International Journal of Advance and Innovative Research
Volume 7, Issue 1 (III): January - March, 2020 Part - 1
ISSN 2394 - 7780

VULNERABILITY ASSESSMENT & PENETRATION TESTING USING RASPBERRY-PI REMOTELY

Prof. Khalil Pinjari and Rizwan Syed
Department of Information Technology, Theem College of Engineering, University of Mumbai

ABSTRACT
This Project Report Expresses The Type Of Hardware, Software And The Results Obtained Along With Procedure Adopted To Carry Out Penetration Testing Of Organizations Network. This Project Was Successful In Quantitative And Qualitative Measurements Of The Penetration Testing Activities Using A Raspberry Pi Device And It' Uses.

This Project Report Specifies In Detail The Setup Of The Device. It Also Provides Brief Description Of The Tools Used. This Project Highlights A Very New Emerging Technique Of Penetration Testing Possible Using High Quality Tools And Reliant Hardware Which Can Be Easily Masked And Used Remotely To Affect The Target. This Project Report Vividly Documents Some Of The Potentials Emerging From This New Tool And Hence Can Be Used To Generate Awareness And Precaution Measures To Mitigate Against Such Tools If Used Unethically.

Keywords: Vapt, Raspberry Pi Infosec, Reverse Ssh Tunnel, Red Team Assessment

I. INTRODUCTION

In order to conduct an Internal Network Penetration Testing, organization needs to provide and setup a physical system for security engineer within the organization in which engineer can install tools needed for performing Reconnaissance, further vulnerability assessments and do an exploiting weakness manually. Instead of that we can use raspberry pi for internal network pen testing andfor wireless analysis.Raspberry Pi is the best way to gather information from remote sites in large distributed organizations.

Many administrations have security measures in place to block incoming connections with the goal of stopping backdoors into their network. In a white-box penetration testing, you may be explicitly able to open up a firewall to permit SSH to your Raspberry Pi. In most cases it is not possible from a company's policy standpoint; it may be difficult to achieve when dealing with multiple sites under multiple administrative controls. Reverse SSH Tunnel is a good alternative to be able to manage a Raspberry Pi running Kali Linux Remotely.

We can use a reverse SSH tunnel to access a Raspberry Pirunning Kali Linux behind a restrictive firewall or NAT gateway from outside world. While in this paper it isdemonstrated its use case for accessing it from any network via a cloud VPS using Automated Reverse SSH Tunnel Relay.

II. VULNERABILITY ASSESSMENTS

Vulnerability assessment refers to the process of recognizing risks and weaknesses in computer networks, systems, hardware, applications, and other parts of the IT environment. It also provides security teams and other participants with the information they need to analyze and prioritize risks for potential remediation in the proper setting.

Vulnerability assessments are a critical section of the vulnerability management and IT risk management lifespans, helping protect systems and data from unauthorized access and data breaches. It typically leverages tools like vulnerability scanners to identify threats and flaws within an organization's IT infrastructure that characterizes potential vulnerabilities or risk disclosures.

Vulnerability Assessment and Penetration Testing (VAPT) are the security services that emphasize on recognizing vulnerabilities in the network, server, web application and system infrastructure.

Why Vulnerability Assessments Are Important

Vulnerability assessments allow security teams to apply a reliable, comprehensive, and clear approach to classifying and determining security threats and risks. This has several benefits to an organization. Vulnerability assessments should always provide clear, actionable data on all identified threats, and the remedial actions that will be needed.

ISSN 2394 - 7780

III. PENETRATION TESTING

Penetration tests are a great way to classify vulnerabilities that exists in a system or network that has an existing security measures in place. A penetration test typically involves the use of attacking methods led by trusted individuals that are similarly used by hostile intruders or hackers

A. Vulnerabilities could be due to multiple reasons, few basic ones being:

1) Flaws in the design of hardware and software
2) Usage of unsecured network
3) Poorly configured computer systems, networks & applications
4) Complex architecture of computer systems
5) Plausible human errors

B. Phases of a penetration test:

1) Reconnaissance & Planning
2) Scanning and Enumeration
3) Actual Exploit
4) Risk Analysis & Recommendations
5) Report Generation

IV. INTERNAL NETWORK PENETRATION TESTING

Given enough time and effort, sophisticated modern-day Security Expert will find existing weaknesses in your network. That is why Red Team spend time and effort identifying vulnerabilities before bad attackers can exploit it.

Internal Network Penetration testing uses ethical hacking and controlled exploits to identify weaknesses in existing network, so you know organization's security posture.

Internal penetration testing evaluates what an insider attack could achieve. The goal is typically the similar as external penetration testing, but the major difference is the attacker either has some sort of authorized access or is starting from a point within the internal network.

A. An internal network test generally:

Tests from the perspective of both an authenticated and non-authenticated user to assess potential exploits. Evaluates the vulnerabilities that exist for systems that are accessible to authorized login IDs and that reside within the network. Checks for misconfigurations that would allow personnel to access information and accidentally leak it online. Once recognized, the vulnerabilities are presented in a format that allows an organization to evaluate their relative business risk and the cost of remediation. These can then be fixed in line with the network owner's budget and risk craving, encouraging an equivalent response to cyber risks.

In order to conduct an Internal Network Penetration Testing, organization needs to provide and setup a physical system for security engineer within the organization in which engineer can install tools needed for performing Reconnaissance, further vulnerability assessments and do an exploiting weakness manually.

Organization conducts the VAPT tests within the certain time frame. A penetration test is basically an attempt to break the security of a network or a system.

The known vulnerabilities, weaknesses or misconfigured systems have not altered within the time frame the penetration test is conducted.

IV. PENETRATION TESTING WITH RASPBERRY PI DROPBOX

The Raspberry Pi is a cheap credit-card sized computer system that may be custom-made for almost about anything including penetration testing. Raspberry Pi is that the best-known platform not as a result of it's low-cost because as a result of it's terribly powerful. Kali is a penetration testing/securityauditing Linux distribution.

Kali Linux has numerous penetration-testing programs, together with Nmap (a port scanner), Aircrack-ng (a software system suite for the penetration-testing of wireless LANs),Wireshark (a packet analyzer), John the Ripper (a password cracker), Burp suite and OWASP ZAP (both web application security scanners) and far a lot of.

ISSN 2394 - 7780

- Use a Raspberry Pi for penetration tests such as breaking wireless security, scanning vulnerabilities in networks, and capturing sensitive data.
- Turn a Raspberry Pi into a honeypot to capture sensitive information (Rogue Wireless Honeypot AP).
- Compromise wireless vulnerable keyboards and mouse.

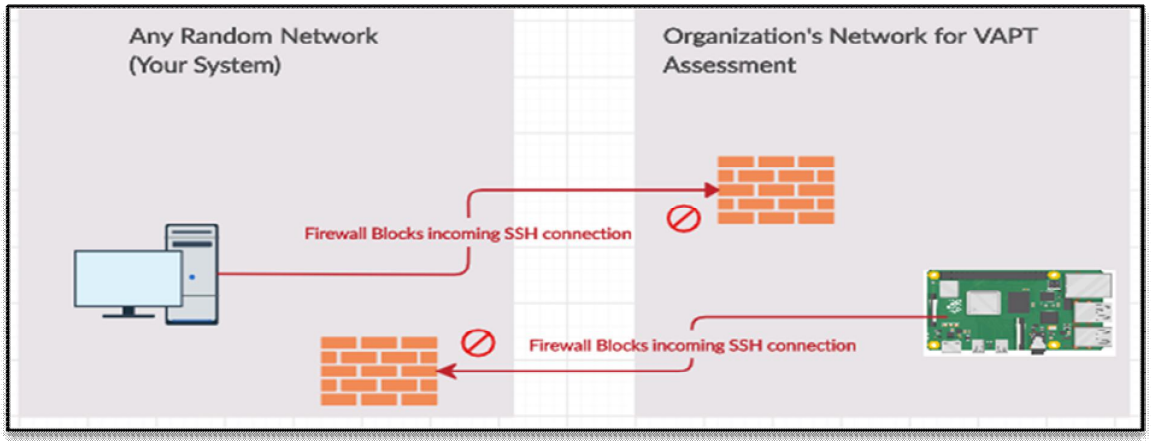
The Raspberry Pi can be configured to run Linux and most applications, nonetheless is tiny enough to suit in a pocket. This device runs most USB devices (it has four USB ports) and draws power from a small USB / Type-C charger or a battery. Also, the Raspberry Pi is an affordable platform costing around $35.00 With the right devices and some setup, the Raspberry Pi is an incredible wireless analysis and network pentest tool. The system can also be configured to begin capturing for wireless packets at boot without user action. This can be set upped anywhere in the network with network cable plugged in. This project helps in delivering low-cost, remote penetration testing nodes to hard-to-reach locations. An example of this is when a security firm offer a penetration testing services to branch offices in various different countries with restricted bandwidth across sites. Rather than flying to each location, security firm can charge their customer the cost to build a Raspberry Pi and ship out each box to a location. They can have a local person plug in the Raspberry Pi as a network tap and perform the penetration test remotely, thereby dramatically saving in travel and hardware costs.

Also, as an offensive approach the Raspberry Pi chipboard can be hidden in any official looking hardware such as a Cisco switch, hub, and so on. The average user wouldn't question a network box that looks like it belongs there. With a Raspberry Pi, the possibilities are infinite. Concerning penetration testing, Kali Linux offers pretty much everything you would need for a basic exercise. This open platform may be limited in computing power, but it does provide many powerful use cases that security professionals can leverage for penetration testing and other service engagements.

V. PREPARING A RASPBERRY PI DROPBOXCONNECT BACK USING REVERSE SSH TUNNEL

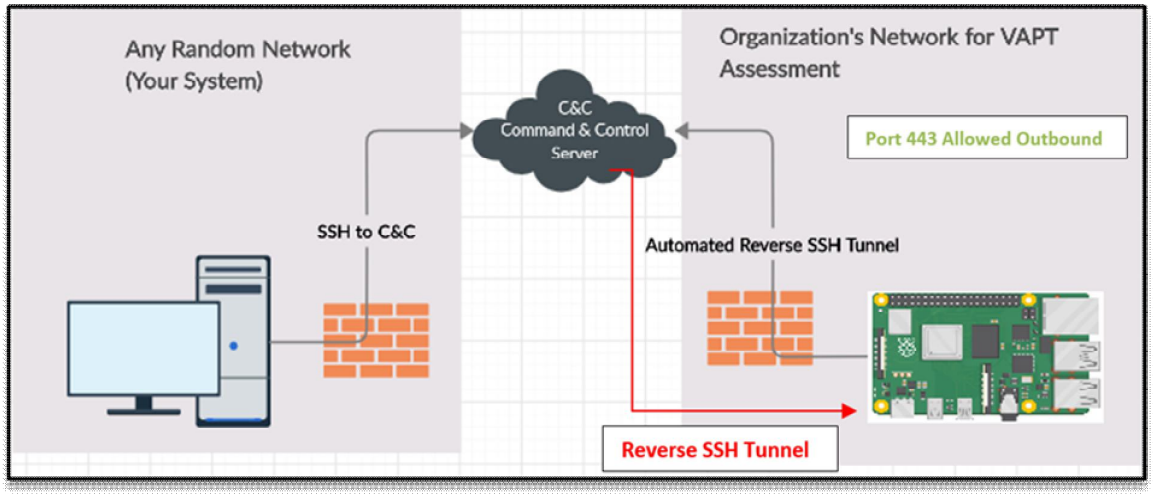
Raspberry Pi becomes common demand for security professionals to gather information from remote sites in giant distributed organizations. An example of this situation is once a security firm participate in an exceedingly security assessment that enclosed multiple locations around the world. For this state of affairs, it absolutely was impractical to travel each location to deliver native penetration testing services. To overcome this, they sent Raspberry Pi devices organized with Kali Linux to every location and remotely assessed the network for vulnerabilities at a really cheap worth.When going to remotely access multiple Raspberry Pi systems, we have a tendency to advocate putting in place a central Command and control (C&C) server instead of accessing every box separately. The C&C server ought to be a lot of powerful system like a standard server thus it will target CPU intensive tasks like breaking passwords through brute force. A lot of significant tasks may embrace exploitation through C&C server to perform the particular analysis and exploitation instead of regionally on the Raspberry Pi. While Raspberry Pi is a Drop box in company network, it connects back to a Command and control Server (C&C) once it's turned on. Either it's connected through SSH Relay (Tunneling) or by VPN to C&C Server, and security engineer connects thereto C&C Server.

Reverse shell through SSH to a Raspberry Pi at remote locations. The vital factor to think about is however you must control the Raspberry Pi once you've got placed the Raspberry Pi on the target's network, the foremost obvious and versatile way would be to SSH into KaliLinux.



ISSN 2394 - 7780

Since Kali Linux is a fully featured Linux OS, you'll control the whole environment through SSH; however, your incoming SSH connections may be blocked by firewalls or other security solutions. Many organizations have security measures in place to block incoming connections with the goal of preventing backdoors into their network. In a white-box assessment, you'll be explicitly ready to open up a firewall to allow SSH to your Raspberry Pi. The bad news is even though this is often possible from a policy standpoint, it's going to be difficult to accomplish when handling multiple sites under multiple administrative controls. Reverse SSH may be a good alternative to manage a Raspberry Pi running Kali Linux. In a reverse connection, the client connects and initiates the connection to the server instead of the server connecting to the client. In both cases, the server controls the client. We follow this approach to Avoid Firewall and Port Forwarding problems in a network.



We will use the R switch in the SSH command to create a reverse connection to the listener. A listener is the device listening to accept reverse SSH connections. In our case, the C&C server is the listener.

Command and Control Server could be any VPS Cloud Server on the internet through which we can communicate to our raspberry pi we need to configure it first by following below steps

I. Steps to follow in command and control server

1. Open your terminal either by using the Ctrl+Alt+T keyboard shortcut or by clicking on the terminal icon and install the openssh-server package by typing:

$ sudo apt install openssh-server

2. Once the installation is completed, the SSH service will start automatically or if not you can enable it manually

$ sudo service ssh start

3. To verify that the installation was successful and SSH service is running type the following command which will print the SSH server status:

$ sudo service ssh status

4. Enable the ssh service at boot, by typing

$ sudo systemctl enable ssh

```
root@ubuntuserver-vpnserver: ~
root srv01-vapt01 SSH ~ # apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.1p1-1).
The following packages were automatically installed and are no longer required:
  libct4 liblttng-ust-ctl4 liblttng-ust0 sqsh
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 143 not upgraded.
root srv01-vapt01 SSH ~ # systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root srv01-vapt01 SSH ~ # service ssh start
```

ISSN 2394 - 7780

5. Make Changes in */etc/ssh/sshd_config*to enable root login over SSH.

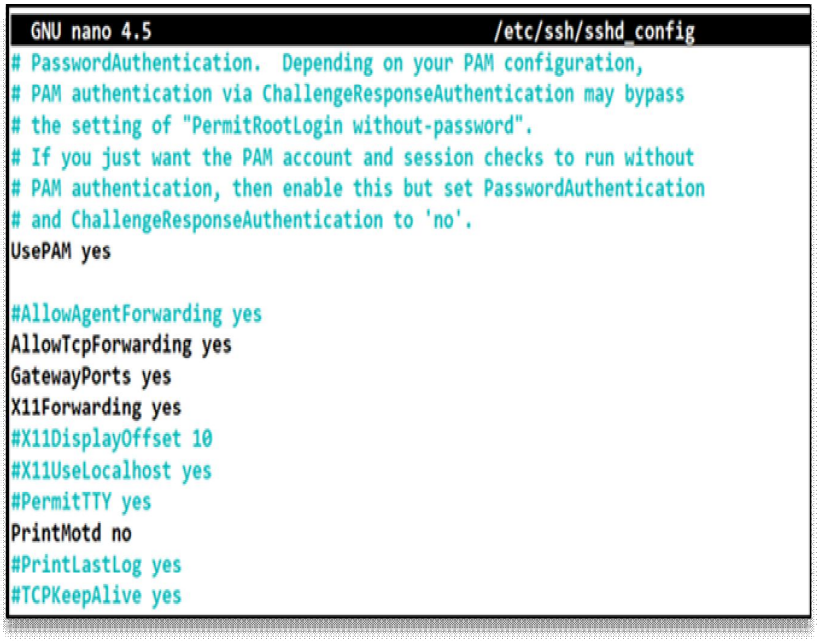
Change PermitRootLogin

PermitRootLogin yes

6. The **AllowTcpForwarding** option in the OpenSSH server configuration file must be enabled on the server to allow port forwarding. And **GatewayPorts** set to no by default prevents connecting to forwarded ports from outside the server computer. By Setting up GatewayPorts to yes, allows anyone to connect to the forwarded ports. If the server is on the public Internet, anyone on the Internet can connect to the port.

AllowTcpForwarding yes

GatewayPorts yes



7. Save the config file restart SSH Service on C&C Server

$ sudo service ssh restart

II. Steps to Follow in Raspberry Pi:

We need to configure our raspberry pi to automatically login to a C&C server via SSH without any interaction

CREATING SSH KEYPAIR FOR USER AUTHENTICATION

SSH keys give a safer approach of work into a server with SSH than using a password alone. whereas a secret will eventually be cracked with a brute force attack, SSH keys are nearly not possible to decipher by brute force alone.

Generating a key pair provides you with 2 long string of characters: a public and a private key. you'll place the public key on any server, and so unlock it by connecting thereto with a client that already has the private key. once the two matches up, the system unlocks without the necessity for a password. you'll increase security even a lot of by protective the private key with a passphrase.

The simplest way to generate a key pair is to run ssh-keygen without any arguments. during this case, it'll prompt for the file in which to store keys. Here's an example:

Eventually this program generates the key and asks for a file in which to store the private key. the public key's stored in a file with an equivalent name however '.pub' appended. The program conjointly asks for a passphrase. The passphrase may be empty to indicate no passphrase (host keys should have an empty passphrase), or it's going to be a string of arbitrary length. A passphrase is similar to a password, except it may be a phrase with a series of words, punctuation, numbers, whitespace, or any string of characters you wish.

ISSN 2394 - 7780

Type,

$ ssh-keygen

#Leave all of the settings default

Once the key pair is generated, we have to place the public key on the server that we want to use as a C&C Server

$ scp /root/.ssh/id_rsa.pub root@<C&C-Server-IP>:/root/

scp /root/.ssh/id_rsa.pub root@<*C&C-Server-IP*>:/directory/to/upload/to/

This above command will securely copy***id_rsa.pub***public key to our C&C Server

III. Steps to follow in command and control server:

Authorized keys configure access credentials and grant access to servers.Authorized keys are configured separately for each user - usually in the *.ssh/authorized_keys* file in the user's home directory.

In the previous step we have copied *id_rsa.pub* public key from our raspberry pi to C&C Server.

Now we need to append the contents of id_rsa.pubpublic key in to the *authorized_keys* file of C&C Server.

$ cat /root/id_rsa.pub >> /root/.ssh/authorized_keys

IV. Steps to Follow in Raspberry Pi:

autossh is a program to start a copy of ssh and monitor it, restarting it as necessary should it die or stop passing traffic.

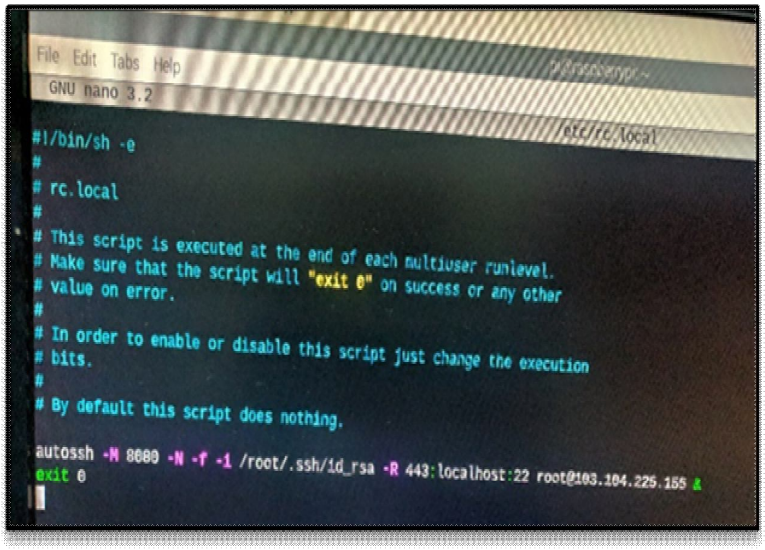
Steps to add the 'autossh' command to **/etc/rc.local** to establish the SSH tunnel at boot.

1. Open ***/etc/rc.local*** file using any text editor
2. Type,

autossh –M 8080 –N –f –i /root/.ssh/_id_rsa –R 443:localhost:22 root@<C&C-Server-IP>&

exit 0

3. Save that file and reboot Raspberry Pi



-M*port[:echo_port]*

With -M AutoSSH will continuously send data back and forth through the pair of monitoring ports in order to keep track of an established connection. If no data is going through anymore, it will restart the connection. The specified monitoring and the port directly above (+1) must be free. The first one is used to send data and the one above to receive data on.

For example, if you specify "-M 20000", **autossh** will set up forwards so that it can send data on port 20000 and receive it back on 20001.

ISSN 2394 - 7780

-f

causes autossh to drop to the background before running ssh. The -f flag is stripped from arguments passed to ssh.

-N

Do not execute a remote command. This is useful for just forwarding ports.

-R

The R switch defines the port that the remote side will connect over or how it will initiate the connection. In other words, we need to pick a port that our remote Raspberry Pi will be able to connect on. Most organizations do not have strict outbound filtering policies, making this approach more effective than a standard SSH connection. We find common ports open are TCP ports 22, 80, 443, or 53, meaning clients may be able to freely connect to the outside world using these ports.

The host-port is the port on your Raspberry Pi that has a service setup for listening. In our case, we are running an SSH server so the host-port by default will be 22.

&

Execute this command but do not wait for output or an exit code. If this is not added, your machine might hang at boot.

4. Test the key-based authentication. If all goes you should end up logged into the C2 server without the requirement of entering a password.

$ ssh root@< C&C-Server-IP>

This assumes port 443 is allowed out from the network our Raspberry Pi is connected on. If that does not work, try different ports. Most organizations will allow outbound port 443.

V. Finally test the connection

Now we can connect to raspberry-pi shell using our C&C Server. At this point raspberry pi attempt to automatically connect to C&C Server.

1. SSH to C&C Server from any network you prefer.
2. Type 'ssh root@localhost –p <port-you-specified>', in our case its 443

$ ssh@localhost –p 443

3. Above command will prompt for password of raspberry pi, Enter the credentials of the pi and you are in.

CONCLUSION

The Raspberry Pi would work perfectly for Red Team Engagement where we can place our Raspberry Pi Dropbox anywhere in client network without need to worry about company's firewall policy. Many administrations have security measures in place to block incoming connections with the goal of stopping backdoors into their network. In a white-box assessment, you may be explicitly able to open up a firewall to permit SSH to your Raspberry Pi. In most cases it is not possible from a company's policy standpoint; it may be difficult to achieve when dealing with multiple sites under multiple administrative controls. Reverse SSH is a good alternative to manage a Raspberry Pi running Kali Linux.

In a reverse SSH connection, the client connects and initiates the connection to the C&C server instead of the server connecting to the client.

REFERENCES

[1] B. Bullock, "How to Build Your Own Penetration Testing Drop Box", *BlackHills Infosec*, 2019. [Online]. Available: https://www.blackhillsinfosec.com/how-to-build-your-own-penetration-testing-drop-box/.

[2] J. Muniz, *Penetration testing with Raspberry Pi*. Birmingham, UK: Packt Publishing, 2015.

[3] R. Tyagi, "Turn your Raspberry Pi Device to an Ultimate Pentesting Machine | Lucideus Research", *Blog.lucideus.com*, 2019. [Online]. Available: https://blog.lucideus.com/2018/01/turn-your-raspberry-pi-device-to.html.

ISSN 2394 - 7780

[4] J. Zaffuto and J. Zaffuto, "How to Build Your Own Penetration Testing Dropbox Using a Raspberry Pi 4 — Artifice Security", *Artifice Security*, 2019. [Online]. Available: https://artificesecurity.com/blog/ 2019/8/6/ how-to-build-your-own-penetration-testing-drop-box-using-a-raspberry-pi-4.

[5] Sverdlov, E. (2019). "How To Set Up SSH Keys | DigitalOcean." [online] *Digitalocean.com*. Available at: https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys--2