Painel / Meus cursos / BCC35D.IC5A CM / Sondagens (Nota 2) / Sondagem - SSH (02/12/2022)

Iniciado em domingo, 4 dez 2022, 16:14

Estado Finalizada

Concluída em domingo, 4 dez 2022, 16:19

Tempo 5 minutos 57 segundos

empregado

Avaliar 6,67 de um máximo de 10,00(**66,67**%)

Ouestão 1

Correto

Atingiu 1,00 de 1,00

No contexto do SSH, o que faz o seguinte comando?

scp teste@10.0.0.1:/tmp/texto.txt .

- a. Copia o arquivo /tmp/texto.txt do servidor SSH 10.0.0.1 para a máquina local.
- b. O comando está errado.
- oc. Copia o arquivo /tmp/texto.txt da máquina local para o do servidor SSH 10.0.0.1
- d. Copia o arquivo /tmp/texto.txt do servidor SSH 10.0.0.1 para o diretório home do usuário aluno mesmo servidor.

Sua resposta está correta.

A resposta correta é:

Copia o arquivo /tmp/texto.txt do servidor SSH 10.0.0.1 para a máquina local.

Questão **2**

Incorreto

Atingiu 0,00 de 1,00

Qual seria o comando SSH para criar um túnel SSH entre um host cliente, utilizando o usuário aluno, com o serviço de HTTP que está disponível no host 172.16.0.1, que é acessível através do servidor SSH 200.2.2.2?

- a. ssh -X -L 8080:172.16.0.1:80 aluno@200.2.2.2
- b. ssh -X -L 8080:127.0.0.1:80 aluno@200.2.2.2
- © c. ssh -X -L 8080:172.16.0.1 aluno@200.2.2.2 -p 80
- Od. ssh -X -L 8080:200.2.2.2:80 aluno@172.16.0.1

Sua resposta está incorreta.

A resposta correta é:

ssh -X -L 8080:172.16.0.1:80 aluno@200.2.2.2

orreto tingiu 1,00 de 1,00 A principal vantagem do SSH em relação ao Telnet é que o SSH provê confidencialidade aos dados transmitidos. Escolha uma opção: ② Verdadeiro ✔ ③ Falso A resposta correta é 'Verdadeiro'.	Questão 3 Correto Atingiu 100 de 100
A principal vantagem do SSH em relação ao Teinet é que o SSH provê confidencialidade aos dados transmitidos. Excolha uma opção: ② Verdadeiro ✔ ⑤ Falso A resposta correta é 'Verdadeiro'. Lustro 4 orreto langui 1.00 de 1.00 É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? ② a. sftp ✔ ③ b. stp ✔ ③ c. slogin ④ d. ssh ✔ Sua respostas corretas são: ssh. sftp, scp Uussão 5 correto langui 0.00 de 1.00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitBootLogin" como 'no', no arquivo de configuração do servidor SSH. Assim. não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ② Verdadeiro ⑥ Falso ★	Atingiu 1 00 de 1 00
Escolha uma opçāc: Verdadeiro Falso A resposta correta ê 'Verdadeiro'. É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? E a. sftp* b. scp* c. slogin d. ssh* Sua resposta está correta. As respostas corretas são: ssh, sftp, scp properties of the state of	ranga you as you
Escolha uma opçāc: Verdadeiro Falso A resposta correta ê 'Verdadeiro'. É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? E a. sftp* b. scp* c. slogin d. ssh* Sua resposta está correta. As respostas corretas são: ssh, sftp, scp properties of the state of	
Escolha uma opçāc: Verdadeiro Falso A resposta correta ê 'Verdadeiro'. É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? E a. sftp* b. scp* c. slogin d. ssh* Sua resposta está correta. As respostas corretas são: ssh, sftp, scp properties of the state of	A principal vantagem do SSH em relação ao Telnet é que o SSH provê confidencialidade aos dados transmitidos.
© Verdadeiro A resposta correta ê 'Verdadeiro'. A resposta correta ê 'Verdadeiro'. Luesto 4 Luesto 4 Luesto 5 Luesto 6 Luesto 7 Luesto 7 Luesto 8 Luesto 8 Luesto 8 Luesto 8 Luesto 8 Luesto 9 Luesto 8 Luesto 9 Luesto 10	
Palso A resposta correta é Verdadeiro . Lestão 4 Orreto Lingu 1,00 de 1,00 É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? a. sttp ✓ b. scp ✓ c. slogin d. ssh ✓ Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Sua resposta está correta. Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRoot Login" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	
A resposta correta é 'Verdadeiro'. Lestão 4 correto dirigiu 100 de 1,00 É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? a. sftp* b. scp* c. slogin d. ssh* Sua resposta está correta. As respostas corretas são: ssh. sftp, scp Lestão 5 Correto Linux (comandos vistos em nossas aulas)? Por questões de seguraça é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitKootLogin": como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	
destato 4 orreto tingiu 1,00 de 1,00 É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? iii a. sftp ✓ iii b. scp ✓ iii c. slogin iii d. ssh ✓ Sua respostas corretas. As respostas corretas são: ssh, sftp, scp vestão 5 correto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro ingla 0,00 de 1,00	○ Falso
É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? ② a. sftp ✓ ③ b. scp ✓ ③ c. slogin ② d. ssh ✓ Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Uuestão 5 correto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ④ Verdadeiro ⑤ Falso ※	A resposta correta é 'Verdadeiro'.
É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? ② a. sftp ✓ ③ b. scp ✓ ③ c. slogin ② d. ssh ✓ Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Uuestão 5 correto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ④ Verdadeiro ⑤ Falso ※	Duartãa 🐔
É ou são comandos SSH comuns em ambientes Línux (comandos vistos em nossas aulas)? a. sftp b. scp c. slogin d. ssh Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Per questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Falso Fa	Correto
É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)? ☑ a. sftp ✓ ☑ b. scp ✓ ☑ c. slogin ☑ d. ssh ✓ Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ◎ Verdadeiro ◎ Falso ★	Atingiu 1,00 de 1,00
■ a. sftp b. scp c. slogin d. ssh Sua resposta está correta. As respostas corretas são: ssh, sftp, scp scp Por questõe 5 scorreto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Verdadeiro	
© b. scp c. slogin d. ssh Sua resposta está correta. As respostas corretas são: ssh, sftp, scp uestão 5 correto tingiu 0.00 de 1.00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ○ Verdadeiro ○ Falso ★	É ou são comandos SSH comuns em ambientes Linux (comandos vistos em nossas aulas)?
© b. scp c. slogin d. ssh Sua resposta está correta. As respostas corretas são: ssh, sftp, scp uestão 5 scorreto tingiu 0.00 de 1.00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ○ Verdadeiro ○ Falso ★	
□ c. slogin □ d. ssh ✓ Sua resposta está correta. As respostas corretas são: ssh, sftp, scp utestão 5 correto tingiu 0.00 de 1.00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ○ Verdadeiro ○ Falso ★	·
Sua resposta está correta. As respostas corretas são: ssh, sftp, scp uestão 5 correto tingiu 0.00 de 1.00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	b. scp
Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Luestão 5 correto tingiu 0.00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	c. slogin
Sua resposta está correta. As respostas corretas são: ssh, sftp, scp Luestão 5 correto tingiu 0.00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	☑ d ssh❖
As respostas corretas são: ssh, sftp, scp Luestão 5 correto titingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	
As respostas corretas são: ssh, sftp, scp Luestão 5 correto titingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	
As respostas corretas são: ssh, sftp, scp Luestão 5 correto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	Sua resposta está correta.
ssp, sftp, scp westão 5 scorreto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso X	
scorreto tingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso ★	
tuestão 5 Incorreto Itingiu 0,00 de 1,00 Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: ○ Verdadeiro ○ Falso ★	
Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	
Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	Nuortão 5
Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso Falso	
Por questões de segurança é altamente recomendado não permitir o login do root via SSH. Tal ação é possível configurando a opção "PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso **	
"PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para o usuário root. Escolha uma opção: Verdadeiro Falso **	
○ Verdadeiro ⑤ Falso ★	"PermitRootLogin" como "no", no arquivo de configuração do servidor SSH. Assim, não será mais possível acessar o SSH utilizando o usuário root, todavia é possível acessar com um usuário comum e depois executar comandos como "sudo" ou "su" para trocar para
○ Verdadeiro ⑤ Falso ★	Escolha uma opção:
A resposta correta é 'Verdadeiro'.	● Falso X
A resposta correta é 'Verdadeiro'.	
	A resposta correta é 'Verdadeiro'.
	The sposal content of vertical content of

2/2022 16:21	Sondagem - SSH (02/12/2022): Revisão da tentativa
Questão 6 Correto	
Atingiu 1,00	de 1,00
J ,	
Qual ou	quais serviços, por motivos de segurança, devem ser diretamente substituídos pelo SSH?
✓ a.	Telnet *
✓ b.	HTTP *
✓ c.	FTP *
d.	DNS
Sua resp	osta está correta.
	ostas corretas são:
Teln	et ,
FTP	
Questão 7	
Correto	
Atingiu 1,00	de 1,00
Qual é a	porta padrão do SSH?
a.	TCP/53
O b.	
	TCP/22♥
d.	
o u.	
	osta está correta.
A respos	sta correta é:
TCP/22	

2/2022 16:21	Sondagem - SSH (02/12/2022): Revisão da tentativa
Questão 8	
Parcialmente correto	
Atingiu 0,67 de 1,00	
É ou são funções comuns do SSH:	
a. Transferência de arquivos	
✓ b. Terminal remoto ✓	
✓ c. Túnel criptográfico ✓	
d. HTTPS	
Sua resposta está parcialmente correta.	
Você selecionou corretamente 2.	
As respostas corretas são: Terminal remoto,	
Transferência de arquivos,	
Túnel criptográfico	
Questão 9	
Correto	
Atingiu 1,00 de 1,00	
Qual ou quais seriam tradicionalmente (que u SSH 10.0.0.1, utilizando o usuário "teste".	utilizamos em nossas aulas) os comandos Linux cliente utilizados para acessar um servidor
a. ssh	
b. ssh 10.0.0.1	
✓ c. ssh teste@10.0.0.1	
d. ssh 10.0.0.1:teste	
Sua resposta está correta.	
A resposta correta é:	
ssh teste@10.0.0.1	

Questão 10	
ncorreto	
Atingiu 0,00 de 1,00	
Qual opção do arquivo de configuração do servidor SSH impede o login de usuários com senha	as em branco?
a. PermitNullPasswords no	
 b. PermitEmptyPasswords no 	
d. NoPermitNullPasswords yes	
Sua resposta está incorreta.	
A resposta correta é:	
PermitEmptyPasswords no	
→ Aula de apoio - SSH e SAMBA (semestre passado)	
Seguir para	
	Sondagem - SAMBA (02/12/2022) ►
	Sondagem - SAMBA (02/12/2022) ►