

**Segurança de Sistema**

Curso de Engenharia Informática

3º Ano, 1º Semestre, Ano Letivo 2020/2021

|  |
| --- |
| -- ACESSO REMOTO SEGURO -- |

1. Serviço de acesso remoto, *secure shell* (**SSH**):
   1. Verifique se o serviço *secure shell* (SSH) se encontra instalado na máquina KUBUNTU. Se não existir execute o seguinte comando:
      1. sudo apt install openssh-server
   2. Utilizando o software ***nmap***, verifique na sua rede quais os hosts que têm o serviço SSH disponível;
      1. Qual o comando que utilizou: nmap -p T:22 –open 192.168.150.0/24
      2. Um desses hosts disponibiliza o serviço SSH num porto diferente do standard (entre 1500 e 2500). nmap
         1. Qual o endereço IP associado? Clique ou toque aqui para introduzir texto.
         2. Qual a versão do serviço SSH?Clique ou toque aqui para introduzir texto.
   3. Utilizando a aplicação ***putty***, faça uma ligação remota por SSH à máquina detetada (e porto detetado), utilizando o seu número de aluno e a password “SSP455#”:
      1. Tome nota da **mensagem de alerta** que irá aparecer e escreva os identificadores da chave Clique ou toque aqui para introduzir texto.
      2. Antes de aceitar a mensagem, confirme se o ***fingerprint*** da chave é idêntico a: *SHA256:arNx2Us86oRoyS/GQG5XT5kKR0HeshaxZA88lo4zgzQ*
      3. Qual é o objetivo desta mensagem de alerta? Clique ou toque aqui para introduzir texto.
      4. Ao aceitar o *fingerprint*, onde é a chave pública fica Guardada? Clique ou toque aqui para introduzir texto.
      5. Execute o acesso ao serviço SSH do Host “Descoberto” através da aplicação PUTTY (Windows). Onde ficam guardadas as chaves publicas autorizadas?

*Regedit* do sistema operativo Windows em: *HKEY\_CURRENT\_USER\Software\SimonTatham\PuTTY\SshHostKeys*

1. Autenticação através de chaves - KUBUNTU.
   1. Crie um par de chaves na sua máquina virtual e copie a chave publica para o HOST (\_\_\_.\_\_\_.\_\_\_.\_\_\_.\_\_\_) detetado no exercício anterior. Qual o comando que utilizou: Clique ou toque aqui para introduzir texto.
   2. Faça uma ligação remota SSH para o HOST detetado no exercício anterior e verifique a conetividade ao serviço SSH. Após acesso com sucesso, execute na máquina remota o seguinte comando para validação dos dados apresentados no exercício *1\_c\_ii*.

ssh-keygen -lf /etc/ssh/ssh\_host\_ecdsa\_key.pub

* 1. Se necessitar de apagar a chave publica guardada na sua máquina Kubuntu, qual o comando que deve executar?
     1. ssh-keygen -R EndereçoIPdaHostRemoto
     2. teste novamente o acesso para verificar se apagou a chave pública;

1. Autenticação através de chaves (LINUX). **Gerar chaves assimétricas** para substituir a autenticação por *username* e *password*:
   1. No sua VM, crie um **par de chaves** assimétricas do **tipo RSA e com 2048 bits**.

Clique ou toque aqui para introduzir texto.

* + 1. Tome nota da ***passphrase*** que inseriu. Clique ou toque aqui para introduzir texto.
    2. Tome nota da **diretoria** onde as chaves são guardadas. Clique ou toque aqui para introduzir texto.
    3. **Quantos ficheiros** foram criados? A que correspondem? Clique ou toque aqui para introduzir texto.
  1. Veja o **conteúdo** e calcule o ***fingerprint*** da sua **chave privada e pública**.
     1. O conteúdo é igual? Clique ou toque aqui para introduzir texto.
     2. O *fingerprint* é igual? Clique ou toque aqui para introduzir texto.
  2. Qual é o problema de criar chaves com um **tamanho muito grande**? Clique ou toque aqui para introduzir texto.
  3. **Altere a *passphrase*** da sua chave assimétrica. Coloque uma *passphrase* vazia. Utilize o comando:
     1. ssh-keygen -p
  4. Copie a chave publica para o HOST remoto (\_\_\_.\_\_\_.\_\_\_.\_\_\_.\_\_\_) detetado no exercício 2. Qual o comando que utilizou: Clique ou toque aqui para introduzir texto.
  5. Faça uma ligação remota SSH para o HOST remoto e verifique a conetividade ao serviço SSH. Após acesso com sucesso, execute no HOST remota o seguinte comando para validação dos dados apresentados no exercício *1\_c\_ii*.

ssh-keygen -lf /etc/ssh/ssh\_host\_ecdsa.key.pub

* 1. Se necessitar de apagar a chave publica guardada na sua máquina Kubuntu, qual o comando que deve executar?
     1. ssh-keygen -R EndereçoIPdaHostRemoto
     2. Teste novamente o acesso para verificar se apagou a chave pública;
  2. Quais as vantagens na utilização de chaves assimétricas para o acesso remoto por SSH?

1. Autenticação através de chaves (PUTTY). **Gerar chaves assimétricas** para substituir a autenticação por *username* e *password*:
   * 1. **Copie a chave privada** para o seu computador físico utilizando o aplicativo WINSCP.
   1. Configure o seu aplicativo PUTTY para realizar autenticação no HOST remoto utilizando a chave privada que acabou de copiar.
   2. Conseguiu utilizar a chave privada?
      1. Não. É necessário **converter** a chave privada utilizando o utilitário PUTTYGen.
      2. Tente **converter** e de seguida, **teste** o acesso remoto por chave privada.
2. Agora, vamos tentar fazer ao contrário, ou seja, vamos criar uma chave assimétrica utilizando PUTTYGEN e de seguida vamos copiá-la para o sistema operativo Kubuntu.
   1. **Crie uma chave assimétrica** no PUTTYGEN com as opções que desejar.
   2. **Guarde** a chave privada numa pasta segura no seu computador.
   3. **Copie a chave pública para o HOST remoto** de modo a que esta seja utilizada pelo openssh-server para autenticar. Para que ficheiro deve copiar? Clique ou toque aqui para introduzir texto.
   4. **Teste** o acesso remoto ao HOST remoto, a partir do PUTTY, utilizando a chave privada.

# Aplicar segurança avançada no SSH no HOST-remoto

1. O serviço SSH utiliza o ficheiro /etc/ssh/sshd\_config para as suas configurações principais.
   1. **Procure** nesse ficheiro:
      1. Onde estão **configuradas** as **chaves** que permitem autenticar o **equipamento** (*ssh\_****host****…)*? Clique ou toque aqui para introduzir texto.
      2. Onde está configurado o **ficheiro** que permite inserir **chaves públicas de utilizadores**? Clique ou toque aqui para introduzir texto.
   2. Altere o serviço de SSH de modo a que o **porto de comunicação** seja diferente do 22 (por exemplo: 2222). Qual é que foi a linha do ficheiro de configuração que alterou? Clique ou toque aqui para introduzir texto.
   3. Depois da alteração feita ao porto de rede do SSH, qual é o **comando** que tem de realizar no HOST para aceder remotamente por SSH ao HOST? Clique ou toque aqui para introduzir texto.
   4. Procure, utilizando o software **NMAP** na sua máquina física, se através da pesquisa **rápida** (nmap -sS X.X.X.X) consegue encontrar o novo porto do SSH no HOST?
   5. Altere o serviço de SSH de modo a que **não sejam permitidas autenticações por *username* e *password***. Qual é que foi a linha do ficheiro de configuração que alterou? Clique ou toque aqui para introduzir texto.
   6. Experimente utilizar o PUTTY para aceder remotamente ao HOST-A **sem recorrer a chaves privadas**. Conseguiu aceder e autenticar-se? Clique ou toque aqui para introduzir texto.
   7. Configure o serviço de SSH de modo a que **apenas o seu utilizador seja autorizado** e todos os restantes sejam negados. Qual é que foi a linha do ficheiro de configuração que alterou? Clique ou toque aqui para introduzir texto.