# UC – SISTEMAS COMPUTACIONAIS E SEGURANÇA

**Título**: Atividade – **SCSLAB08**

**Data 13/11/23**

**Grupo de no Máximo de 5 até 10 alunos**

Lucas Ferreira Andrade – 4231921505

Pedro Castro Melo - 4231925168

Bruno Batista Satyro de Castro – 4231922400 Bernardo Marconi Santos De Almeida – 4231920332 Maria Clara Marques Lino – 4231924407

Renzzo Silva Rocha – 4231925318

Erick Oliveira – 4231924394

Filipy da Silva Furtado – 42321649

Victor Henrique Dias – 4231920004

Rogério Lopes da Silva Filho - 4231925527

***Tema:*** *Atividade de Interação*
***Objetivo:*** *Acompanhamento dos projetos*
***Roteiro:*** *Formar grupos e desenvolver as atividades propostas.*

Execute os testes na interface do kali e diante da análise dos resultados verifique as proposições abaixo:

6.1. Identifique quais são as configurações de sua máquina na rede e explique qual a finalidade de aplicação de interfaces, por meio de portas SSH, em sistemas computacionais.

```
┌──(root㉿kali)-[/home/kali]
└─# ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 08:00:27:60:7f:b9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.106/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 3143sec preferred_lft 3143sec
    inet6 2804:d45:a03d:1f00:132c:c83d:5b52:5c79/64 scope global dynamic noprefixroute
       valid_lft 3356sec preferred_lft 3356sec
    inet6 fe80::eabe:fed7:83f1:cc56/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.107/24 brd 192.168.100.255 scope global dynamic noprefixroute eth1
       valid_lft 3143sec preferred_lft 3143sec
    inet6 2804:d45:a03d:1f00:f6bc:b3:b91d:eff2/64 scope global dynamic noprefixroute
       valid_lft 3356sec preferred_lft 3356sec
    inet6 fe80::5abb:9a02:3ac9:f8c3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

*Imagem 1 Configurações de rede do autor.*

**Finalidade:**

O SSH é um protocolo de rede que permite através de um ID de usuário e uso de chaves públicas, criar uma interface entre um computador local e computador remoto para uma comunicação criptografada. Com o uso dessa interface é possível realizar transferências de

arquivo, atualização de sistemas e inclusive criar um túnel seguro para o transporte de outros protocolos de aplicativo.

6.2. Identificar as informações das portas SSH e do *"fingerprint"* criado, quando da habilitação do SSH. Comparar com outras máquinas em sua rede.

```
┌──(root㉿kali)-[~]
└─# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Sun 2023-11-12 23:48:53 EST; 18min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 23518 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 23519 (sshd)
      Tasks: 1 (limit: 4603)
     Memory: 3.6M
        CPU: 275ms
     CGroup: /system.slice/ssh.service
             └─23519 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 12 23:56:32 kali sshd[27258]: Failed password for invalid user filip from 192.168.100.103 port 41575 ssh2
Nov 12 23:56:37 kali sshd[27258]: pam_unix(sshd:auth): check pass; user unknown
Nov 12 23:56:39 kali sshd[27258]: Failed password for invalid user filip from 192.168.100.103 port 41575 ssh2
Nov 12 23:56:42 kali sshd[27258]: pam_unix(sshd:auth): check pass; user unknown
Nov 12 23:56:44 kali sshd[27258]: Failed password for invalid user filip from 192.168.100.103 port 41575 ssh2
Nov 12 23:56:44 kali sshd[27258]: Connection reset by invalid user filip 192.168.100.103 port 41575 [preauth]
Nov 12 23:56:44 kali sshd[27258]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.103
Nov 12 23:56:59 kali sshd[27572]: Accepted password for kali from 192.168.100.103 port 41576 ssh2
Nov 12 23:56:59 kali sshd[27572]: pam_unix(sshd:session): session opened for user kali(uid=1000) by (uid=0)
Nov 12 23:57:00 kali sshd[27572]: pam_env(sshd:session): deprecated reading of user environment enabled
```

*Imagem 2 - Configurações de porta ssh no computador do autor.*

6.3. Explique e comente qual o significado do termo *"fingerprint"* na configuração e verificação do status da porta SSH. Quais informações importantes podemos identificar no comando **netstat**?

A "fingerprint" se refere à identificação única da versão do software ou do sistema operacional que está sendo executado em um determinado servidor.
No comando netstat, após listar as conexões de rede, podemos identificar várias informações importantes como portas abertas e escutando, ou seja portas esperando conexão, podemos identificar também endereços IP conectados, também indica se a conexão é TCP ou UDP, mostra se a conexão está estabelecida, esperando, fechada, etc.

6.4. Explique e comente qual o significado da habilitação do serviços SSH para a sua máquina. Justifique sua resposta.

**Resposta:**

Significa que eu estou habilitando a interface para conexão remota por meio do protocolo SSH (Secure Shell). Isso ocorre porque o SSH permite a criação de uma conexão criptografada entre dois hosts para envio de comandos e arquivos, ou o uso para tunelamento de outros procotocolos. Permitindo que administradores de sistemas possam fazer o seu trabalho de forma remota.

6.5. ( **Pesquisa** ) O Instituto **SANS** - *System Administration, Networking and Security,* foi lançado em 1989 como uma cooperativa para liderança inovadora em segurança da informação, a missão contínua da SANS é capacitar os profissionais de segurança cibernética. Já o **OWASP**-*Open Web Application Security Project,* é uma metodologia utilizada em ambientes e

aplicações Web. O OWASP é voltado para segurança de aplicações **Web** e apresenta uma plataforma *open source* com diversas documentações. Ela mantém uma lista de ataques a serem efetuados em aplicações web com as principais vulnerabilidades encontradas.

Acesse o link **https://owasp.org/Top10/pt_BR/ ,** analise o documento e compare com o relatório contido em **https://www.sans.org/top25-software-errors/.** Selecione **UM** tópico que apresente características semelhantes entre as **duas** abordagens. Após **comente e justifique sua escolha**.

Tópico escolhido: Falsificação de Solicitação do Lado do Servidor (SSRF)

SANS: CWE-918
OWASP: A10:2021

O meu grupo escolheu esse tópico por ser recorrente tanto em segurança no contexto de aplicações web e de necessário conhecimento para aqueles que desejam se capacitar em segurança cibernética. A Falsificação de solicitação do lado do servidor ocorre geralmente, quando se trata de aplicações web, no momento em que aplicativo da web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de lista de controle de acesso à rede (ACL).

Existem algumas formas de defesa contra esse ataque. Dentre elas, as que mais se destacam:

Imponha políticas de firewall para “negar por padrão” ou regras de controle de acesso à rede para bloquear todo o tráfego da intranet, exceto o essencial (camada de rede);

Desabilite redirecionamentos de HTTP; (camada de aplicação)

Não envie a resposta crua ao cliente (camada de aplicação)