]

3.3.1 Tentativa Bruteforce com Metasploit

Usei um auxiliar do Metasploit para tentar várias passwords de uma wordlist e com várias tentativas falhadas e o device não dá um timeout o que faz com que o atacante poupe tempo com ataques Brute Force.

[12] https://www.barix.com/product/retailplayer-sp400/

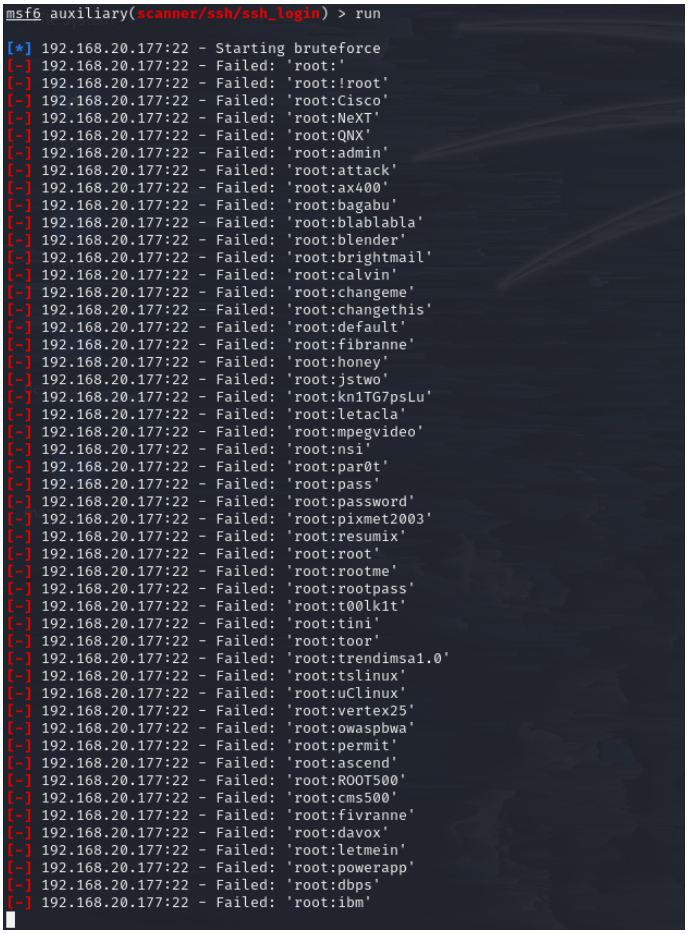

Figura 18 Brute Force acesso ao root remotamente por ssh

3.3.2 Teste DoS hping3

O que é um Denial of Service (DoS), DoS[13] é um tipo de ataque onde o atacante envia uma grande quantidade de pedidos num curto espaço de tempo para um servidor ou serviço web até fazer esse serviço web deixar de funcionar.

Quando se envia vários request pela porta 80 diretamente para o ip do player device o portal funciona normalmente apenas afeta é o portal interno do player interface weblocal.

[13] https://en.wikipedia.org/wiki/Denial-of-service_attack

```
┌──(root㉿kali)-[~]
└─# hping3 -V -S -p 80 -s 5050 192.168.20.177 --flood
using eth0, addr: 10.0.2.15, MTU: 1500
HPING 192.168.20.177 (eth0 192.168.20.177): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.20.177 hping statistic ---
25267604 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿kali)-[~]
```

Figura 19 DOS com hping3

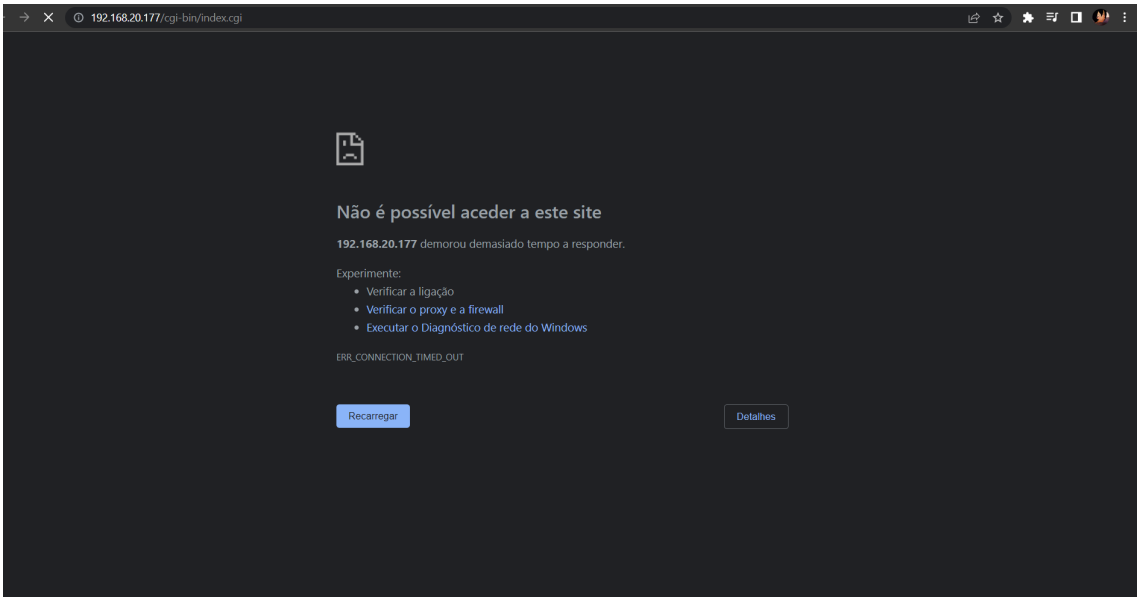

Figura 20 Resultado do DOS no Hub do retail player device

O weblocal do dispositivo vai abaixo o que pode impedir com que a vítima feche a porta 22 ssh caso o atacante queira criar uma ligação remota.

O dispositivo está vulnerável a este tipo de ataques porque não tem um limit rate ou anti spam.

3.3.3 Cartão SD

O cartão micro SD é bastante visível ao abrir a caixa do dispositivo e fácil de o retirar, com um adaptador podemos aceder ao conteúdo do cartão SD no computador e manipular System documentos como a root password, que depois vai nos dar acesso remoto ao device por ligação ssh porta 22.

Como alteramos a password root?

O sistema operativo do device é Linux logo por default as passwords do sistema vão estar encriptadas no ficheiro shadow, se encriptarmos uma password e colocarmos a Hash dessa password encriptada no ficheiro shadow em vez da hash antiga o sistema vai ler a nossa hash e desencriptar a nossa hash que vai dar a nossa password dando nos acesso ao root, também é possível identificar o tipo de encriptação antes da hash temos um valor com dois símbolos

dólares e no meio deles podemos ter por exemplo um 6 que nesse caso equivalia ao tipo de encriptação SHA512[14].

Neste caso eu usei a Hash do meu sistema Linux para alterar a password do device.

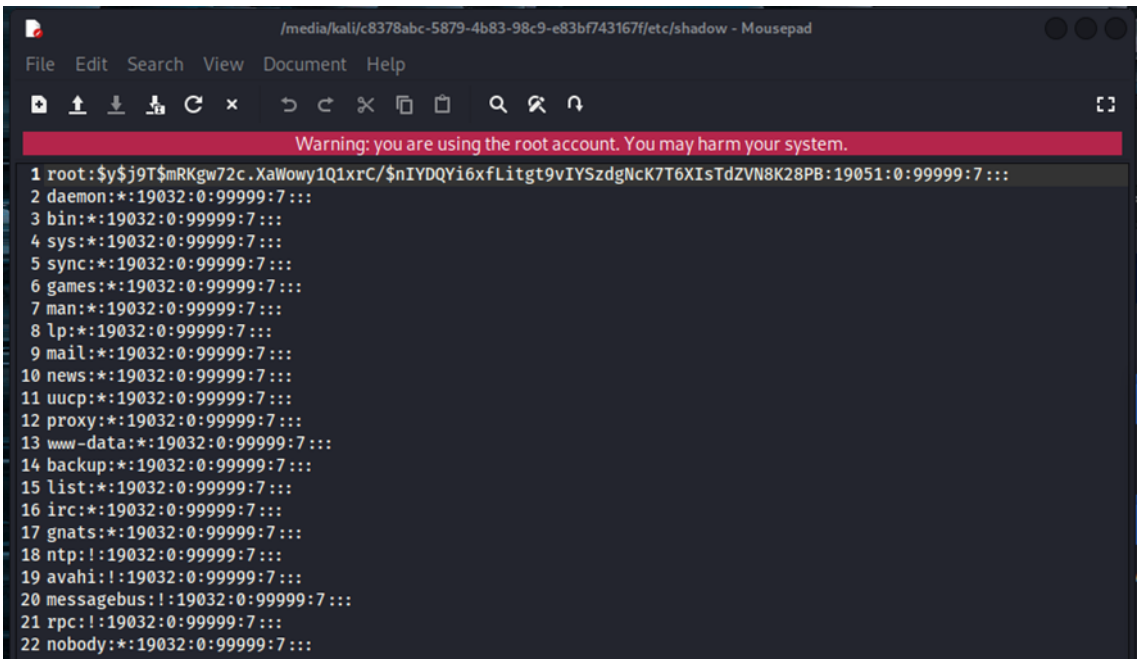

Figura 21 Pasta shadow do Root do Cartão SD do Dispositivo

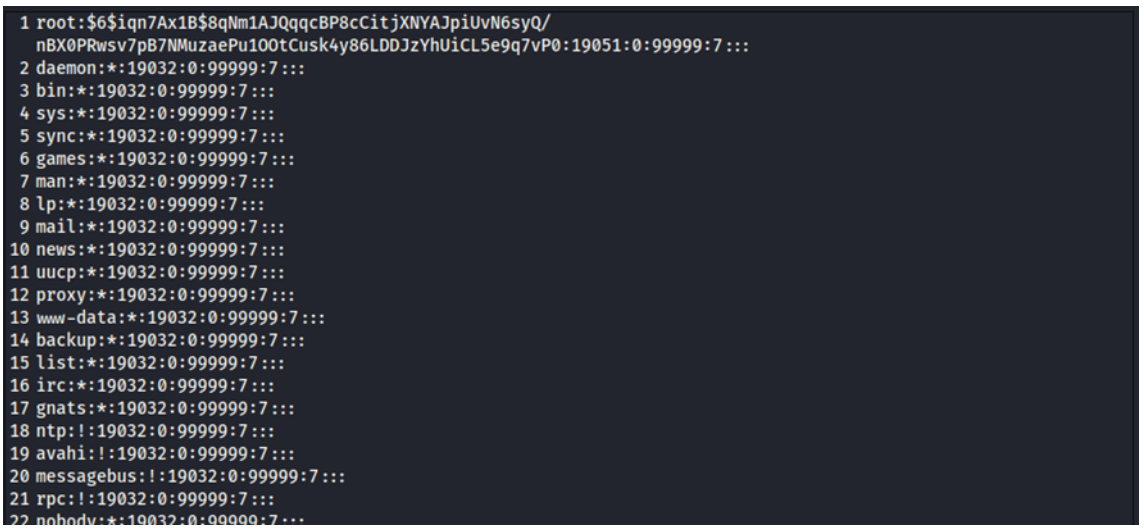

Figura 22 Pasta shadow com password hash do Root do Cartão SD do dispositivo alterada

[14] https://pt.wikipedia.org/wiki/SHA-2

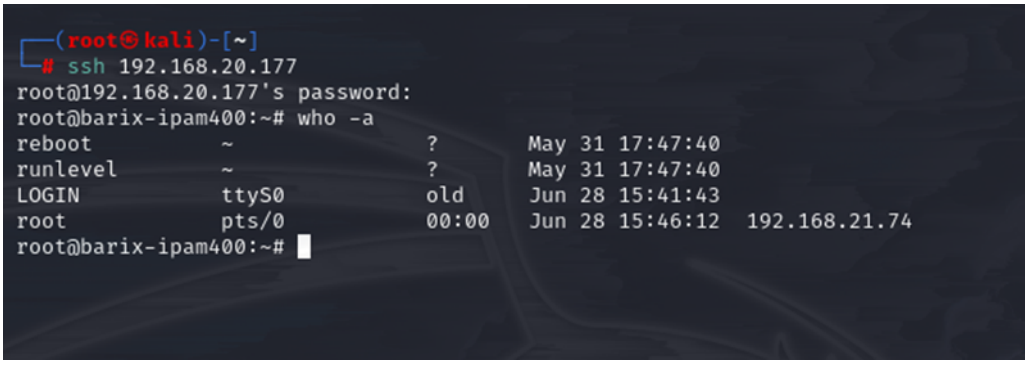

Figura 23 Acesso remoto ao root do dispositivo

Na figura 23 criamos um acesso remoto ao root do dispositivo com sucesso.

3.4 Scans no dispositivo

3.3.4 Nmap - Retail Player Device

Scan de Portas do dispositivo retail player

```
sudo nmap -sU -pU:123 -Pn -n --script=ntp-monlist
192.168.20.177
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04
05:17 EDT

Nmap scan report for 192.168.20.177

Host is up (0.0051s latency).

PORT    STATE SERVICE

123/udp open  ntp


Nmap done: 1 IP address (1 host up) scanned in 5.77
seconds

sudo nmap -n -PN -sT -sU -p- 192.168.20.177

PORT    STATE SERVICE

22/tcp  open  ssh

80/tcp  open  http

123/udp open  ntp
```

Scan de portas mais completo e discreto

```
sudo nmap -sS -A -T4 -p- 192.168.20.177

Nmap scan report for 192.168.20.177
```

```
Host is up (0.00082s latency).

Not shown: 64823 filtered tcp ports (no-response), 710
closed tcp ports (reset)

PORT   STATE SERVICE VERSION

22/tcp open  ssh     Dropbear sshd 2019.78 (protocol 2.0)

80/tcp open  http    lighttpd 1.4.55

|_http-server-header: lighttpd/1.4.55

|_http-title: 401 Unauthorized

| http-auth:

| HTTP/1.1 401 Unauthorized\x0D

|_  Digest algorithm=MD5 charset=UTF-8 qop=auth
realm=Barix Login
nonce=626282ec:58cc025eaeaf7ad0c2d8ed3b1364fa60

Device type: bridge|general purpose|switch

Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU
(93%), Bay Networks embedded (88%)

OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
cpe:/h:baynetworks:baystack_450

Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user
mode network gateway (93%), Bay Networks BayStack 450
switch (software version 3.1.0.22) (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


TRACEROUTE (using port 80/tcp)

HOP RTT     ADDRESS

1   0.45 ms 10.0.2.2

2   0.48 ms 192.168.20.177


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 1111.77
seconds
```

3.3.5 Nikto Retail Player Device

Web análise de vulnerabilidades do dispositivo através da porta 80.

sudo nikto -host 192.168.20.177

- Nikto v2.1.6

```
+ Target IP:          192.168.20.177
+ Target Hostname:    192.168.20.177
+ Target Port:        80
+ Start Time:         2022-05-02 06:39:36 (GMT-4)
Server: lighttpd/1.4.55
+ The anti-clickjacking X-Frame-Options header is not
present.
+ The X-XSS-Protection header is not defined. This header
can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This
could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ / - Requires Authentication for realm 'Barix Login'
+ No CGI Directories found (use '-C all' to force check
all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ 8066 requests: 0 error(s) and 4 item(s) reported on
remote host
+ End Time:           2022-05-02 07:04:54 (GMT-4) (1518
seconds)
```

Capítulo 4

Conclusões

Graças a este estágio na Qiba consegui melhorar as minhas competências e conhecimentos na área de cibersegurança. O estágio proporcionou-me um melhor entendimento de como os websites e API's funcionam, e também sobre outras áreas que não tinha conhecimento prévio, como Redis[15].

Apesar de a empresa Qiba não ter equipa de cibersegurança e pentest ser uma das áreas mais difíceis para começar, consegui ultrapassar as minhas dificuldades. Tive alguma ajuda dos developers do website e da equipa da Barix, nomeadamente em resposta a questões sobre o website e dispositivos retail player, mas, acima de tudo, desenvolvi aumentado de forma crescente a minha autonomia. O ser autónomo permitiu não sobrecarregar os meus colegas e criaram sinergias que fortaleceram o sentido de equipa.

Concluo então que este estágio foi uma excelente oportunidade para aprender mais sobre pentest/hacking, experienciar ser pentester numa empresa, conhecer e travar amizades com os os meus colegas, que não só me ajudaram profissionalmente, mas também me ajudaram a crescer como pessoa. Tudo isto culminou numa tremenda motivação para perseguir os meus objetivos profissionais e expandir o meu conhecimento na área.

O Curso de Cibersegurança deu-me bases bastante úteis para me tornar um profissional apesar do curso falhar um pouco no que toca a sistemas linux o que me dificultou um pouco no estágio e na área de Cibersegurança é bastante importante.

[15] https://redis.io/docs/management/security/

Referências

"WIKIPEDIA (2022) – *Nikto* [em linha]. [Consult. Abril 2022] Disponível em https://pt.wikipedia.org/wiki/Nikto_(software)"

"WIKIPEDIA (2023) – *Nmap* [em linha]. [Consult. Abril 2022] Disponível em https://en.wikipedia.org/wiki/Nmap"

"WIKIPEDIA (2022) – *Burp Suite* [em linha]. [Consult. Maio 2022] Disponível em https://pt.wikipedia.org/wiki/Burp_Suite"

"WIKIPEDIA (2020) – *SQLMap* [em linha]. [Consult. junho 2022] Disponível em https://pt.wikipedia.org/wiki/Sqlmap#:~:text=Sqlmap%20%C3%A9%20uma%20ferramenta%20de,dados%20fora%20do%20sistema%20invadido."

"WIKIPEDIA (2020) – *Metasploit* [em linha]. [Consult. Abril 2022] Disponível em https://pt.wikipedia.org/wiki/Metasploit"

"Kali Linux Tools (2022) – *hping3* [em linha]. [Consult. julho 2022] Disponível em https://www.kali.org/tools/hping3/